DET JURIDISKE FAKULTET
KØBENHAVNS UNIVERSITET

Kriminalitet i en digitaliseret verden

Samlet rapport

Peter Kruize

Oktober 2013

Kriminalitet i en digitaliseret verden
Samlet rapport

Peter Kruize

Oktober 2013

ISBN 978-87-985490-2-4

Det projekt, der beskrives i denne rapport, er støttet økonomisk af Justitsministeriets Forskningspulje og Det Kriminalpræventive Råd. Projektets gennemførelse og resultater er alene forfatterens ansvar. De vurderinger og synspunkter, der fremsættes i rapporten, er forfatterens egne og deles ikke nødvendigvis af hverken Justitsministeriet eller Det Kriminalpræventive Råd.

Forord

Forskningsprojektet *Kriminalitet i en digitaliseret verden* skulle oprindeligt resultere i to delrapporter. Den første del blev publiceret i maj 2013 og belyser omfanget af og omkostningerne ved identitetstyveri og bedrageri på internettet ud fra eksisterende statistikker, offerundersøgelser og interviews med nøglerespondenter. Den anden del skulle publiceres i september 2013 og belyse gerningsmandsprofiler ud fra politiets registre.

I sommeren 2013 viste det sig dog, at Danmarks Statistik havde haft spørgsmålene vedrørende identitetstyveri og e-bedrageri som en del af deres omnibusundersøgelse i en længere periode end planlagt. Disse ekstra data fik jeg tilbudt. Desuden lancerede digitaliseringsstyrelsen i foråret 2013 en informationsportal om identitetstyveri. Det er digitaliseringsstyrelsen, der står for den overordnede koordinering af indsatsen mod identitetstyveri i Danmark, og i forbindelse med lanceringen af informationsportalen kom styrelsen med en mere snæver definition af identitetstyveri, der ikke inkluderer misbrug af betalingskortoplysninger.

Disse to begivenheder – ekstra data og en mere snæver definition af begrebet identitetstyveri – gjorde, at jeg i samråd med repræsentanter fra Justitsministeriets Forskningskontor og Det Kriminalpræventive Råd besluttede at aktualisere den første delrapport og skrive den sammen med anden delrapport. Resultatet af den samlede publikation foreligger her.

Projektet er økonomisk støttet af Justitsministeriets Forskningspulje og Det Kriminalpræventive Råd. Sociologistuderende Sanna Larsen har assisteret ved undersøgelsen og læst korrektur.

Jægerspris, d. 2. oktober 2013
Peter Kruize

Oversigt og resumé

Denne rapport belyser identitetstyveri, betalingskortmisbrug og handelsbedrageri i online verdenen. Ingen af disse kriminalitetsformer er nye, men med internettets opkommen er der åbnet op for alternative kriminelle muligheder i forbindelse hermed. Det kan derfor ikke undlades at give plads til en beskrivelse af de metoder, som internetkriminelle benytter til at begå deres gerning. De nævnte kriminalitetsformer belyses i denne rapport ud fra følgende perspektiver: Omfang, fremgangsmåde, tab, offerprofil, forebyggelse, anmeldelse, efterforskning, gerningsmandsprofil og strafudmåling.

Offerundersøgelse

For at få indblik i omfanget, tabet, offerprofilerne, anmeldelsesraten og efterforskningen benyttes en offerundersøgelse. Data er indsamlet som led i Danmarks Statistiks omnibusundersøgelse i perioden oktober 2012 til og med juli 2013. I omnibusundersøgelse adspørges ca. 960 personer pr. måned. I løbet af de ti måneder er der således adspurgt 9.582 respondenter, enten telefonisk eller via et internetspørgeskema. Respondenterne er spurgt, om de har været udsat for bedrageri ved køb eller salg af varer/ydelser over internettet indenfor de sidste 12 måneder. I så fald er de spurgt nærmere ind til e-bedrageriet: Type af e-bedrageri, vare/ydelse, beløb, hæftelse for tab, politianmeldelse og opklaring af sagen. Endvidere er alle respondenterne spurgt, om de har været udsat for misbrug af personoplysninger, identitetsbeviser eller betalingskortoplysninger inden for de sidste 12 måneder. I forbindelse hermed er respondenter, der har været udsat herfor, spurgt yderligere ind til sagen: Type oplysninger, tilegnelse, misbrug, opdagelse, beløb, hæftelse for tab, politianmeldelse og opklaring af sagen.

Polsas data

For at få indblik i gerningsmandsprofilerne of strafudmåling benyttes politiets oplysninger om sigtede personer. Rigspolitiet har stillet to datafiler til rådighed for denne undersøgelse. Den første datafil omfatter sigtelser på anmeldelser indgivet i perioden 2010-2012 mod personer, som er sigtet for overtrædelse af straffelovens §§ 171, 263, stk. 2, 279 og 279a. Analysen i dette projekt bygger på unikke personer. Det betyder, at en person som er sigtet for 30 forhold (ofte samlet i ét sagskompleks) kun tæller en enkelt gang i analysen. Den anden datafil fra Rigspolitiet er vedrørende tidligere overtrædelser. Udtrækket omfatter alle sigtelser på de cpr-numre, der optræder i den første datafil. Anmeldelserne er indgivet i perioden 2001-2009 for overtrædelse af straffeloven. Udtrækket er opdelt i henholdsvis ligeartet og anden straffelovskriminalitet. Disse to datafiler kobles sammen via sigtedes cpr-nummer. I rapporten udformes gerningsmandsprofiler over hackere, skimmere, identitetstyve, betalingskortmisbrugere og bedragere på det private marked.

Definering af identitetstyveri

Identitetstyveri er et ofte anvendt begreb, dog findes der i Danmark ikke en juridisk definition heraf. De seneste par år har der været debat om, hvorvidt identitetstyveri skal være et selvstændigt begreb i straffeloven. Der er imidlertid ikke politisk flertal for en særskilt straffebestemmelse for identitetstyveri. Identitetstyveri defineres som tilegnelse og misbrug af identitetsoplysninger. Spørgsmålet er, hvad der betragtes som identitetsoplysninger. I denne rapport anses bankooplysninger, cpr-numre, kodeord og identitetspapirer (sygesikringsbevis, kørekort m.m.) som identitetsoplysninger. I tidligere undersøgelser (Kruize, 2009, 2013) er misbrug af betalingskortoplysninger lagt under begrebet identitetstyveri. I denne rapport behandles betalingskortmisbrug separat. Grunden hertil er, at digitaliseringsstyrelsen påpeger i deres informationsportal om identitetstyveri, at misbrug af kortoplysninger ikke hører hjemme under begrebet identitetstyveri.

Omfang

Ifølge offerundersøgelsen har 4 procent af danskerne været udsat for en af de kriminalitetsformer, som denne rapport har fokus på, indenfor de sidste 12 måneder. Det svarer til ca. 166.500 danskere. Risikoen er størst for bedrageri ved internethandel. Tabellerne O.1 og O.2 giver et overblik.

Tabel O.1 Offerrisiko (n=9.582)

	Antal udsatte	Offerrisiko
Misbrug af almene ID-oplysninger	29	0,30 %
Misbrug af bank ID-oplysninger	35	0,37 %
Misbrug af digitale profiler	30	0,31 %
Misbrug af betalingskortoplysninger	71	0,74 %
Bedrageri ved butiksnethandel	159	1,66 %
Bedrageri ved privat nethandel	74	0,77 %
I alt*	**384**	**4,01 %**

* Antal udsatte summer til 398, men 14 personer har været udsat for to af kriminalitetsformerne.

Tabel O.2 Antal udsatte i Danmark: estimat og 95 % interval

	Estimat	95 % - interval
Identitetstyveri	46.900	38.400 – 55.400
Misbrug af betalingskortoplysninger	29.400	22.500 – 36.300
Bedrageri ved internethandel	109.900	95.700 – 124.100
I alt	**166.500**	**149.900 – 183.100**

Fremgangsmåde

I sagens natur sker bedrageri ved nethandel online. Ved identitetstyveri og misbrug af betalingskort kan tilegnelsen af oplysninger ske offline. Hensigten med identitetstyveriet og betalingskortmisbruget også kan knytte sig til handlinger offline, så som køb i fysiske butikker. Tabel O.3 viser, at tilegnelsen sker offline i forbindelse med en tredjedel af de misbrugte betalingskort. Derudover

svarer mange af respondenter, at de har mistet deres kortoplysninger i forbindelse med internethandel. Det fremgår ikke af undersøgelsen, hvorfor respondenterne har mistet deres kortoplysninger. Men det kan skyldes databrud i internetforretningerne. Ved identitetstyveri tegner hacking/phishing sig for mere end halvdelen af tilegnelserne af oplysninger.

Tabel O.3 Tilegnelses/misbrugsmetoder

	ID-tyveri	Kortmisbrug	Bedrageri ved internethandel
Offline	18 %	33 %	-
Hacking/phishing	53 %	24 %	-
Internethandel	16 %	41 %	100 %
Andre metoder online	13 %	2 %	-

Økonomiske tab

Alle tre former for internetkriminalitet kan føre til økonomiske tab for de udsatte. De fleste som udsættes for bedrageri i forbindelse med internethandel har økonomiske tab. Det er lidt færre af de som udsættes for misbrug af betalingskort online, der har tab. Mens det igen er færre af de som udsættes for identitetstyveri online, der har økonomiske tab. Tabel O.4 viser de samlede tab for respondenterne i offerundersøgelsen. På baggrund af det mediane tab er der udregnet et estimat for, hvad disse kriminalitetsformer koster på landsplan. Dog kender vi det officielle økonomiske tab for de som udsættes for betalingskortmisbrug fra Nets og andre kortselskaber. I 2012 er det samlede tab ifølge den officielle opgørelse 96 mio. kroner, hvilket er meget tæt på estimatet, som laves på baggrund af offerundersøgelsen. Det lyder nemlig på 91 mio. kroner.

Tabel O.4 Samlet økonomiske tab

	Undersøgelse (kroner)	Estimat for DK (mio. kroner)
Identitetstyveri	311.127	59
Misbrug af betalingskortoplysninger	639.149	91
Bedrageri ved internethandel	779.489	81
I alt	**1.729.765**	**231**

Offerprofiler

I offerundersøgelsen er der oplysninger om respondenternes køn, alder, erhverv og uddannelsesniveau. Sidstnævnte viser sig ikke at have markant indflydelse på offerrisikoen, men det har de tre øvrige. Generelt gælder det, at mænd oftere udsættes end kvinder, dog forholder det sig omvendt i forbindelse med nethandelbedrageri. Desuden daler risikoen med alderen. Det gælder dog ikke de som udsættes for kortmisbrug. Her er sammenhængen parabolsk. Ses der på sammenhængen mellem erhverv og offerrisiko, har studerende den højeste risiko og pensionister den laveste risiko.

Mens risikoen for dem i den arbejdsdygtige er midt i mellem. Igen forholder det sig anderledes for de som udsættes for kortmisbrug, her er risikofordelingen mere eller mindre jævn.

Konklusionen i forhold til offerprofilerne er, at de ikke er ens. Ved identitetstyveri er risikoen størst for yngre mænd og mindst for ældre kvinder. Forskellen er en faktor 4, offerrisikoen for yngre mænd er således 1,9 %, og for ældre kvinder er den 0,5 %. Ved kortmisbrug er risikoen størst for midaldrende mænd, mens yngre kvinder har mindst risiko. Her er forskellen en faktor 3, offerrisikoen for midaldrende mænd er således 1,1 %, og for yngre kvinder er den 0,4 %. Alder har den største indflydelse på offerrisikoen i forbindelse med bedrageri ved nethandel. Yngre kvinder har den største risiko for at blive udsat herfor, deres offerrisiko er 4,5 %. Mens ældre kvinder har den laveste risiko, deres offerrisiko lyder på 1,1 %. Forskellen er således en faktor 4.

Tabel O.5 Offerrisiko

	ID-tyveri	Kortmisbrug	Internethandel-bedrageri
Mænd	1,2 %	0,9 %	2,4 %
Kvinder	0,8 %	0,6 %	2,5 %
Under 30 år	1,6 %	0,6 %	4,0 %
30 – 49 år	1,1 %	0,9 %	3,1 %
50 år og ældre	0,6 %	0,6 %	1,4 %
Med arbejde	1,1 %	0,7 %	2,5 %
Uden arbejde	1,0 %	1,1 %	3,0 %
Studerende	1,6 %	0,7 %	4,0 %
Pensionist	0,2 %	0,6 %	0,9 %

Forebyggelse

Forebyggelse af identitetstyveri på internettet kan ske ved teknisk sikring af computeren og ved forsvarlig adfærd på internettet. Den tekniske sikring retter sig mod at undgå malware, mens den varsomme adfærd retter sig mod at hindre phishing. Der findes imidlertid mange private computere, som ikke er optimalt sikrede. Men myndighederne er nu så småt begyndt at hjælpe borgerne med at opdatere deres softwareprogrammer: Når man logger ind med NemID på Skats internetside, og den nyeste version af Java ikke er installeret på computeren, kræves en opdatering, før man kan gennemføre login-processen. Det samme gælder for virk.dk fra Digitaliseringsstyrelsen.

Misbrug af Dankort på internettet kan ske, når gerningsmanden har oplysninger vedrørende kortnummer, udløbsdato og kontrolcifre. Visa og Mastercard har introduceret den såkaldte 3D Secure: Udover kortnummer, udløbsdato og kontrolcifre skal betaleren indtaste en selvoprettet kode, før betalingen gennemføres. Det er op til den enkelte internetforretning, om denne ekstra sikring an-

vendes. Langt de fleste danske internetforretninger vælger løsningen fra. Grunden hertil er, at forretningerne vægter brugervenlighed højere end sikkerhed. Men nu hvor NemID er udrullet i Danmark, overvejes det, hvorvidt det skal fungere som 3D Secure løsning for Dankortet.

NemID – Danmarks digitale signatur – introduceres i juli 2010, og hermed er adgangen til netbank og offentlige services bedre sikret end tidligere. Når en kunde logger ind i et af disse systemer kræves en unik seks-cifret nøgle, som aflæses på kortet/viseren. Nordea benytter sig desuden af endnu et tiltag for at sikre deres netbanksløsning i forbindelse med overførsel af penge til udlandet: Der spørges om en ekstra godkendelse (sms) fra kunden. Bevæggrunden herfor er, at pengene oftest overføres til udlandet ved netbankindbrud. Der kan tænkes flere tekniske forhindringer, men også i forbindelse med forebyggelse af netbankindbrud gælder balancegangen mellem sikkerhed på den ene side og brugervenlighed på den anden side.

Sikring af netbanksløsninger sker ikke kun ved at sikre adgangen, men også ved overvågning af betalinger. Overvågning finder sted ved bankernes datacentraler. Datacentralerne kan spotte et formentligt netbankindbrud ved, at der sker en usandsynlig overførsel eller deres opmærksomhed vækkes på anden vis. Når der er tale om en pengeoverførsel til udlandet, sker den reelt set ikke med det samme, der er en såkaldt clearingsperiode – typisk på et par timer. Datacentralerne har hermed et par timer til at stoppe pengeoverførslen. Tal fra Finansrådet viser, at det lykkes datacentralerne at stoppe pengeoverførslen i clearingsperioden i forbindelse med mere end halvdelen af netbankindbruddene.

Nets fungerer som indløser af (Visa/)Dankort og sørger således for, at betalingen overføres fra køberens konto til forretningens konto. Nets overvåger ved at spotte unormale betalingsmønstre, og kriterierne herfor er erfaringsbaserede og justeres løbende. Der benyttes blandt andet såkaldte hurtigløbsovervågninger: Et kort brugs inden for en (meget) kort tidsperiode ved kortudstedernes egen bank, en anden bank, og der købes også for op til 4.000 kr. i en butik.

Privatpersoner opfordres til at være realistisk ved køb på internettet: Hvis prisen næsten er for god til at være sand, skal man være skeptisk. Desuden er der indført et e-mærke for at beskytte danskere, der handler på internettet. I alt er der 1.569 e-mærkede internetbutikker (pr. 20. september 2013), og i 2012 er der 298 sager, hvor en falsk internetbutik anmeldes for at misbruge e-mærket.

Når danskere handler på aktionssider som qxl.dk eller lauritz.com, er de beskyttet på samme vis som ved butikshandel. Det er dog ikke tilfældet ved privathandel. For at øge sikkerheden ved køb tilbyder dba.dk derfor cpr- eller nemID-validering af sælgeren.

Politianmeldelse og efterforskning

Politiets efterforskningsberedskab i forbindelse med internetkriminalitet består af tre lage. Det første lag er den almene betjent. Det andet lag er den pågældende politikreds' IT-koordinatorer, i Danmark findes i alt ca. 45 IT-koordinatorer. I princippet anmeldes og efterforskes en internetforbrydelse i politikredsen, men det er muligt at benytte NITES som har specialiseret viden inden for feltet. NITES er en del af Rigspolitiet og står for National IT-efterforskningssektion, og de er det tredje lag i politiets efterforskningsberedskab i forbindelse med internetkriminalitet. Der arbejder godt 60 personer ved NITES, og ca. 50 af disse er politiuddannede efterforskere med efteruddannelse i datalogi eller computervidenskab (ofte i udlandet). Det betyder, at der findes ca. 100 politiuddannede medarbejdere ved Dansk Politi, som har en mere specialiseret viden om efterforskning af internetkriminalitet (koordinatorer og NITES-ansatte). Dette svarer til ca. 1 procent af politiets styrke.

Efterforskning kræver en anmeldelse. Men langt fra alle anmelder identitetstyveri til politiet. I offerundersøgelsen svarer ca. 20 procent af respondenterne, der har været udsat for identitetstyveri, at de har anmeldt sagen. En anmeldelse fører dog ikke automatisk til efterforskning, selvom der altid er et digitalt spor at følge. Politiet prioriterer blandt andet ud fra tabets omfang, og om hvorvidt der er tale om en serie forbrydelser. 17 procent af respondenterne, der har været udsat for identitetstyveri og efterfølgende anmeldt sagen til politiet, svarer, at dette har ført til opklaring.

Nets står typisk for anmeldelse af betalingskort, der er spærret på grund af (forsøg på) misbrug. Dermed kan offerundersøgelsen ikke give et praj om anmeldelsestilbøjelighed i forbindelse med misbrug af betalingskort.

I offerundersøgelsen svarer 18 procent af respondenterne, der har været udsat for e-bedrageri, at de efterfølgende har anmeldt sagen til politiet. Anmeldelse sker betydeligt hyppigere i forbindelse med bedrageri ved privathandel end ved handel gennem en (falsk) internetbutik. Politiet opklarer 38 procent af sagerne, hvori anmeldelse er optaget. Men i enkelte af tilfældene i offerundersøgelsen afviser politiet anmeldelsen. I halvdelen af sagerne handler det om et butikskøb: Der er således købt en vare over nettet, men aldrig modtaget levering. I den anden halvdel af sagerne, hvor politiet afviser anmeldelsen, er der tale om private handler, hvor betaling aldrig er modtaget. Hvorfor politiet afviser anmeldelserne er ikke kendt.

Gerningsmandsprofiler

De profiler, der i rapporten udarbejdes over gerningspersonerne, baserer sig på sigtede personer. Men eftersom langt fra alle sager anmeldelse til politiet, og politiet kun opklarer et begrænset antal af de anmeldte sager, er det langt fra sikkert, at de sigtede er repræsentative for alle gerningspersoner. Specielt i forbindelse med hackersager er der grund til at tro, at kun de nemme og mere amatøragtige fører til sigtelse.

Tabel O.6 viser, at de internetkriminelle hovedsageligt er mænd. Det er blandt bedragere ved internethandel, at der findes den største andel af kvinder. Hackere, kortmisbrugere og nethandel bedragere er i mere end halvdelen af tilfældene under 25 år gamle. Specielt skimmere er lidt ældre, den største andel er mellem 25-34 år gamle. Aldersspændet for identitetstyve er bredere, de er typisk mellem 15-44 år gamle. Langt de fleste sigtede er dansk statsborger, dog er de sigtede skimmere næsten udelukkende rumænske statsborger. Derfor er de heller ikke registreret i Danmark for tidligere sigtelser. Identitetstyve, kortmisbrugere og specielt nethandel bedragere er ofte gamle kendte af politiet. En fjerdedel af nethandel bedragerne er tidligere sigtet for mere end 10 forhold.

Tabel O.6 Karakteristik over gerningspersoner

	Hackere	ID-tyve	Skimmere	Kort-misbrugere	Nethandel bedragere
Mænd	96 %	81 %	98 %	76 %	74 %
Kvinder	4 %	19 %	2 %	24 %	26 %
14 år eller yngre	4 %	-	-	4 %	-
15-24 år	45 %	39 %	19 %	54 %	60 %
25-34 år	16 %	31 %	52 %	25 %	31 %
35-44 år	21 %	24 %	25 %	11 %	24 %
45-54 år	11 %	5 %	4 %	6 %	7 %
55-65 år	3 %	2 %	-	1 %	-
Dansk statsborger	92 %	78 %	6 %	77 %	98 %
Ikke dansk statsborger	8 %	22 %	94 %	23 %	2 %
Ikke tidlige sigtet	60 %	39 %	96 %	40 %	26 %
Tidlige sigtet < 10 forhold	28 %	42 %	4 %	41 %	48 %
Tidlige sigtet >= 10 forhold	12 %	19 %	-	19 %	26 %

Strafudmåling

En sigtelses afgørelse kan træffes af anklagemyndigheden eller domstolen. Anklageren kan afgøre sagen med påtaleopgivelse (manglende beviser), tiltalefrafald eller bødeforlæg. Domstolen kan afgøre lovovertrædelsen med ubetinget eller (delvis) betinget frihedsstraf, bøde eller en anden type afgørelse, fx en foranstaltningsdom eller frikendelse.

Tabel O.7 viser, at i ca. en tredjedel af sagerne opgives sigtelsen eller tiltalen frifindes. Det vil sige, at der i en tredjedel af sagerne mangler beviser i forhold til skyldspørgsmålet. Der er dog en undtagelse i forbindelse med sigtede for bedrageri ved internethandel, 9 ud af 10 dem findes skyldige.

Når en sigtet findes skyldig i en af internetkriminalitetsformerne fører det oftest til en ubetinget eller betinget frihedsstraf. Det gælder dog ikke for sigtede i hackingsager, de dømmes sjældent til en ubetinget straf. Til gengæld anvendes bøde og tiltalefrafald hyppigere i forbindelse med hackingsager. Ses der specifikt på skimmere, kan de regne med en ubetinget frihedsstraf, når de findes skyldige.

Tabel O.7 Strafudmåling

	Hackere	ID-tyve	Skimmere	Kort-misbrugere	Nethandel bedragere
Under kriminelle lavalder	5 %	-	-	5 %	-
Påtaleopgivelse	34 %	28 %	23 %	30 %	9 %
Tiltalefrafald	16 %	2 %	-	6 %	11 %
Bødeforlæg/dom	17 %	2 %	-	8 %	9 %
Betinget dom	21 %	30 %	-	24 %	31 %
Dom	5 %	33 %	66 %	22 %	37 %
Frifindelse	2 %	5 %	11 %	5 %	3 %
Ikke beviselig skyldigt	36 %	33 %	34 %	35 %	12 %
Fundet skyldigt	59 %	67 %	66 %	60 %	88 %

Indholdsfortegnelse

1 Indledning

1.1 Internettet: en ny verden

Efter et kapløb med en britisk ekspedition ledet af Robert Scott når den norske polarforsker Roald Amundsen Sydpolen d. 14. december 1911. Hans ekspedition er den første på Sydpolen, og hermed er jorden kortlagt. Der er ingen nye horisonter, der kan opdages, i hvert fald ikke på jorden. Nye verdener skal i stedet opdages i rummet, og det er et privilegium for en meget begrænset elite af astronauter og videnskabsmænd. Men omkring den tid, hvor Neil Armstrong som første mand lander på månen (d. 20. juli 1969), lægges fundamentet til en ny verden: Den digitale verden (internettet, cyberspace). Det er *homo technologicus*, som står bag. Den nye verden rummer mange nye muligheder og er ikke kun tilgængelig for videnskabsmænd, men også for almindelige mennesker (Stol, 2012).

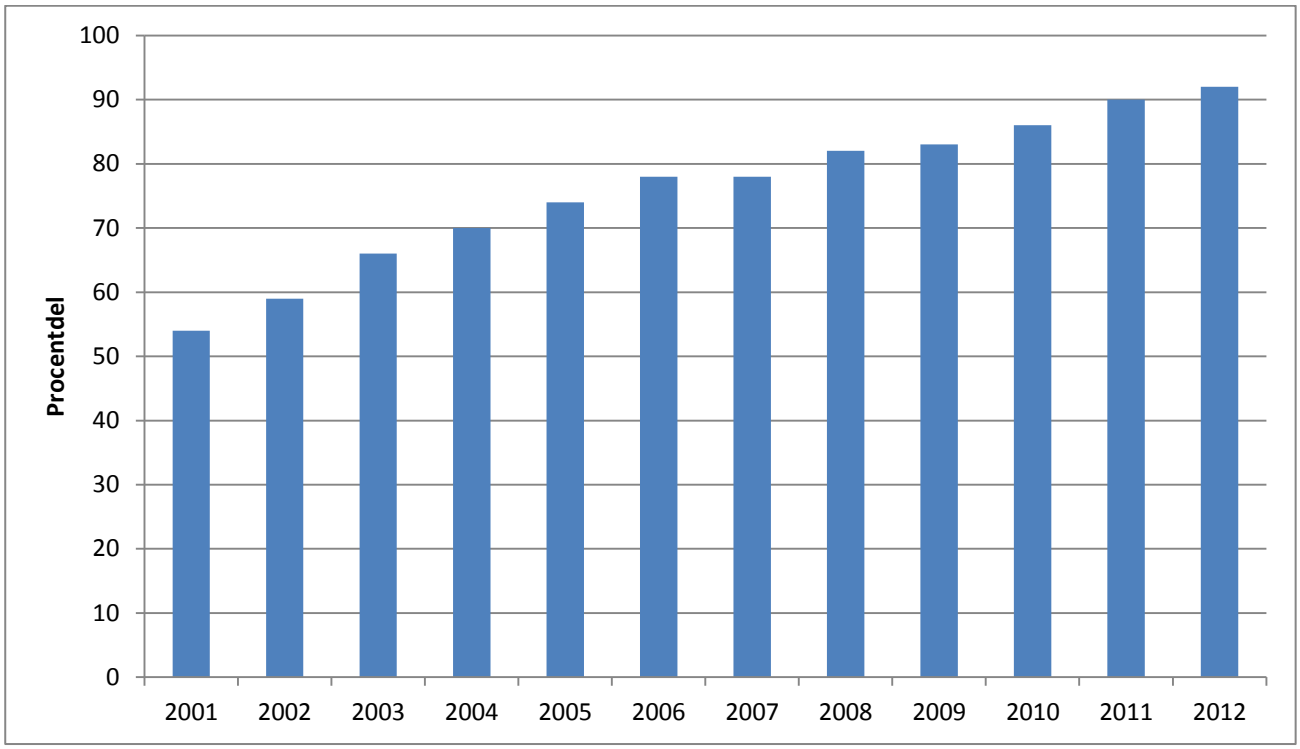
Internet er en sammentrækning af inter (mellem) og net (datanet). Det er et netværk af computere, og idéen stammer fra det amerikanske forsvar. I 1968 oprettes Arpanet, der kobler tre knudepunkter sammen. Betegnelse internet anvendes dog først i 1974, hvor antallet af hosts i netværket er 23. Det store gennembrud kommer i 1992 med oprettelsen af World Wide Web. Internettet betragtes som en af de vigtigste opfindelser i det 20. århundrede. Dette skyldes i højere grad de store samfundsmæssige konsekvenser, det fører med sig, end den tekniske innovation.

Internettets betydning er i stadig vækst, og i dag foregår en vigtig del af folks hverdag her: Både offentlige institutioner og private virksomheder benytter internettet som kommunikationsvej til deres kunder, og også internethandel er i hastig vækst. Herudover plejes personlige kontakter og venskaber på internettet ved hjælp af sociale medier som Facebook.

I 2012 er der en computer tilgængelig i 92 procent af de danske hjem, og stort set alle med computer i hjemmet har adgang til internettet. Men adgang betyder ikke nødvendigvis, at man benytter internettet. En mindre del af danskerne (6 %) bruger det aldrig, mens 81 procent er dagligt på internettet. Desuden har mere end tre ud af fire danskere (79 %) netbank, og de fleste danskere (73 %) køber varer eller ydelser over internettet. Det er først og fremmest rejserelaterede køb danskerne gør sig, efterfulgt af køb af billetter til biograf, teater mm samt tøj og sportsudstyr. Der er forskel på, hvad mænd og kvinder køber på internettet. Mænd køber oftere tekniske varer, som computersoftware og elektronik, mens kvinder oftere køber tøj, bøger og dagligvarer. Ældre danskere

(pensionister) benytter sig mindre hyppigt af internetkøb end de yngre generationer (Wijas-Jensen, 2013).

Figur 1.1 Procentdel af danskere med internetadgang i hjemmet (2001-2012)



Kilde: Danmarks Statistik (Wijas-Jensen, 2013)

1.2 En opdeling af internetkriminalitet

Når internettet indtager denne vigtige plads i vores dagligdag, er det ikke overraskende, at en stadig større del af kriminaliteten foregår her. Oversigtsværker over internetkriminalitet (fx Jewkes & Yar, 2010) viser forskelligheden i de kriminelle handlinger, der kan foretages på internettet.

Det er vigtigt at skelne mellem metode og formål i forbindelse med internetkriminalitet. Ligesom et koben kan anvendes til at brække en dør op for at komme ind i et hus, kan en trojaner bruges til at skaffe adgang til en computer. Dette er en metode til fx at stjæle forurettedes personoplysninger. Det er dog langt fra altid nødvendigt at hacke en computer i forbindelse med internetkriminalitet: At uploade eller downloade børnepornografi eller ophavsretlig beskyttet musik kræver ikke adgang til en anden persons computer. Desuden kan køb af varer med aflurede kortoplysninger klares med en almindelig adgang til en computer, og for at gøre det endnu mere komplekst kan man på internettet foretage kriminelle handlinger med oplysninger, som er opsnappet i den fysiske verden (offline).

Blandt kriminologer er der debat om, hvorvidt der opstår nye kriminalitetsformer med internettets opkommen, eller om vi kan beskrive og forklare internetkriminalitet med eksisterende begreber og teorier. David Wall (2007) skelner mellem tre former for internetkriminalitet:

1. *Computerintegritet forbrydelser* (computer integrity crimes): Disse forbrydelser retter sig mod selve computeren. Det kan fx dreje sig om hacking (uautoriseret adgang til en computer), distribuering af malware (vira, orme, trojanere) eller DDoS-angreb (overbelastning af en internetside). Disse former for internetforbrydelser kan betragtes som nye i forhold til de traditionelle former for kriminalitet.
2. *Computerassisterede forbrydelser* (computer assisted crimes): Disse forbrydelser omfatter kendte kriminalitetsformer såsom tyveri og bedrageri, der begås med hjælp fra internetteknologi. I forbindelse hermed er det især penge, varer og information, som er i fokus. Der er således en mindre grad af nyskabelse ved disse forbrydelser end ved forbrydelser, som retter sig mod computerens integritet. Men set med kriminologiske øjne er der også nye aspekter ved computerassisterede forbrydelser, fx spiller afstand og geografiske grænser ingen rolle i cyberspace.
3. *Computerindhold forbrydelser* (computer content crimes): Disse forbrydelser knytter sig til ulovligheder i forbindelse med indholdet af filer, beskeder eller andre informationer, der sendes ud på internettet. Ulovligt indhold kan fx være børnepornografisk, racistisk eller voldeligt (fx terrorisme). I forbindelse hermed handler det igen om forbrydelser, som vi kender til i forvejen, men som internettet tilfører en ny dimension i kraft af mulighederne her.

1.3 Undersøgelsens fokus, formål og problemstilling

Dette projekt har ikke til formål at undersøge al internetkriminalitet, men derimod at se nærmere på enkelte former for (berigelses)kriminalitet: Identitetstyveri på internettet, misbrug af betalingskort-oplysninger og bedrageri ved internethandel. Når disse *computerassisterede* kriminalitetsformer undersøges nærmere, må metoderne hertil også belyses.

I dette forskningsprojekt er formålet at få et bedre indblik i disse former for internetkriminalitet. I afdækningen heraf er det basale spørgsmål som omfang, udvikling, fremgangsmåde, tab, offer- og gerningsmandsprofil, der søges svar på. Projektet har desuden til formål at belyse henholdsvis borgernes, virksomhedernes og myndighedernes indsats overfor at undgå og bekæmpe disse internetkriminalitetsformer. I forbindelse hermed defineres indsats bredt: Det kan således være alt fra borgernes internetadfærd, virksomhedernes tekniske forhindringer, overvågning, privatefterforskning til myndighedernes rolle i forbindelse med disse former for kriminalitet. Forskningsprojektets problemstilling er følgende:

- I hvilket omfang og på hvilken måde er danskere udsat for identitetstyveri på internettet, misbrug af betalingskortoplysninger og bedrageri ved internethandel?
- Hvad er størrelsesbeløbet på økonomiske tab som følge af disse former for internetkriminalitet, og hvem betaler regningen?
- Hvordan ser offerprofiler ud for dem, der udsættes for identitetstyveri på internettet, misbrug af betalingskortoplysninger og bedrageri ved internethandel?
- Hvordan ser gerningsmandsprofiler ud for dem, der er sigtet for forbrydelser relateret til identitetstyveri på internettet, misbrug af betalingskortoplysninger og bedrageri ved internethandel?
- Hvilke muligheder er der for at undgå at blive udsat for identitetstyveri på internettet, misbrug af betalingskortoplysninger og bedrageri ved internethandel?
- Hvilke muligheder er der, når det gælder efterforskning og strafforfølgelse af identitetstyveri på internettet, misbrug af betalingskortoplysninger og bedrageri ved internethandel?

1.4 Undersøgelsesmetoder

Kendskab til kriminalitet baseres typisk på offerundersøgelser eller anmeldelser til politiet. Begge måleinstrumenter har sine fordele og ulemper. Offerundersøgelser kræver, at der er en forurettet part, som vil medvirke i et (telefon)interview eller en spørgeskemaundersøgelse. Politiets anmeldelsesregister er ofte blot toppen af isbjerget, da dette afhænger af privatpersonernes og virksomhedernes anmeldelsestilbøjelighed. Der benyttes derfor både eksisterende statistikker og en offerundersøgelse blandt danskere til at få indblik i identitetstyveri, misbrug af betalingskortoplysninger og bedrageri ved internethandel.

1.4.1 Eksisterende statistikker og anden viden

Det er ikke altid i virksomhedens interesse at informere politiet eller andre myndigheder, hvis de har været udsat for internetkriminalitet. Informationer herom kan nemlig tænkes at være skadelige for virksomhedens troværdighed. Eksempelvis kan det være fordelagtigt at holde et indbrud i computersystemet med kundeoplysninger skjult for offentligheden. Samtidig har politiet ikke nok ressourcer til at efterforske hver enkel forbrydelse. Det er (formentlig) almen praksis, at virksomheden selv står for overvågning, og at politiet først kommer ind i billedet, når den strafferetlige vej skal benyttes. Det betyder, at virksomheder – fx banker og betalingskortselskaber – samt brancheorganisationer antageligt har bedre indblik i internetkriminalitetens omfang end politiet.

For at få indblik i omfanget af og fremgangsmåden ved identitetstyveri på internettet, misbrug af betalingskortoplysninger og bedrageri ved internethandel inddrages derfor eksisterende statistikker, oversigter, undersøgelser samt opgørelser fra offentlige og private aktører:

- Malware og phishing (DK•CERT)
- Netbankindbrud (Finansrådet)
- Dankortmisbrug (Nets)
- Kriminalstatistik (Danmarks Statistik, Rigspolitiet)
- Internetbrug og handel (Danmarks Statistik, FDIH)

1.4.2 Offerundersøgelser blandt danskere

Danmarks Statistik gennemfører årligt en spørgeskemaundersøgelse blandt danskere om deres IT-vaner og internetadfærd. I undersøgelserne fra 2010, 2011 og 2012 er der desuden medtaget spørgsmål om sikkerhed og sikkerhedsproblemer. Undersøgelsen fra 2010 baserer sig på en stikprøve på 4.588 danskere i alderen 16-89 år, og data er indsamlet i april 2010 (Danmarks Statistik, 2011, s. 56). Undersøgelsen fra 2011 byger på en stikprøve på 4.988 danskere i alderen 16-89 år, og data er indsamlet i april og maj 2011 (Danmarks Statistik, 2012a, s. 34). Undersøgelsen fra 2012 bygger på en stikprøve på 5.224 danskere i alderen 16-89 år, og data er indsamlet i april og maj 2012 (Danmarks Statistik, 2012b, s. 32).

Danmarks Statistiks spørgeskemaundersøgelse om danskernes IT-vaner og internetadfærd giver interessante data i forbindelse med internetkriminalitet, men for at få nærmere indblik i identitetstyveri, misbrug af betalingskortoplysninger og bedrageri ved internethandel er der udført en supplerende offerundersøgelse. I forbindelse hermed er der udarbejdet et spørgeskema (se bilag 1), og data er indsamlet som led i Danmarks Statistiks omnibusundersøgelse i perioden oktober 2012 til og med juli 2013. I omnibusundersøgelse adspørges ca. 960 personer pr. måned[1]. I løbet af de ti måneder er der således adspurgt 9.582 respondenter, enten telefonisk eller via et internetspørgeskema. Tabel 1.1 viser fordelingen.

[1] "Alle månedlige bruttostikprøver er på omkring 1.700 personer. Fra bruttostikprøven ekskluderes personer, der er emigreret, er afgået ved døden, har forskerbeskyttelse eller har hemmelig adresse. Den resterende del udgør nettostikprøven, som er på omkring 1.500 personer pr. måned. Dataindsamlingen finder sted den 1.-15. i hver måned og foregår således, at der først udsendes et informationsbrev til alle i nettostikprøven. I brevet opfordres respondenterne til at besvare spørgeskemaet på internettet. Hvis de ikke har besvaret spørgeskemaet på internettet efter ca. tre dage, ringes de op af en telefoninterviewer fra Danmarks Statistik. Personer med hemmeligt nummer kan ikke ringes op, men har som alle andre mulighed for at deltage via internettet, ligesom de opfordres til selv at kontakte Danmarks Statistik med henblik på at deltage i undersøgelsen. Omtrent midt i dataindsamlingsperioden udsendes et rykkerbrev til dem, der endnu ikke har besvaret spørgeskemaet" (Tambour Jørgensen, 2013, s. 3-4).

Tabel 1.1 Respondenterne i offerundersøgelsen vedr. ID-tyveri og e-bedrageri

	Telefonisk	Internet	I alt
Oktober 2012	606	373	979
November 2012	619	379	998
December 2012	579	371	950
Januar 2013	539	430	969
Februar 2013	586	408	994
Marts 2013	590	397	987
April 2013	538	365	903
Maj 2013	599	366	965
Juni 2013	554	387	941
Juli 2013	542	354	896
I alt	**5.752**	**3.830**	**9.582**

1.4.3 Offerundersøgelser blandt virksomheder og myndigheder

Danmarks Statistik (Lundø, 2011) har undersøgt danske virksomhedernes brug af IT, og denne undersøgelse omfatter også et afsnit om IT-sikkerhed. Virksomhedernes besvarelser er indsamlet fra februar til juni 2011 i en spørgeskemabaseret stikprøveundersøgelse. 3.905 virksomheder indgår i datagrundlaget. Populationen består af firmaer med mindst 10 fuldtidsansatte, og hovedparten af brancherne i de private byerhverv er repræsenteret. I undersøgelsen er der spurgt til udsathed for sikkerhedsproblemer, sikkerhedsforanstaltninger og sikkerhedspolitik.

Danmarks Statistik (Lundø, 2012) har også undersøgt danske myndigheders anvendelse af informationsteknologi. Besvarelserne er indsamlet i august 2011 i en spørgeskemabaseret undersøgelse, der omfatter stat, regioner og kommuner. Alle landets kommuner og regioner har modtaget spørgeskemaet. Inden for den statslige sektor indgår alle departementer, styrelser og direktorater samt de største uddannelsesinstitutioner (længerevarende og videregående) i datagrundlaget. Den samlede svarprocent for alle tre sektorer er 75 procent. I undersøgelsen er der bl.a. spurgt til myndighedernes IT-sikkerhedstiltag og udsathed for IT-sikkerhedsproblemer.

1.4.4 Interviews

Der er mange (branche)organisationer og adskillige myndigheder indblandet i indsatsen overfor internetkriminalitet. For at belyse fænomenet fra flere sider er det vigtigt at inddrage de vigtigste spillere. Disse spillere publicerer statistikker, årsberetninger/rapporter og kommenterer udviklingen i diverse medier. Ikke al viden er (umiddelbart) offentlig tilgængelig. Der er derfor afholdt personlige interviews med følgende personer:

- Jesper Goul, Juridisk konsulent, Finansrådet.
- Jørgen Brinch, Senior Manager, Infrastructure DK, Nets Danmark A/S.

- Henrik Theil, Public Affairs & Kommunikationschef, FDIH – Foreningen for Distance- og Internethandel.
- Johnny Lundberg, Leder af National IT-efterforskningssektion (NITES), Rigspolitiet.

Interviewene er optaget og varer typisk 1½ time.

1.4.5 Gerningsmandsprofiler

For at få indblik i gerningsmandsprofiler benyttes politiets oplysninger om sigtede personer. Et problem med disse data er dog, at anmeldelser for identitetstyveri på internettet, misbrug af betalingskortoplysninger og bedrageri ved internethandel kan knyttes til flere forskellige lovparagraffer. I en pjece om identitetstyveri skriver politiet, at identitetstyverier kan være omfattet af straffelovens § 171 (dokumentfalsk), § 263 (hacking), § 276 (tyveri) og § 279 (bedrageri). I forbindelse med identitetstyveri på internettet, misbrug af betalingskortoplysninger og bedrageri ved internethandel forventes det, at de fleste sager findes under hacking (§ 263, stk. 2), bedrageri (§ 279) og databedrageri (§ 279a).

Rigspolitiet har stillet to datafiler til rådighed for denne undersøgelse. Den første datafil omfatter sigtelser på anmeldelser indgivet i perioden 2010-2012. Personerne er sigtet for overtrædelse af straffelovens §§ 171, 263, stk. 2, 279 og 279a. Sigtelser, hvor cpr-nummeret ikke er korrekt og sigtelser rejst mod en virksomhed, indgår ikke i filen. Data er leveret som en Excel-fil. Analysen i dette projekt bygger på unikke personer. Det betyder, at en person som er sigtet for 30 forhold (ofte samlet i ét sagskompleks) kun tæller en enkelt gang i analysen. Datafilen indeholder oplysninger om:

- Politikreds
- Gernings-, anmeldelses-, sigtelses- og afgørelsesdato
- Genstand (sagsresumé)
- Gerningskode
- Sigtedes nationalitet, køn og fødselsdato
- Forurettedes køn og fødselsdato
- Afgørelseskode

Sigtedes alder på gerningstidspunktet beregnes ud fra gerningsdato og vedkommendes fødselsdato. Sagsresuméet (genstand) benyttes til at finde frem til internetrelateret kriminalitet. I Excel kan data nemlig udvælges på baggrund af en filtrering. Filteret kan indstilles således, at teksten (sagsresuméet i dette tilfælde) indeholder eller ikke indeholder bestemte ord. Herunder beskrives, hvordan udvælgelsen finder sted:

Hackere: Det er nemmest at finde frem til personer, som er sigtede for hacking. Eftersom disse har overtrådt § 263, stk. 2, og hertil knytter sig en specifik gerningskode i Polsas (kode 74215). Datafilen indeholder oplysninger om 75 unikke personer, som er sigtede for hacking i perioden 2010-2012.

Skimmere: Skimming foregår ikke på internettet, og sigtede herfor er derfor umiddelbart ikke relevante for denne undersøgelse. Men skimmede kort anvendes oftest på internettet, da de ikke kan bruges i Danmark i en fysisk butik, efter chippen blev indført. Desuden omfattes skimming under databedrageri, straffelovens § 279a (Polsas gerningskode 76151). Derfor inkluderes gerningsmandsprofiler af skimmere i denne rapport. Datafilen indeholder oplysninger om 52 unikke personer, som er sigtede for skimming i perioden 2010-2012.

Misbrugere af id-oplysninger: Misbrug af identitetsoplysninger finder sted efter tilegnelsen af oplysningerne, som er en kriminalitet i sig selv, nemlig typisk hacking, skimming eller tyveri. Desuden hører misbrug af betalingskortoplysninger ikke under misbrug af identitetsoplysninger (jf. afsnittet nedenfor). I forbindelse med misbrug af identitetsoplysninger er der tale om, at gerningspersonen misbruger en andens navn, cpr-nummer, bankoplysninger eller lignende til at oprette et lån eller foretage en betaling over nettet. For at finde sigtede herfor i datafilen søges først på ordet 'net' (som også inkluderes i inter**net** og **net**tet) og bagefter på 'identitet', 'lån', 'navn', 'cpr' 'netbank' og 'konto'. Datafilen indeholder oplysninger om 59 unikke personer, som er sigtede for misbrug af id-oplysninger i perioden 2010-2012.

Misbrugere af betalingskort: Misbrug af betalingskort kan anses som en form for misbrug af identitetsoplysninger. Men i denne rapport betragtes misbrug af betalingskort som sin egen kriminalitetsform, idet digitaliseringsstyrelsen udelukker misbrug af betalingskort i deres definition af identitetstyveri. For at finde frem til misbrugere af betalingskort på internettet i datafilen søges først på ordet 'net' (som også inkluderes i inter**net** og **net**tet) og bagefter på 'kort'. Efterfølgende fjernes sager med ordene 'kørekort' og 'sygesikringskort'. Datafilen indeholder oplysninger om 344 unikke personer, som er sigtede for misbrug af betalingskort i perioden 2010-2012.

Bedragere på det private marked: Undersøgelsens første delrapport viste, at e-bedrageri kan forekomme, når en privatperson snyder en anden privatperson. Men også hvis en internetbutik ikke leverer en vare eller ydelse. Sidstnævnte optræder ikke i datafilen, da virksomheder ikke er en del af datasættet. Desuden er der ikke mange eksempler i datafilen, hvor privatpersoner enten ikke har betalt eller leveret en vare til en anden privatperson. Jeg formoder, at det skyldes, at alment bedrageri ikke indgår i datafilen: Det er kun databedrageri og bedrageri med stjålne dankort. Dette opdagede jeg først sent, hvorfor gerningsmandsprofilen dannes på baggrund af de få sager, der er med i datafilen. Jeg antager dog, at profilen ikke ville

være væsentlig anderledes, hvis den blev dannet på baggrund af flere sager. Men datagrundlaget burde selvfølgeligt være mere solidt. For at finde frem til bedragere på det private marked i datafilen søges først på ordet 'blå' og dernæst 'dba'. Det formodes nemlig, at mange af sagerne knytter sig til annoncer på Den Blå Avis (dba.dk). Sager fra Sy**dba**nk, hove**dba**negården og en reference til en **blå** bil dukker op i forbindelse med søgningen, og de frasorteres. Efterfølgende søges på sager, hvor ordne 'net' og 'handel' optræder. Datafilen indeholder oplysninger om 53 unikke personer, som er sigtede for bedrageri på det private marked i perioden 2010-2012.

Den anden datafil fra Rigspolitiet er vedrørende tidligere overtrædelser. Udtrækket omfatter alle sigtelser på de cpr-numre, der optræder i den første datafil. Anmeldelserne er indgivet i perioden 2001-2009 for overtrædelse af straffeloven. Udtrækket er opdelt i henholdsvis:

- Ligeartet kriminalitet: Straffelovsparagrafferne 171, 263, stk. 2, 279 og 279a.
- Anden straffelovskriminalitet: De øvrige gerningskoder i straffeloven

Disse to datafiler kobles sammen via sigtedes cpr-nummer.

2 Identitetstyveri

2.1 Hvad er identitetstyveri

Begrebet identitetstyveri har efterhånden fundet fodfæste i det danske sprog, og i langt de fleste tilfælde benyttes det i forbindelse med internet(handel). Internettet spiller således i dag en central rolle i forbindelse med misbrug af identitetsoplysninger. Men at sløre sin egen identitet har altid været en del af den kriminelle verden. Rådet for IT-sikkerhed nedlægges i 2006, men det arbejde inden da ud fra følgende definition af identitetstyveri:

> 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.

IT-sikkerhed og identitetstyveri hører nu under digitaliseringsstyrelsens kompetence. I 2013 kommer styrelsen med en informationsportal om identitetstyveri (http://www.digst.dk/Arkitektur-og-standarder/Identitetstyveri), og her defineres identitetstyveri på følgende vis:

> Det er identitetstyveri, når personlige oplysninger bliver stjålet og/eller misbrugt. Identitetstyveri dækker altså både over, at nogen ulovligt tilegner sig en andens oplysninger, og at nogen misbruger disse oplysninger til fx at optage lån, købe ting eller chikanere på forskellig måde. De personlige oplysninger kan fx være CPR-nummer, adgangskoder, sundhedsoplysninger eller andre følsomme persondata. Det er *ikke* identitetstyveri, hvis nogen opsnapper en andens kreditkortoplysninger og misbruger dem.

Forskellen mellem disse to definitioner er, at digitaliseringsstyrelsen udelukker misbrug af betalingskortoplysninger fra begrebet identitetstyveri. Dette er nyt, og Danmark adskiller sig således fra de fleste europæiske lande. Jeg har i hvert fald ikke kendskab til andre, som udelukker misbrug af betalingskortoplysninger. Det diskuteres imidlertid internationalt, hvorvidt kortsvindel hører under begrebet identitetstyveri. Særligt repræsentanter fra finansverdenen mener, at dette ikke burde være tilfældet (se fx Cheney, 2005, p. 2). Denne diskussion er specielt aktuel i USA, men The Federal

Identity Theft and Assumption Deterrence Act fra 1998 inkluderer kortsvindel i begrebet identitetstyveri.[2]

Ifølge digitaliseringsstyrelsens definition er der to led i forbindelse med identitetstyveri: (1) at tilegne sig en andens personoplysninger, og (2) at udgive sig for at være denne person. Danmark tilslutter sig dermed måden, hvorpå identitetstyveri ofte defineres internationalt. Dog påpeger bl.a. McNally & Newman (2008), at der ikke er konsensus om definitionen af identitetstyveri, men at begrebet generelt set refererer til en situation, hvor en person anvender en andens personlige oplysninger til at begå svig eller misbrug. OECD drager samme konklusion, nemlig at der ikke findes en internationalt accepteret definition, og beskriver identitetstyveri på følgende vis:

> 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. (OECD, 2009, s. 16).

Ifølge McNally & Newman bruges begreberne identitetstyveri (identity theft) og identitetssvig (identity fraud) ofte 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) betragtes identitetssvig både som misbrug af rigtige personoplysninger og misbrug ved hjælp af fiktive oplysninger, mens identitetstyveri kun knytter sig til misbrug af rigtige personoplysninger.[3]

I denne rapport anvendes digitaliseringsstyrelsens definition af identitetstyveri, hvilket betyder, at brugen af en *fiktiv* identitet ikke regnes under begrebet identitetstyveri. Tilegnelse og misbrug af betalingskortoplysninger anses ikke for identitetstyveri, og denne form for kriminalitet beskrives derfor særskilt i kapitel 5.

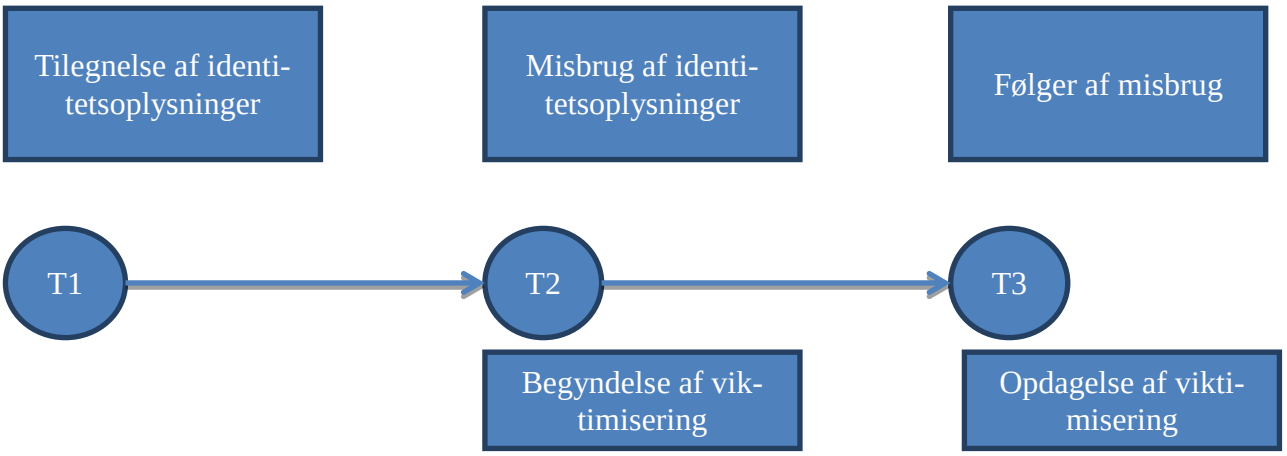
---

[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."

[3] "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).

De forskellige varianter af identitetstyveri har det tilfælles, at specifikke identitetsoplysninger tilegnes af gerningspersonen, og at disse oplysninger misbruges på et senere tidspunkt. Det betyder, at der er en tidsforskel mellem tilegnelse og misbrug. Desuden kan det også tage tid, førend forurettede opdager, at vedkommendes identitetsoplysninger er blevet misbrugt. Nedenstående skema viser processen.

Skema 2.1 Tre faser af identitetstyveri i tidsperspektiv



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

2.2 Identitetstyveri og straffeloven

Identitetstyveri er et ofte anvendt begreb, dog findes der i Danmark ikke en juridisk definition af det. Juridisk set er identitetstyveri et misvisende begreb. Ordet tyveri lægger nemlig op til, at man ejer sin identitet akkurat som en materiel genstand (Prins & Van der Meulen, 2006). Rigsadvokaten tilkendegiver på spørgsmål fra retsudvalget, at en falsk profil på internettet, hvor en udgiver sig for at være en anden eksisterende person, som udgangspunkt ikke i sig selv kan anses for strafbar. Rigsadvokaten tilføjer, at der imidlertid kan være tale om strafbare forhold i forbindelse med sådan en handling (JM, 2009, s. 2):

> Efter omstændighederne vil oprettelsen af en falsk internetprofil, hvorved man udgiver sig for at være en anden eksisterende person – og i den forbindelse videregiver oplysninger om den pågældende – imidlertid kunne udgøre en overtrædelse af straffelovens § 264 d. Efter denne bestemmelse straffes den, der uberettiget videregiver meddelelser eller billeder vedrørende en andens private forhold eller i øvrigt billeder af den pågældende under omstændigheder, der åbenbart kan forlanges unddraget offentligheden. Det er uden betydning for strafbarheden, om meddelelsen er sand.

> Tilsvarende må det antages, at oprettelsen af en profil på internettet i en andens navn efter omstændighederne vil kunne udgøre en overtrædelse af straffelovens § 267, hvorefter den, som krænker en andens ære ved fornærmelige ord eller handlinger eller ved at fremsætte eller udbrede sigtelser for et forhold, der er egnet til at nedsætte den fornærmede i medborgeres agtelse, straffes.

Ifølge OECD har ikke mange lande specifik lovgivning vedrørende identitetstyveri. USA må betragtes som forgangsland på dette område, idet identitetstyveri er en selvstændig forbrydelse her. I USA defineres identitetstyveri (ID Theft) på følgende vis:

> Knowingly transfers, possesses, uses, with-out 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 bliver et lovforslag vedrørende identitetstyveri i 2005 ikke til noget, da den franske justitsminister trækker forslaget tilbage i 2006 med den begrundelse, at identitetstyveri på tilstrækkelig vis kan straffes efter den eksisterende lovgivning (OECD, 2009, p. 50). Ifølge OECD har der ikke været andre initiativer i EU-medlemsstaterne til at betragte identitetstyveri som en selvstændig forbrydelse.

I Norge er identitetstyveri efter den nye straffelov en selvstændig forbrydelse. Den nye bestemmelse om identitetskrænkelse giver straf til den, som tager en andens identitet, optræder med en andens identitet 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 indbefatte 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, der omfattes af den nye bestemmelse, allerede er strafbare under den gamle straffelov. Det gælder blandt andet bedrageribestemmelser. Dog er det her en forudsætning, at en stjålet identitet bruges til at udføre en strafbar handling, førend der kan være tale om en straffesag. Den nye straffebestemmelse gør det enklere at strafforfølge identitetstyveri, idet det nu er lettere at bevise identitetskrænkelse end et forsøg på fuldbyrdet bedrageri.

I Danmark har der de seneste par år været debat om, hvorvidt identitetstyveri skal være et selvstændigt begreb i straffeloven. Dansk Folkeparti fremsætter den 26. oktober 2011 et forslag til folketingbeslutning om en særskilt straf for identitetstyveri og identitetssvindel (2011/1 BF 3). Forslaget er til første behandling i Folketinget den 17. januar 2012 og henvises til behandling i retsudvalget. Retsudvalget afholder en høring den 8. maj 2012. Det viser sig, at der ikke er politisk flertal for

en særskilt straffebestemmelse for identitetstyveri. Et mindretal i retsudvalget opfordrer efterfølgende regeringen til at foretage initiativer, der sikrer, at myndigheder, virksomheder og privatpersoner står bedst muligt rustet over for identitetstyveri og de kriminelle følger heraf. Desuden opfordrer mindretallet regeringen til i den kommende tid tæt at følge de norske erfaringer og den norske praksis i forhold til en særskilt straffelovsparagraf vedrørende identitetssvindel. Herudfra kan der løbende overvejes, om en indførelse af en sådan særskilt straffelovsparagraf vil tjene et formål i dansk sammenhæng.

2.3 Omfang af identitetstyveri i Danmark

Først når selve misbruget af identitetsoplysninger opdages, er offeret klar over, at vedkommende har været udsat for en kriminel handling. Eksempelvis antages det, at ikke alle opsnappede cpr-numre anvendes efter et databrud. Omfanget af dette mørketal er – i sagens natur – ukendt. Men for at få et indtryk af hvad omfanget af den opdagede del af identitetstyveri er i Danmark, benyttes data fra en offerundersøgelse. Brug af offerdata er ikke problemfrit. For det første er det vigtigt, at respondenten forstår spørgsmålet korrekt. I forlængelse heraf benyttes begrebet identitetstyveri derfor – bevidst – ikke i spørgeskemaet. I stedet er der spurgt til, om respondenten har været udsat for misbrug af personoplysninger eller identitetsbeviser. For det andet er det ikke sikkert, at respondenten husker tidsperioden korrekte. Der er derfor spurgt til, om respondenten har været udsat for dette misbrug inden for de sidste 12 måneder. Men kan respondenten huske, om det er 11 eller 13 måneder siden? Et indblik i omfanget af identitetstyveri på baggrund af en offerundersøgelse skal således betragtes som et estimat.

Som beskrevet i kapitel 1 er offerundersøgelsen gennemført som led i Danmarks Statistiks omnibusundersøgelser. Offerundersøgelsen baserer sig på en stikprøve blandt tilfældige danskere i alderen 16-74 år. Der er stillet spørgsmål omkring identitetstyveri (se bilag 1) til 9.582 respondenter i perioden oktober 2012 til og med juli 2013. Af disse 9.582 respondenter angiver 165 personer, eller 1,7 procent, at de har været udsat for identitetstyveri indenfor de sidste 12 måneder. Det er *inklusiv* personer, hvis betalingskortoplysninger er misbrugt. Som beskrevet i afsnit 3.1 udelukker digitaliseringsstyrelsen misbrug af betalingskortoplysninger fra begrebet identitetstyveri, og derfor er der 94 personer, eller 1,0 procent af respondenterne, som har været udsat for identitetstyveri indenfor de sidste 12 måneder.

Stikprøven er repræsentativ for befolkningen som helhed. Der kan dog være en skævhed i bortfaldet. For at teste om der er tale om en sådan skævhed udarbejder Danmarks Statistik vægte baseret på personoplysninger. Når disse vægte anvendes stiger offerrisikoen for identitetstyveri fra 1,0 procent til 1,1 procent. Ifølge de vægtede data har 46.894 danskere været udsat for identitets-tyveri indenfor de sidste 12 måneder. Det handler i øvrigt ikke nødvendigvis om strafbare forhold (se afsnit 2.2).

Da opgørelsen baseres på en stikprøve, medfører dette en vis statistisk usikkerhed. Hvis stikprøven – som antaget – er a-selektiv, kan et 95 % -sikkerhedsinterval beregnes. Intervallet ligger mellem 0,9 og 1,3 procent, eller, når det ganges op til at gælde hele den danske befolkning, mellem 38.368 og 55.420 danskere. Det skal understreges, at denne offerrisiko omfatter både online og offline identitetstyveri.

Tabel 2.1 Offerrisiko for identitetstyveri i Danmark

	2009 **inkl**. kort	2013 **inkl**. kort	2013 **uden** kort
Omfang stikprøve	1.853	9.582	9.582
Antal udsatte	20	165	94
Andel af udsatte for identitetstyveri	1,1 %	1,7 %	1,0 %
95 % -interval	0,6 – 1,6 %	1,5 – 2,0 %	0,9 – 1,3 %
Antal udsatte i Danmark (estimat)	47.850	70.150	46.900

I offerundersøgelsen spørges der til, hvilke slags identitetsoplysninger, som er stjålet. Der sondres mellem fire slags: navn/cpr-nummer, identitetsbeviser (pas, id-kort, sygesikringskort, kørekort), bankoplysninger (kontonummer, adgangskode) og digitale profiler (e-mail, Facebook mm). Desuden er der en restkategori, som bl.a. inkluderer personer, der har mistet fx kørekort og bankoplysninger. I dette tilfælde er der nemlig tale om en kombination. Tabel 2.2 viser oversigten.

Tabel 2.2 Offerrisiko efter type af misbrugte identitetsoplysninger

	Antal ofre	Procentdel
Navn/cpr-nummer	18	19 %
Identitetsbeviser	3	3 %
Bankoplysninger	28	30 %
Digitale profiler	30	32 %
Kombination	9	10 %
Andet	6	6 %
I alt	**94**	**100 %**

3 Tilegnelse af ID-oplysninger

3.1 Online og offline tilegnelse

Der er mange måder, hvorpå gerningspersonen kan tilegne sig en andens identitetsoplysninger. Offentligt tilgængelige registre, fx telefon- og navneregister, indeholder oplysninger såsom navn, adresse og telefonnummer. Internetsiden krak.dk er et eksempel herpå. Desuden lægger stadigt flere privatpersoner frivilligt personoplysninger ud på egne internetsider eller på sociale netværkssider som Facebook og LinkedIn.

Der kan skelnes mellem online og offline identitetstyveri (fx OECD, 2009). Online identitetstyveri knytter sig til internettet og det faktum, at når en enhed (computer, smartphone, tablet) tilsluttes internet, er det muligt at trænge ind i den og/eller kommunikerer med brugeren. Offline identitetstyveri indebærer, at der er tale om en handling i den fysiske verden. Denne kan dog være af teknisk art, fx skimming. I offerundersøgelsen er de 94 respondenterne, der har været udsat for identitetstyveri, spurgt om de har en idé om, hvordan gerningspersonen har fået fat i deres identitetsoplysninger. Lidt under halvdelen – 45 ud af de 94 respondenter (48 %) – har en idé herom. Mere end 80 procent mener, at det er sket online. Tabel 3.1 viser en oversigt over de metoder, der efter respondenternes egen vurdering, er blevet anvendt til tilegnelse af deres identitetsoplysninger.

Tabel 3.1 Anvendte metoder ved tilegnelse af identitetsoplysninger

	Antal	Procentdel
Offline (stjålet, selv oplyst)	8	18 %
Online	37	72 %
Online metoder		
Malware (spyware)	14	31 %
Internethandel	7	16 %
Lagt selv/fundet på internettet	6	13 %
Falsk e-mail/internetside	10	22 %
I alt	**45**	**100 %**

Note: 49 respondenter har ingen anelse om, hvordan deres identitetsoplysninger er blevet stjålet.

Oversigten viser, at i ca. halvdelen af tilfældene er der tale om phishing: At fiske efter personoplysninger i den digitale verden (kategorierne malware og falsk e-mail/internetside i tabel 3.1). Svarka-

tegorien internethandel knytter sig til, at betalingskortsoplysninger eller andre informationer er stjålet fra en database eller et register. I så fald bryder hackere ind i et computersystem, hvor disse data er gemt. Det kan fx være en internetbutiks kundekartotek.

3.2 Malware

Når en enhed (computer, smartphone, tablet) tilsluttes internettet, kan den kommunikere med omverden. Bagsiden herved er, at enheden kan angribes af andre brugere. Den mest kendte form for angreb er computervira. En computervirus er et lille program, som forsøger at inficere andre programmer. Oftest syner programmet harmløst, og det skal aktiveres manuelt for at kunne indlede spredningen. Virusprogrammer kan være meget skadelige, fx kan de slette vigtige data og/eller programfiler fra den inficerede computer. De fleste brugere har udstyret deres computer med et antivirusprogram. Men som nævnt er computervira langt fra de eneste programmer, hvormed en computer kan inficeres. Listen er lang, og alle disse programmer hører hjem under betegnelse *malware*. Malware er en sammentrækning af de engelske ord *malicious software* (på dansk: ondsindet programkode). Det bruges som en fællesbetegnelse for en række kategorier af computerprogrammer, der gør skadelige eller uønskede ting på de computere, de kører på. Eksempler på malware er:

- *Orme*: En orm kan sprede sig selv fra maskine til maskine uden at aktiveres manuelt. Det foregår ofte ved at udnytte sikkerhedsbrister i operativsystemet eller browseren. En orm medbringer ofte en skadelig payload (last) i form af et eller flere programmer, fx en trojansk hest eller en computervirus.
- *Keyloggere*: En keylogger er et program, der registrerer, hvad der skrives på tastaturet. Det bruges til at spionere og oftest med henblik på at aflure passwords, kontonumre og andre følsomme oplysninger, når brugeren handler eller ordner bankforretninger via internettet. Oplysningerne kan gemmes i en logfil på offerets computer og/eller automatisk sendes til en forudbestemt e-mail-adresse.
- *Trojanske heste*: En trojansk hest er malware forklædt som noget harmløst. Trojaneren er ofte et serverprogram, som gør det muligt at fjernstyre den smittede enhed. Det kaldes derfor også at installere en bagdør. Adgangen kan fx misbruges til at foretage denial-of-service-angreb mod andre systemer på internettet. Fjernstyringsprogrammet Back Orifice(en) er et af de mest kendte programmer til trojanske heste, selvom programmet i sig selv er lavet til legale formål.

I DK•CERT's (Computer Emergency Response Team i Danmark) trendrapport fra 2012 oplyses fordelingen af malware, som identificeres på danskernes computere af antivirusproducenten F-secure. Trojanske heste er klart den største malware-trussel i 2012. I trendrapporten bemærkes følgende i forhold til exploit-malware (Ahmed et al, 2013, s. 7):

Exploits har tidligere udgjort under tre procent af de fundne programmer, men deres andel steg i 2012 til 8,6 procent. Et exploit er et angrebsprogram, der udnytter en sårbarhed til at få kontrol med pc'en. Forklaringen på den stigende mængde exploits kan være, at der er kommet flere såkaldte exploit kits på nettet. Det er serverprogrammer, der afprøver en lang række kendte exploits i forsøget på at inficere de besøgende computere. I årets løb var der stigende opmærksomhed på det problem. Det mest udbredte exploit kit hedder Blackhole. Ifølge sikkerhedsfirmaet Sophos tegnede det sig for 28 procent af de web-baserede trusler, firmaet registrerede fra oktober 2011 til marts 2012.

Tabel 3.2 Procentfordeling af danske malware-infektioner (2012; n=5.536)

Malware	Procentdel
Trojaner	39,9 %
Adware	8,9 %
Exploit	8,6 %
Applikation	8,3 %
Virus	2,6 %
Bagdør	1,7 %
Trojaner downloader	1,0 %
Andet	25,0 %

Kilde: DK•CERTs Trendrappport 2012, s. 7

Andre tendenser, som DK•CERT peger på i trendrapporten fra 2012, er en stigende mængde af afpresningsprogrammer. Det er skadelig software, der tager brugerens data som gidsel. En besked på skærmen fortæller, at alle data er krypteret, og at man skal betale for at få adgang til dem igen. Den mest kendte variant er politi-ransomware. Her får brugeren at vide, at adgangen er spærret af politiet, fordi brugeren er blevet taget i at bruge piratkopier eller børneporno. DK•CERT forventer, at den type malware vil fortsætte med at stige i udbredelse. DK•CERT råder danskere til at investere proaktivt i en backup af deres data i stedet for at betale bagmænd for at åbne op for computeren igen. I trendrapporten forklares effektiviteten af politi-ransomware med en kombination af autoritetstro og frygten for at andre tror, at der er noget om snakken.

En anden tendens, DK•CERT beskriver i trendrapporten fra 2012, er en kraftig stigning i skadelige programmer rettet mod smartphones med Android som styresystem. Grunden til, at det primært er smartphones med Android-styresystem, der er udsat for malware angreb, er muligheden for installation af applikationer uden om Google Play.

3.3 Phishing

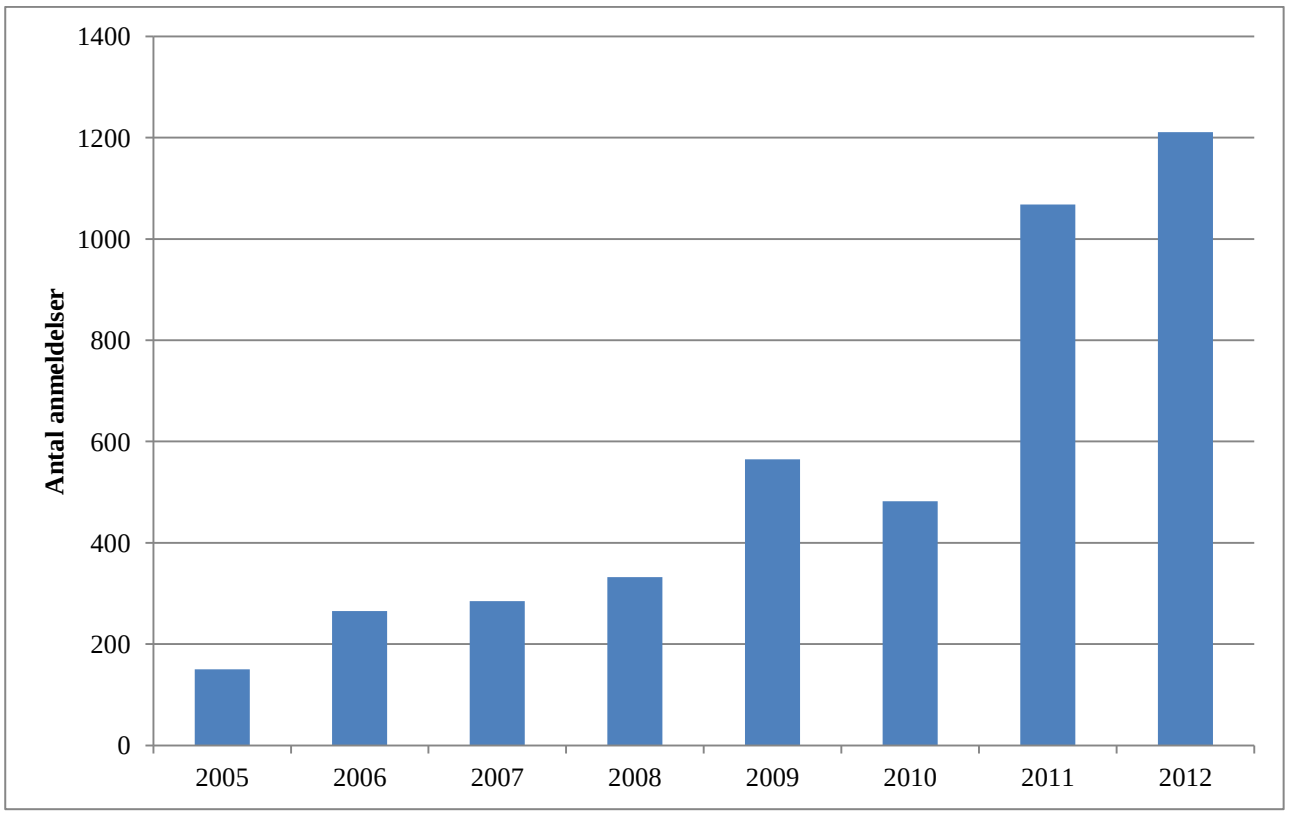
Formålet med phishing er at franarre offeret fortrolige oplysninger, typisk identitets- og finansielle oplysninger. Phishing sker hyppigst ved, at en mail sendes til rigtigt mange adresser. For et par

hundrede dollars kan en mail sendes til en million adresser. I mailen opfordres ofret enten til at taste de ønskede oplysninger ind og sende mailen retur eller til at klikke videre til en phishing side (pharming). Ifølge Sikkerhedsfirmaet Symantec er ca. 0,3 procent af alle mails, sendt til danskere, phishing mails (Ahmed et al, 2013, s. 8).

DK•CERT modtager anmeldelser angående danske internetsider med trojanere og phishing sider, og i 2012 er der 1.211 anmeldelser vedrørende inficerede danske internetsider. Ifølge DK•CERT fiskes specielt efter betalingskortoplysninger og i mindre omfang efter bank- eller skatteoplysninger (Ahmed et al, 2013, s. 9).

Figur 3.1 viser, at antallet af inficerede danske internetsider stiger støt i perioden fra 2005 til 2012. Men samtidig lukker hostingselskaberne og internetudbyderne hurtigere phishing-sider. I DK•CERTs trendrapport fra 2008 oplyses, at danske hostingudbydere er langsomme til at reagere og lukke phishing-sider på deres servere. Den mediane levetid for en phishing side er 16 dage i 2008. I trendrapporten for 2011 oplyses, at levetiden for phishing-sider er faldet til lidt over to dage (54 timer og 37 minutter). "Det er stadig lang tid, men man er øjensynlig blevet hurtigere til at reagere hos hostingselskaberne og internetudbyderne", ifølge DK•CERT (Ahmed et al, 2012, s. 12).

Figur 3.1 Danske internetsider med phishing-sider og malware



Kilde: DK•CERTs Trendrappport, adskillige årgange

3.4 Omfanget af hackerangreb

I Danmarks Statistiks årlige undersøgelse af danskernes IT-vaner og internetadfærd er der først i 2010 spurgt om sikkerhed og sikkerhedsproblemer. Undersøgelsen fra 2010 baserer sig på en stikprøve på 4.588 danskere i alderen 16-89 år, og data er indsamlet i april 2010 (Danmarks Statistik, 2011, s. 56). Undersøgelsen fra 2011 bygger på en stikprøve på 4.988 danskere i alderen 16-89 år, og data er indsamlet i april og maj 2011 (Danmarks Statistik, 2012a, s. 34). Undersøgelsen fra 2012 bygger på en stikprøve på 5.224 danskere i alderen 16-89 år, og data er indsamlet i april og maj 2012 (Danmarks Statistik, 2012b, s. 32).

I Danmarks Statistiks undersøgelser er der spurgt til, om respondenten i de seneste 12 måneder har været udsat for computervirus eller andre skadelige programtyper som fx orme, trojanske heste, bagdøre, adware og spyware, der medfører tab af informationer eller tid. Spørgsmålet dækker dermed begrebet *malware*. For at afklare omfanget af malware er det vigtigt at fastslå, om en computer betragtes som en fælles genstand i husstanden, eller om den betragtes som en personlig ejendel. Med andre ord: Svarer alle personer i en husstand 'ja', hvis (en af) husstandens computere er blevet udsat for et malware angreb med tab af informationer eller tid som følge? Svaret er sikkert forskelligt fra husstand til husstand, men i beregningerne er det antaget, at en computer betragtes som en fælles husstandsgenstand.

Tabel 3.3 viser, at ca. en ud tre danskere med internetadgang i husstanden indenfor det seneste år har været udsat for malware, der har medført tab af informationer eller tab af tid. Når dette procenttal omregnes til antal husstande, ses det, at omkring trekvart mio. husstande i Danmark har været udsat herfor. Danmarks Statistiks undersøgelser viser et markant fald i antal danskere, der har været udsat for malware i 2012 i forhold til 2010 og 2011.

Tabel 3.3 Danskere der har været udsat for malware (seneste 12 måneder)

	2010	2011	2012
Omfang stikprøve	4.588	4.988	5.224
Andel af udsatte internetbrugere i stikprøven	31 %	33 %	18 %
Antal udsatte husstande i Danmark[4]	675.000	765.000	465.000

Kilde: Danmarks Statistik (2011, 2012a, 2012b). Egne beregninger

Datasikkerhed er et vigtigt emne for danske internetbrugere. De ligger ikke kun tekniske forhindringer i forbindelse med at holde hackere og malware væk, også deres internetadfærd påvirkes af bekymringer i forhold til sikkerhed. Omkring en tredjedel af internetbrugerne afholder sig fra at

[4] Der er registreret 2.573.417 husstande i Danmark i 2010. 85 procent har internetadgang, hvilket svarer til 2.187.404 husstande. I 2011 tæller Danmark ifølge Danmarks Statistik 2.584.479 husstande, og 90 procent af disse husstande har internetadgang. Dette svarer til 2.326.031 husstande.

afgive eller indtaste personoplysninger på sociale medier eller professionelle netværkstjenester. Mange danskere har en Facebook konto, men de behøver ikke nødvendigvis at afgive deres rigtige personoplysninger i forbindelse med oprettelsen. Desuden er en betydelig del af internetbrugerne påpasselige med at downloade software, musik, videoer eller spil på internettet. Dette gælder også køb af varer eller ydelser på internettet (hvilket kræver afgivelse af betalingskort-oplysninger). At benytte netbankstjenester (og dermed risikerer netbankindbrud) er internetbrugerne mindre påpasselige med. Tabel 3.4 viser oversigten:

Tabel 3.4 Andel af internetbrugere som holdt sig fra aktiviteter på internet

	2010	2011	2012
Afgive/indtaste personoplysninger til sociale/professionelle tjenester	33 %	34 %	31 %
Downloade software, musik eller videofiler, spil eller andre datafiler	23 %	26 %	20 %
Bestille eller købe produkter eller tjenester til private formål	21 %	26 %	21 %
Bruge netbank	13 %	14 %	10 %
Kommunikere med den offentlige sektor	7 %	7 %	6 %

Kilde: Danmarks Statistik (2011, 2012a, 2012b)

Danske Virksomheder

I 2011 gennemførte det globale konsulentfirma PwC en undersøgelse vedrørende kriminalitet blandt 3.800 virksomheder i 78 lande under navnet *Global Economic Crime Survey*. I Danmark deltager 116 virksomheder, og den danske afdeling af PwC udarbejder en rapport over de danske undersøgelsesresultater. Cybercrime er medtaget – for første gang – som selvstændig type virksomhedskriminalitet i 2011-udgaven af undersøgelsen. Virksomheder rapporterer både globalt set og i Danmark, at cybercrime er den tredje største trussel efter misbrug af aktiver og regnskabsmanipulation (PwC, 2011a, s. 7). Globalt set har 23 procent af virksomhederne været udsat for internetkriminalitet indenfor de seneste 12 måneder. De danske virksomheder ligger tæt på det globale gennemsnitstal, nemlig på 21 procent. I forhold til Vesteuropa og Norden er de danske virksomheder dog mindre udsatte: 25 procent af virksomhederne i både Vesteuropa og Norden har været udsat for internetkriminalitet mod 21 procent i Danmark. Denne forskel kan imidlertid godt skyldes stikprøvens beskedne omfang.

I tilknytning til internetkriminalitet er fire ud af ti danske virksomheder meget bekymrede for spionage (tyveri af deres immaterielle rettigheder) og deres image, hvilket er meget lig tallene for virksomhederne globalt set. Afbrydelse af service, fx som følge af et DDoS-angreb, skrammer både godt en ud af tre danske virksomheder såvel som virksomheder globalt set. Tab af personoplysninger, fx kundekartotek med kreditkortoplysninger, er virksomhederne globalt set mere bekymrede for end de danske virksomheder. Der er således 35 procent af virksomhederne, der globalt set bekymrer sig herfor, og 23 procent i en dansk kontekst. Tabel 3.5 viser oversigten:

Tabel 3.5 Virksomhedernes bekymring[5] for internetkriminalitet (2011)

	Danmark	Globalt
Tyveri af immaterielle rettigheder, herunder tyveri af data	41 %	36 %
Image (reputation)	40 %	40 %
Afbrydelse af service	32 %	34 %
Tyveri eller tab af personoplysninger	23 %	35 %
Direkte økonomisk tab	15 %	31 %

Kilde: PwC, 2011a, s. 10 og PwC, 2011b, s. 12.

Umiddelbart skulle man forvente, at virksomheder frygter, at truslen kommer udefra. Godt halvdelen af de danske respondenter (51 procent) mener også, at truslen kommer fra eksterne gerningspersoner. Mens den anden halvdel er splittet mellem at mene, at truslen kommer fra interne gerningspersoner (9 procent), både ekstern og intern (18 procent), eller de har ingen idé (22 procent) (PwC, 2011a, s. 10). Undersøgelsen fra PwC viser, at 24 procent af de danske virksomheder ikke selv har ressourcer til at forebygge og opdage internetkriminalitet. En betydelig større del af virksomhederne indrømmer (69 procent), at de ikke har kapacitet til at undersøge internetkriminalitet.

Danmarks Statistik har ikke kun undersøgt borgernes, men også virksomhedernes (med 10 eller flere ansatte) erfaringer med IT-sikkerhed. Den seneste rapport om danske virksomheders brug af IT udkommer i 2011, og besvarelserne er indsamlet fra februar til juni 2011 i en spørgeskemabaseret stikprøveundersøgelse blandt 3.905 virksomheder. I denne undersøgelse svarer 7 procent af respondenterne, at virksomheden har været udsat for virus eller uautoriseret adgang. Hacking har for 0,3 procent af de adspurgte virksomheder medført tab af fortrolige data. Når dette ganges op til at gælde samtlige ca. 25.000 virksomheder med 10 eller flere ansatte i Danmark, har ca. 75 virksomheder tabt fortrolige data på grund af hacking-indbrud i 2011.

I Danmarks Statistiks offerundersøgelse fra 2010 fremgår det, at 6 procent af de adspurgte virksomheder (med 10 eller flere ansatte) har oplevet et angreb, fx. et DDoS-angreb. Dette svarer til ca. 1.500 virksomheder, når det ganges op til at gælde samtlige ca. 25.000 virksomheder med 10 eller flere ansatte i Danmark.

Danske myndigheder

Danmarks Statistiks undersøgelse af myndighedernes IT-vaner er spørgeskemabaseret. Skemaet sendes til alle landets kommuner, regioner, departementer, styrelser og statslige uddannelsesinstitutioner. Det svarer i alt til 202 skemaer, og 151 af dem besvares. Undersøgelsen viser, at 15 procent af myndighederne har været udsat for et virusangreb med tab af data eller arbejdstid til

[5] Procentdelen af virksomheder som har svaret 'meget bekymret'.

følge. Det lyder umiddelbart som et højt procenttal, det er derfor vigtigt at være opmærksom på, at et 'ja' står fx for en kommune, det vil sige alle kommunale afdelinger og institutioner. Tabel 3.6 viser oversigten:

Tabel 3.6 Myndighedernes IT-sikkerhedsproblemer (2011)

	Procentdel
Virusangreb med tab af data eller arbejdstid	15 %
Denial of service angreb	9 %
Uautoriseret adgang til systemer og data	9 %
Økonomisk it-misbrug	3 %
Afpresning/trusler mod data eller software	1 %

Kilde: Danmarks Statistik (Lundø, 2012, s. 18)

90 procent af myndighederne har formelt udnævnte it-sikkerhedsansvarlig. Godt tre ud af fire myndigheder har it-sikkerhedsstyring efter DS 484, mens 63 procent har en ajourført it-beredskabsplan. Endelig har 41 procent af myndigheder løbende it-sikkerhedsuddannnelse af medarbejdere.

3.5 Gerningsmandsprofil af hackere

Betegnelsen hacker er oprindelig et positivt begreb, som henviser til computerentusiaster omkring Massachusetts Institute of Technology (MIT) i 1960'erne (Furnell, 2010). Hackere er i stand til at finde elegante, kreative og effektive løsninger på tekniske problemer (Yar, 2006). Deres etik bygger på idéen om fri adgang til information og viden (Levy, 1984), og de skaffer sig adgang til computere via nysgerrighed (Yar, 2006).

Nu til dags har betegnelsen hacker en anden lyd. Hackere referer til personer, som skaffer sig uberettiget adgang til computere og informationssystemer. I Danmark er hacking kriminaliseret i straffelovens § 263, stk. 2: "Den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem, straffes med bøde eller fængsel i indtil 1 år og 6 måneder".

Der findes forskellige typologier over hackere (Europol, 2003; Rogers, 2006; McAfee, 2006). Fælles for disse er, at de sondrer mellem hackere med gode intentioner (som fx at afsløre sikkerhedshuller i systemer) og kriminelle motiver (hærværk, økonomisk gevinst mv.). Traditionelt skelnes der mellem såkaldte *white hats* (hvide hatte) og *black hats* (sorte hatte). I modsætning til *black hats* arbejder *white hats* ofte for virksomheder, de har til opgave at beskytte deres IT-systemer. Det er dog

ikke usædvanligt, at en *white hat* hacker har startet sin løbebane og udviklet sine kompetencer på den anden side af loven.[6]

En skelnen mellem kun to kategorier af hackere viser ikke diversiteten. Sort-hvid er altså en for strikt opdeling, der arbejdes derfor ofte med en kategori imellem. Denne kaldes *grey hats* (grå hatte). Et eksempel på en hacker, der kan betegnes som grå hat, er den medieomtalte Søren Louv-Jansen. Han oprettede en hjemmeside ved navn 'cpr-lotteriet', hvor flere danske politikers cpr-numre blev udstillet. Cpr-numrene havde han skaffet ved at lave et computerprogram, der testede de 270 mulige firecifrede endelser, som er tilknyttet enhver fødselsdato. Formålet med aktionen var at sætte fokus på sikkerhedsbristen ved cpr-systemet, men det forhindrer ikke, at han sigtes for overtrædelse af persondataloven (Weekendavisen, 2. august 2013).

Opdelingen i white, grey og black hats baserer sig på hackernes formål og (il)legalitet. Desuden er der indenfor kategorien *black hats* forskellige typer af hackere, de differentieres ud fra deres færdigheder og organisering. Bl.a. betegnes hackere, der anvender købte færdigudviklede hacker-produkter på nettet, som *script kiddies*. Det kræver altså for tiden ikke særlige hackerkvaliteter at bryde ind i systemer, men der eksisterer også hackere på den anden side af spektret: Cyber kriminelle som bedriver organiseret kriminalitet. Ifølge Europol (2013) begår de kriminelle grupperinger primært bedrageri og finansielle forbrydelser, og de rekrutterer blandt unge akademier med IT-kundskaber (Europol, 2011).

Politikens journalist Mads Zacho Teglskov tegner i en artikel fra den 19. juni 2011 et billede af den globale hackerverden med forskellige led. Det første led er en lille gruppe af højtuddannede og talentfulde hackere, der udvikler gør-det-selv-værktøjer til dem, som vil udføre et hackerangreb (*script kiddies*). Disse værktøjer havner hos netbrugere med hackerintentioner via et mellemled, der tilbyder computervira, orme eller trojanske heste på en internetside. Teglskov beretter om ca. 500 mellemmænd på verdensplan, men det er uklart, hvilken kilde han henviser til i denne sammenhæng.

Den sidste type af hackere beskrevet i litteraturen har en aktivistisk hensigt. De er politisk eller religiøst motiverede og betegnes ofte som hacktivister. I Danmark er Anonymous-bevægelsen det mest kendte eksempel på hacktivisme. Anonymous opstår i 2003 og bliver kendt i 2008 på grund af deres aktion mod Scientology. Årsagen er, at den religiøse bevægelse forsøger at undgå, at en vi-

[6] I artiklen 'Den etiske hacker' (Weekendavisen, 2. august 2013) nævnes Dave Dittrich, forsker ved University of Washington. I 2009 afslører han på en konference, at han ti år forinden bryder loven, da han griber til selvtægt og på ulovlig vis skaffer sig adgang til systemer for at advare folk om, at de er inficeret af skadelig software.

deo med skuespilleren Tom Cruise florerer på nettet. Mads Munck Petersson argumenter i en kronik i Information (4. september 2012) for, at hacktivisme er den nye generationers fortolkning af, hvordan man kan udøve aktivt medborgerskab. Han skriver:

> Den type angreb kan altså opfattes som en sit down-protest, hvor man blokerer adgangen til et givent sted, som fx da studerende på KU blokerede rektors kontor tilbage i 1968. Og ligesom sit down-protester ikke er indbrud, er Anonymous' typiske angreb heller ikke hacking.

Ud fra ovenstående beskrivelse af forskellige typer af hackere kan det konkluderes, at alle hackere – bortset fra *white hats* – overtræder den danske hacker paragraf i straffeloven. Der er imidlertid store forskelle i formålet med at begå deres hacker (u)gerning. Det kan – efter eget udsagn – være en nobel intention (fx i forbindelse med en advarsel mod sikkerhedsproblemer) eller et udtryk for et aktivistisk synspunkt. Men det kan også være hærværk eller en måde at tjene penge på. Tabel 3.7 giver oversigten.

Tabel 3.7 Oversigt over forskellige typer af hackere

Formål	Legalt	Illegalt
IT-sikkerhed	White hats	Grey hats
Aktivisme		Hacktivists
Hærværk		Script kiddies
Penge		Black hats

Sigtede hackere i Danmark

I perioden 2010-2012 er der sigtet 75 unikke personer i Danmark for hacking. Den gængse fordom om, at hackere er mænd, bekræftes af de danske data fra denne periode. 72 af de 75 sigtede hackere er nemlig mænd. Den anden sædvanlige forestilling om, at hackere er unge, stemmer ikke overens med de danske data. Aldersfordelingen er vist i tabel 2.6. De fleste sigtede hackere er 15-24 år, men ca. halvdelen er over 25 år gamle. Blandt de 15-24-årige er halvdelen af de sigtede (17 personer) mindreårige, mens den anden halvdel er i alderen 18-24 år. De tre kvindelige hackere er alle 45-54 år.

Tabel 3.8 Aldersfordelingen blandt sigtede hackere i Danmark (2010-2012)

	Antal	Procentdel
14 år eller yngre	3	4 %
15-24 år	34	45 %
25-34 år	12	16 %
35-44 år	16	21 %
45-54 år	8	11 %
55-64 år	2	3 %
I alt	**75**	**100 %**

Langt de fleste hackere sigtet i Danmark er af dansk nationalitet, nemlig 69 ud af de 75 sigtede (92 procent). De seks sigtede af udenlandsk nationalitet stammer fra Afghanistan, Aserbajdsjan, Bosnien, Irak (2) og Syrien. De er ikke *hard core* hackere fra udlandet, som oftest omtalt i pressen. Men de er drenge, der bor i Danmark, og deres hackeraktiviteter falder for det meste ind i kategorien drengestreger. De to sigtede med irakisk nationalitet er begge 15-årige drenge. Den ene har slettet sin 16-årige ekskærestes mails og Facebook-beskeder, mens den anden har logget sig på skolens intranet via en kammerats kode. Den sigtede med syrisk nationalitet er under den kriminelle lavalder (11 år) og har hacket sig ind på et spil for børn på nettet. Den sigtede med afghansk nationalitet er 16 år og har hacket og videresolgt brugerdata fra et onlinespil, mens den sigtede med aserbajdsjansk nationalitet har ændret sin årskarakter i dansk ved at logge ind i systemet med lærens password. Til sidst har den 17-årige sigtede dreng med bosnisk nationalitet overtaget styring af en 15-årig piges computer.

Datafilen med oplysninger om de 75 sigtede hackere indeholder en kort beskrivelse af sagerne. Ud fra disse sagsresuméer kan det læses, at de fleste hackingsager kendetegnes ved, at forurettede og sigtede kender hinanden (ekskærester, skolekammerater, tidligere ansatte mv.). Dette billede stemmer overens med en analyse af 159 hackingsager fra Holland (Leukfeldt et al, 2010). Her finder forskerne også, at i mange af sagerne kender forurettede og sigtede hinanden. Desuden er hævn og nysgerrighed den drivende kraft i disse sager.

Tabel 3.9 Hackerens forhold til forurettede i Danmark (2010-2012)

	Antal	Procentdel
Kender hinanden	46	70 %
Skolerelateret	*10*	
(Eks)ansatte	*9*	
Ekskærester	*7*	
Kender ikke hinanden	20	30 %
I alt	**66**	**100 %**

I 9 sager mangler oplysninger, der kan klargøre sigtede og forurettedes forhold til hinanden

Gennemgangen af sagsresuméerne viser, at sigtede og forurettede i 70 procent af tilfældene kender hinanden. Det oplyses ikke i alle resuméer, hvordan relationen er. Men der tegner sig et billede af, at de fleste kender hinanden enten fra uddannelsesstedet eller arbejdspladsen, ellers har de været kærester. Jeg antager, at der er en klar overrepræsentation af sager, hvor sigtede og forurettede kender hinanden i forhold til alle hackingsager (som for de meste ikke fører til en politianmeldelse). Det er naturligvis nemmere for politiet at opklare sagen, når anmelderen mere eller mindre kan udpege gerningspersonen. Herunder står et par typiske eksempler på hackersager, hvor sigtede og forurettede kender hinanden:

Bekendte (uden nærmere beskrivelse): Hacking af forurettedes computer for at skaffe adgang til hendes forskellige mailforbindelser. Under tilkobling er der foretaget ændringer i tekst på mindst én mailkonto (38-årig mand fra Falster).

Skolerelateret: De to sigtede benyttede klassekammerats kode til at logge på hans profil på skolens elevintra. Herefter blev der sendt smædebeskeder til klasselæreren – ingen trusler. Drengene meldte sig selv, men blev alligevel bortvist fra skolen (to 15-årige drenge fra Nordvestsjælland).

Tidligere ansatte: Sigtede har uretmæssig logget på firmaets administrationssystem efter vikarperiode i bogholderiet hos anmelderen ved brug af kollegas lånte kode (47-årig mand fra Sydvestsjælland).

Ekskæreste: Sigtede har hacket sig ind på ekskærestes Jubii mail og videre derfra til hendes Facebook profil, hvor han kunne læse indholdet og ændrede koder i systemerne (33-årig mand fra Fyn).

I de 20 sager hvor sigtede tilsyneladende ikke har en relation til den forurettede part, kan der i to tilfælde spores en form for hacktivisme. I det ene tilfælde hackes Dansk Folkepartis hjemmeside af en 15-årig dreng, og han mistænkes desuden for aktiv deltagelse i et DDoS-angreb mod PayPals hjemmeside. Afgørelserne i forbindelse med sigtelserne for disse to forhold viser imidlertid, at sigtelserne opgives som grundløse (§ 721, stk. 1, nr. 1). I det andet tilfælde, hvor der kan spores en form for hacktivisme, hackes socialdemokraternes hjemmeside af en 36-årig mand fra Københavns Vestegn. Han findes skyldig og får en betinget dom.

De resterende 18 sigtede hackere mistænkes først og fremmest for at skaffe sig adgang til virksomheders hjemmesider, hvor de forsøger at stjæle kundeoplysninger, eller at komme ind i virksomhedernes fakturasystemer. Der er et par sager, hvor *gaming sites* er målet. Her ændres i spilleforholdene eller – som i en sag – slettes en ban liste. Der beskrives også en hackingsag, hvor tilegnelsen af kundeoplysninger fører til pengeafpresning af indehaveren.

Kriminel løbebane

Blandt de 75, som sigtes for hacking i perioden 2010-2012, sigtes 30 også for en eller flere lovovertrædelser i perioden 2001-2009. Det svarer til en recidivprocent på 40. Halvdelen af recidivisterne sigtes en eller to gange i perioden fra 2001-2009, mens den anden halvdel sigtes tre eller flere gange.

Tabel 3.10 Antal sigtelser for lovovertrædelser i perioden 2001-2009

	Antal personer	Også ligeartet
Ingen sigtelser	45	
1 sigtelse	9	1
2 sigtelser	6	1
3-10 sigtelser	6	1
Mere end 10 sigtelser	9	6
I alt	**75**	**9**

9 ud af de 30 recidivister har begået ligeartet kriminalitet i perioden 2001-2009 (se også afsnit 1.4.5), og 6 af disse falder i kategorien 'meget kriminel aktiv' (mere end 10 sigtelser). De er således mere hårdkogte kriminelle. Bl.a. registreres en 19-årig mand for 24 sigtelser i perioden 2001-2009, og en af disse er for ligeartet kriminalitet. I 2010-2012 sigtes han for hacking (af kundeoplysninger) og efterfølgende (forsøg på) afpresning. Sigtelsen opgives dog grundet manglende beviser. Et andet eksempel omhandler en 32-årig fra København, som sigtes for 87 forhold i 2012. De drejer sig alle om uberettet adgang til Hotmail-konti. Vedkommende registreres desuden for 8 sigtelser i 2001-2009, hvoraf 3 er for ligeartet kriminalitet.

Tabel 3.11 Sammenhæng mellem recidiv og alder

	Antal sigtede	Antal recidivister	Andel recidivister
14 år eller yngre	3	-	-
15-24 år	34	8	24 %
25-34 år	12	10	83 %
35-44 år	16	10	63 %
45-54 år	8	2	25 %
55-64 år	2	-	-
I alt	**75**	**30**	**40 %**

Ud fra data ses det, at der er en sammenhæng mellem recidiv og alder. Naturligvis sigtes de yngre mindre hyppigt i perioden 2001-2009. Men det er bemærkelsesværdigt, at de 25-44 årige er så markant overrepræsenteret blandt recidivisterne.

4 Misbrug af ID-oplysninger

4.1 Hensigt med misbrug

Identitetsoplysninger kan misbruges på mange forskellige måder. Meulen (2006) skelner mellem økonomisk og kriminelt misbrug. Meulen nævner desuden en tredje form for misbrug, nemlig identitetskloning. I et sådan tilfælde overtager gerningspersonen en anden persons identitet totalt, som det skete for Angela Bennett (Sandra Bulllock) i filmen *The Net* (1995). Selvom det ikke kan udelukkes, at identitetskloning finder sted, må det regnes for et yderst sjældent fænomen.[7] Der findes imidlertid – flere og flere – eksempler på identitetsmisbrug, som ikke sigter efter økonomisk gevinst eller kriminelt misbrug. I stedet kan det betragtes som socialt misbrug: Identitetsoplysninger misbruges med henblik på at opnå adgang til udsattes digitale profil eller til at sende beskeder ud i udsattes navn.

Offerundersøgelsen viser, at hensigten med identitetstyveri i godt halvdelen af tilfældene er at opnå økonomisk gevinst. Hyppigst overføres penge fra ofrets konto ved hjælp af kontooplysninger, men oplysningerne anvendes også til blandt andet køb af varer og ydelser, for det meste online.

Meulen (2006) beskriver to basisformer for økonomisk misbrug af identitetsoplysninger. Den første form er kendt som *account take over*, hvor gerningspersonen misbruger en eksisterende bankkonto. Den anden form for økonomisk misbrug kaldes *true name fraud*. Denne henviser til situationer, hvor gerningspersonen misbruger identitetsoplysninger til at oprette lån, bestille kreditkort eller erhverve formue på bekostning af ofret på anden vis. Offerundersøgelsen giver ikke mulighed for at skelne mellem disse to former for misbrug.

I forbindelse med økonomisk misbrug af identitetsoplysninger er et relevant spørgsmålet, hvordan gerningspersonen tilegner sig penge, varer og/eller ydelser i en andens navn uden at blive sporet med det samme. Til dette formål kan bruges et såkaldt muldyr: En person der bevidst eller ubevidst hjælper gerningspersonen med at transportere penge og/eller varer ud af landet. Typisk overføres stjålne penge til muldyrets konto, hvorefter pengene hæves i kontanter og sendes ud af landet.

[7] I England har enkelte privatpersoner 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. Dette kaldes *pseudocide* (afledt af suicide), skrev Nyheds-avisen i oktober 2006 (Stove & Valeur, 2007, s. 37).

Muldyret rekrutteres oftest igennem spammail, som sendes ud til mange tusinde modtagere på samme tid. I mailen lokkes med lette penge og et hurtigt udbytte.

Ved kriminelt misbrug af identitetsoplysninger anvender gerningspersonen ofrets identitet, når vedkommende anholdes af politiet for en forbrydelse. Formålet med identitetsmisbrug er i dette tilfælde at undgå strafforfølgelse. Meulen (2006) påpeger, 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. Blandt andet anholdes en uskyldig mand for besiddelse af børnepornografi, da hans kreditkortoplysninger er blevet brugt til at skaffe adgang til en internetside med børnepornografi. Et andet af Klerks eksempler stammer fra ombudsmanden. En hollandsk mands identitet misbruges af narko-forbrydere, han har således uretmæssigt 43 forbrydelser knyttet til sit navn, hvorfor han har problemer med at rejse, har været anholdt flere gange og har været udsat for ransagning af sin bolig. Ombudsmanden er overrasket over, hvor svært det er at rette op på følgerne af dette misbrug, selvom ofret har fået hjælp af myndighederne. I offerundersøgelsen oplyser to respondenter, at deres identitetsoplysninger er misbrugt i forbindelse med at vildlede myndighederne.

Tabel 4.1 Hensigt med misbrug af identitetsoplysninger

	Antal	Procentdel
Økonomisk misbrug		
Købe online	14	15 %
Købe offline	3	3 %
Leje noget/afslutte abonnement	3	3 %
Hæve/overføre penge	27	29 %
Uspecificeret økonomiske misbrug	3	3 %
I alt økonomisk misbrug	*50*	*53 %*
Kriminelt misbrug	2	2 %
Socialt misbrug	30	32 %
Uoplyst formål	12	13 %
I alt	**94**	**100 %**

Omfanget af socialt misbrug er mindre end økonomisk misbrug, men fænomenet er formentlig i vækst. 32 procent af respondenterne rapporterer, at deres identitetsoplysninger er blevet misbrugt til at publicere noget på internettet, sende e-mails ud eller misbrug profiloplysninger på anden vis. Misbrug af en Facebook profil er i pressen døbt *Facerape*. Politiken[8] beretter om en sag, hvor to teenagedrenge dømmes ved retten i Helsingør til bøder på henholdsvis 2.000 og 4.000 kr. for at

[8] Drenge får bøde for at ændre i piges Facebookprofil, Politiken, 20. februar 2013.

logge ind på en jævnaldrende piges Facebook konto og ændre hendes profil. Drengene sigtes for overtrædelse af brevhemmeligheden, blufærdighedskrænkelse og at viderebringe meddelelser om andres forhold.

Ikke alt socialt misbrug er strafbart. Suzanne Bjerrehuus oplever misbrug af sine personoplysninger, da en person opretter en profil i hendes navn på Facebook med billeder af hende. Hun politianmelder sagen men får besked på, at det ikke er strafbart at oprette falske profiler på Facebook. Bjerrehuus er ikke den eneste kendte dansker, der oplever misbrug af personlige oplysninger. Chefredaktøren på Berlingske Tidende, Lisbeth Knutsen, oplever i maj 2007, at der sendes en stribe mails til personer i hendes adressekartotek blandt andet med ordlyden: "Jeg vil gerne frabede mig alle jeres sleske e-mails." Knutsens computer er genstand for en hacker, som har overtaget hendes mail-identitet (Stove & Valeur, 2007, s. 37).

4.2 Netbankindbrud

En måde hvorpå bankoplysninger kan misbruges er ved indbrud i en netbank. Bankerne offentliggør oplysninger herom. Anvendelse af internetbanker er steget støt de seneste år, og i 2012 anvender 79 procent af den danske befolkning mellem 16 og 74 år en netbank (Danmarks Statistik, 2012b). I Danmarks Statistiks undersøgelse af danskernes it-anvendelse i 2012 fremgår det, at risikoen for netbankindbrud afholder 10 procent af internetbrugerne fra at benytte denne internetaktivitet. Blandt danskerne har 92 procent internetadgang og 79 procent anvender netbank. Der er således 13 procent af de danske internetbrugere, der ikke har netbankadgang. Dette tal er stort set lig med de 10 procent, der angiver, at risikoen for indbrud afholder dem fra at anvende netbank. Bekymringen for misbrug er således den væsentligste grund til at fravælge netbank.

Det første netbankindbrud i Danmark finder sted i 3. kvartal 2006. Når der sker et indbrud melder banken det til Finansrådet, som kvartalsvis offentliggør enkelte statistiske oplysninger omkring netbankindbrud. I forbindelse hermed offentliggøres tre tal:

- *Netbankindbrud*: Samtlige antal forsøg på netbankindbrud, både de der lykkes og ikke lykkes. Forsøg der ikke lykkes, skal forstås som, at gerningspersonen skaffer sig adgang til en kundes netbank, men det lykkes ikke at overføre penge. Forsøg hvor 'døren står åben' og gerningspersonen ikke er til stede til at gennemføre *real time phishing*, tælles ikke med. Dog tilkendegiver interviewrespondenten fra Finansrådet, at det sker en del for tiden (dvs. i efteråret 2012).
- *Netbankindbrud med tab*: Samtlige antal netbankindbrud, hvor det lykkes for gerningspersonen at slippe af sted med penge.
- *Tabets omfang:* Beløbet som gerningspersonen slipper af sted med. Dette korrigeres, såfremt nogle af pengene kommer retur. Banken dækker tabet for privatkunder, mens er-

hvervskunder selv hæfter for tabet.[9] Erhvervskunder kan tegne en forsikring for netbankindbrud – separat eller som en del af en kriminalitetsforsikring – ved deres forsikringsselskab.

Tabel 4.2 viser, at antallet af netbankindbrud stiger fra 2006 til 2008. I 2009 vender kurven og falder drastisk i 2010 og 2011. Men i 2012 tager antallet af netbankindbrud til igen. Hvordan denne tendens kan tolkes, vendes der tilbage til (se kapitel 7). Samme tendens viser sig også ved indbrud med tab. Men det lykkes oftere for bankerne at begrænse procentdelen af netbankindbrud med tab i 2012 end i årene 2008 og 2009. Der vendes også tilbage til en mulig forklaring herpå i kapitel 6. Tabets omfang ligger på knap 7 mio. kr. i henholdsvis 2008 og 2009, mens tabet er under 1 mio. kr. i hvert af årene 2010 og 2011. I 2012 stiger tabet igen til godt 6 mio. kr. Over årene svinger det gennemsnitlige tab pr. indbrud, hvor det lykkes for gerningspersonen at opnå et udbytte.[10]

Tabel 4.2 Netbankindbrud i Danmark (2006-2012)

	Antal netbank-indbrud	Antal netbank-indbrud m. tab	Procentdel af indbrud m. tab	Tabets omfang (mio. kr.)	Gennemsnitligt tab pr. indbrud
2006	84	27	32 %	1.9	72.169
2007	187	81	43 %	0,3	3.760
2008	251	132	53 %	6,5	49.541
2009	111	63	57 %	6,8	107.781
2010	12	6	50 %	0,4	72.174
2011	10	4	40 %	0,2	39.917
2012	199	55	28 %	6,3	114.359

Kilde: Finansrådet, egne beregninger

4.3 Tab på grund af identitetsmisbrug

Ved økonomisk misbrug af identitetsoplysninger kan der opstå et tab. Men det sker ikke nødvendigvis: Banken stopper i visse tilfælde betalingen, og så er der intet økonomisk tab (se også kapitel 6). I offerundersøgelsen angiver 36 ud af de 50 respondenter, som har været udsat for økonomisk misbrug, at der var tale om et tab. Tabel 4.3 viser oversigten. Det gennemsnitlige tab (blandt de 36 respondenter, der rapporterer om tab) er 8.642 kr. Gennemsnittet trækkes op på grund af enkelte større beløb (2x 30.000; 70.000). Derfor ligger medianen på et lavere beløb, nemlig 3.280 kr. I alt er der samlet set tale om et tab på 311.127 kr. for de 36 respondenter.

[9] Medmindre privatkunderne har været groft uagtsomme i deres adfærd. Alle udsatte privatkunder har ubeskåret fået erstattet deres tab ifølge vores interviewrespondent fra Finansrådet. Bankerne vil ikke oplyse, hvordan fordelingen mellem privat- og erhvervskunder ser ud.

[10] Det gennemsnitlige udbytte kan påvirkes kraftigt af indbrud med store tab. Bankerne oplyser imidlertid ikke tabet pr. indbrud, så det er ikke muligt at beregne medianen eller at korrigere for ekstreme beløb.

Tabel 4.3 Tabets omfang på grund af økonomisk misbrug ved hjælp af identitetsoplysninger

	Antal	Procentdel
Intet tab	14	28 %
<= 1.000 kr.	10	20 %
1.001 – 5.000 kr.	12	24 %
5.001 – 10.000 kr.	6	12 %
>= 10.001 kr.	8	16 %
I alt	**50**	**100 %**

I de fleste tilfælde hæfter ofrene ikke for tab, der knytter sig til økonomisk misbrug som følge af identitetstyveri. 11 ud af de 36 respondenter med tab svarer, at de selv har betalt (en del af) tabet. Det er imidlertid en meget beskeden del af tabet. I alt har udsatte for identitetstyveri selv betalt 15.050 kr. Det svarer til 5 procent af det samlede tab.

4.4 Offerprofil i forbindelse med identitetsmisbrug

Offerundersøgelsen viser, at risikoen for at blive udsat for identitetsmisbrug falder med alderen. Når denne observation kombineres med de udsattes køn, viser det sig, at unge mænd (under 30 år) har større risiko for at blive udsat for identitetsmisbrug. Denne offerprofil kan formentlig forklares med unge mænds adfærd på internettet. Hypotesen testes dog ikke i undersøgelsen.

Tabel 4.4 Offerrisiko for identitetsmisbrug efter køn og alder

	Mand	Kvinde	I alt
Under 30 år	1,9 %	1,3 %	1,6 %
30 – 49 år	1,3 %	1,0 %	1,1 %
50 år og ældre	0,7 %	0,5 %	0,6 %
I alt	**1,2 %**	**0,8 %**	**1,0 %**

Note: Antal ofre er 94, og stikprøven omfatter 9.582 respondenter.

Offerrisikoen er mere eller mindre uafhængig af uddannelsesniveau, og de små forskelle i forbindelse hermed forsvinder, når der samtidig korrigeres for køn. Der er en sammenhæng mellem erhverv og offerrisiko, hvilket tabel 4.5 viser. De to grupper med afvigende offerrisici – de studerendes og pensionisternes – knytter sig formentlige til aldersvariablen.

Tabel 4.5 Offerrisiko for identitetsmisbrug efter erhverv

	Antal ofre	Antal resp.	Offerrisiko
Med arbejde	61	5.461	1,1 %
Uden arbejde	9	898	1,0 %
Studerende	20	1.286	1,6 %
Pensionister	4	1.928	0,2 %
I alt	**94**	**9.573**	**1,0 %**

Note: Uden erhverv omfatter også førtidspensionister, mens efterlønsmodtagere hører til kategorien pensionister.

4.5 Gerningsmandsprofil af identitetstyve

I forbindelse med misbrug af identitetsoplysninger kan gerningspersonen (1) overfører penge fra forurettedes netbank, eller (2) enten prøve eller lykkes med at optage (forbrugs)lån over internettet ved hjælp af forurettedes identitetsoplysninger. Identitetsoplysningerne kan gerningspersonen enten få fat i via indbrud (hacking), phishing eller på anden vis (fx social engineering). Når oplysninger misbruges i forhold til mail, Facebook mm, registrerer politiet sagen som hacking. Gerningsmandsprofilen af hackere beskrives i afsnit 3.5.

Ud fra sagsresuméerne i den datafil, som Rigspolitiet har stillet til rådighed for denne undersøgelse, er det ikke muligt at danne sig overblik over, hvordan de, der er sigtede for at overføre penge fra forurettedes netbank, har opnået adgang til netbankkoderne. Der er fx en sag, hvor en 58-årig kvinde fra Greve er sigtet for netbankoverførsler til hendes konto. I alt er der overført 570.000 kr., og i sagsresuméet står der, at en ukendt gerningsperson har overført pengene til hendes bankkonto. Jeg formoder, at hun har fungeret som muldyr. Denne formodning styrkes af strafudmåling, som lyder på en betinget dom. I en anden sag har en 32-årig mand fra Nordjylland af to omgange i alt overført 428.000 kr. fra en 32-årig kvindes konto til sin egen. I sagsresuméet står, at han i et af tilfældene har overført pengene til en budgetkonto først. Dette kan tyde på, at sigtede og forurettede kender hinanden. Strafudmålingen (delvis betinget dom) giver yderligere anledning til at tro, at der er formildnende omstændigheder.

Af sagsresuméerne fremgår det, at i nogle af sagerne, hvor personerne er sigtede for at oprette lån med forurettedes oplysninger over internettet, er lånet udbetalt ved fremvisning af kørekort (hvor sigtede har indsat sit eget billede) og/eller sygesikringsbevis. I forbindelse hermed er der formentlig tale om organiseret kriminalitet. Politiet henviser nemlig til en pas/kørekortbande i sagsresuméerne. Desuden er der i flere af sagerne en del sigtede i flere forskellige politikredser, hvilket indikerer, at de efterforskes på nationalt plan.

I perioden 2010-2012 er der sigtet 59 unikke personer i Danmark for misbrug af identitetsoplysninger. Blandt de sigtede er kønsfordelingen skæv, eftersom kun 11 ud af de 59 (19 procent) er kvinder. Andelen af sigtede kvinder er således lidt større sammenlignet med hacking og skimming (jf.

afsnit 3.5 og 5.3). Godt tre ud af fire sigtede har dansk statsborgerskab, og blandt de 13 sigtede med udenlandsk nationalitet kommer størstedelen fra europæiske lande (det gør 10 ud af de 13). De tre øvrige sigtede kommer fra afrikanske lande. Den yngste person sigtet for misbrug af identitetsoplysninger er 16 år, og den ældste er 68 år. Det er imidlertid ikke mange af de sigtede, der er ældre end 45 år.

Tabel 4.6 Aldersfordeling blandt sigtede id-misbrugere i Danmark (2010-2012)

	Antal	Procentdel
15-24 år	23	39 %
25-34 år	18	31 %
35-44 år	14	24 %
45-68 år	4	7 %
I alt	**59**	**100 %**

Kriminel løbebane

Blandt de 59, som sigtes for identitetstyveri i perioden 2010-2012, er 36 også sigtede for en eller flere lovovertrædelser i perioden 2001-2009. Det svarer til en recidivprocent på 61. 30 procent af recidivisterne sigtes en eller to gange i 2001-2009, mens 70 procent af recidivisterne tegner sig for tre eller flere sigtelser.

Tabel 4.7 Antal sigtelser for lovovertrædelser i perioden 2001-2009

	Antal personer	Også ligeartet
Ingen sigtelser	23	
1 sigtelse	8	2
2 sigtelser	3	1
3-10 sigtelser	14	5
Mere end 10 sigtelser	11	8
I alt	**59**	**16**

16 ud af de 36 personer, der betegnes som recidivister, begår ligeartet kriminalitet i perioden 2001-2009 (se også afsnit 1.4.5). Halvdelen af dem falder i kategorien 'meget kriminel aktiv', hvilket svarer til mere end 10 sigtelser. Et eksempel herpå er en 31-årig mand fra Nordsjælland, der registreres for 113 sigtelser i perioden 2001-2009. 16 af disse er for ligeartet kriminalitet. I perioden 2010-2012 sigtes han for misbrug af identitetsoplysninger (cpr-nummer og identitetsbeviser), idet han med disse har optaget adskillige lån over internettet. Et andet eksempel er en 24-årig kvinde, der i 2010-2012 sigtes for at oprette internet- og mobiltelefonabonnementer i en anden persons navn. Hun sigtes desuden i perioden 2001-2009 26 gange, og to af disse sigtelser handler om ligeartet kriminalitet.

Ud fra data ses det, at der er en sammenhæng mellem recidiv og alder. Umiddelbart skulle man forvente, at de yngre mindre hyppigt sigtes i perioden 2001-2009. Men det viser sig, at to tredjedele af de sigtede i alderen 15-34 år er recidivister, mens det kun er halvdelen af de sigtede over 35 år.

Tabel 4.8 Recidiv og alder

	Antal sigtede	Antal recidivister	Andel recidivister
15-24 år	23	15	65 %
25-34 år	18	12	67 %
35-44 år	14	7	50 %
45-68 år	4	2	50 %
I alt	**59**	**36**	**61 %**

5 Misbrug af betalingskort

5.1 Markedet for betalingskort

Når en forbruger benytter sit betalingskort til at betale for en vare eller ydelse, igangsættes et samspil mellem en række aktører for at betalingen kan gennemføres. De fem centrale aktører er (Konkurrence- og Forbrugerstyrelsen, 2012, s. 8):

- Kortselskab
- Kortudsteder (bank)
- Kortindløser
- Betalingsmodtager (forretning)
- Kortbruger (forbruger)

Traditionelt har betalingskortmarkedet i Danmark været domineret af Dankort. I forbindelse med en kortbetaling med Dankort fungerer Nets (det tidligere PBS) både som kortselskab og kortindløser, hvorfor der ikke er fem men fire centrale aktører indblandet.[11] Der findes en række forskellige typer af betalingskort. Konkurrence- og Forbrugerstyrelsen skelner mellem hævekort, debetkort, kreditkort, forudbetalte betalingskort og internationale betalingskort. Disse kort defineres på følgende vis (Konkurrence- og Forbrugerstyrelsen, 2012, s. 10):

> *Hævekort* kan alene benyttes til at hæve kontanter eller til at overføre penge. Udbredelsen af hævekort, som udstedes af bankerne, er relativt begrænset, da hævekort ikke kan bruges til at betale for varer og tjenesteydelser. En række banker tilbyder dog hævekort til børn og unge, der er mellem 12-17 år.
>
> *Debetkort* er et betalingskort, hvor købsbeløbet trækkes fra forbrugerens konto med det samme eller senest næste bankdag. Derfor er det ofte banker, som udsteder debetkort, da det er nødvendigt at have direkte adgang til kortbrugerens konto for at kunne trække købsbeløbet med det samme. Dankort er et eksempel på et debetkort. Flere banker tilbyder

[11] Nets-koncernen er et resultat af, at PBS i 2009 fusionerer med det norske selskab Nordito, som også leverer løsninger inden for betalingskort, betalingsformidling og informationstjenester. Nets-koncernen er ejet af danske og norske pengeinstitutter samt Danmarks Nationalbank, og selskabets bestyrelse består af repræsentanter fra ejerpengeinstitutterne (Konkurrence- og Forbrugerstyrelsen, 2012, s. 8).

debetkort med såkaldt saldokontrol. Ved sådanne debetkort undersøges det, om der er tilstrækkeligt indestående på forbrugerens konto til at dække købsbeløbet, før en transaktion påbegyndes. Er dette ikke tilfældet, afvises transaktionen. Eksempler på saldokontrolkort er MasterCard debet, Maestro og Visa Electron.

Kreditkort er et betalingskort, hvor der går et vist tidsrum, inden beløbet trækkes fra forbrugerens konto. Hvor lang tid, der går, afhænger af den aftale, som forbrugeren har med kortudstederen. Fx kan det være aftalt, at kortbrugeren ved udgangen af hver kalendermåned betaler for månedens køb på kortet. Det kan også aftales, at kortbrugeren ud over den løbende måned har en ekstra måneds kredit. Et kreditkort kan således være et alternativ til et lån i en bank eller hos en detailforretning. Eksempler på kreditkort er MasterCard, Diners Club og American Express.

Forudbetalte betalingskort er udstedt med et på forhånd betalt beløb, som kortbruger løbende kan bruge. Eksempler på forudbetalte kort er telekort og gavekort. For nogle af disse kort gælder, at kortet er værdiløst, når værdien er opbrugt, mens andre kan genoplades i særlige terminaler. I forhold til debet- og kreditkort kan mange af de forudbetalte betalingskort kun benyttes i begrænset omfang, fx alene til telefonopkald eller køb af varer i en bestemt forretning.

Internationale betalingskort kan benyttes i flere lande. Disse kort kan være både debet- og kreditkort. Eksempler på internationale debet- og kreditkort er Visa Electron og MasterCard debet (debetkort) samt Diners Club, AmericanExpress og MasterCard (kreditkort).

Til og med 2012 er der udstedt ca. 4,5 mio. Dankort, hvoraf ca. 3,5 mio. er Visa/Dankort (Konkurrence- og Forbrugerstyrelsen, 2012, s. 16). Det faktiske antal af dansk udstedte internationale betalingskort er fortroligt, men Konkurrence- og Forbrugerstyrelsen anslår, at antallet ligger på omkring 5 mio. i 2012. I perioden 2005 til 2012 ses en fordobling i antallet af internationale betalingskort ifølge styrelsen (2012, s. 19). Selvom antallet af udstedte internationale betalingskort overstiger antallet af (Visa/)Dankort, står (Visa/)Dankort stadig for hovedparten af brugen af betalingskort. Både målt i antallet af transaktioner og omsætning står (Visa/)Dankort således for fire femtedele af markedet.

5.2 Tilegnelse af kortoplysninger

Der findes forskellige metoder, hvormed betalingskort kan misbruges. Først og fremmest kan kortet blive stjålet ved et lommetyveri eller et indbrud. Så længe ofret ikke opbevarer sin pinkode sammen med kortet, kan et stjålet kort ikke anvendes i en pengeautomat (ATM) eller i en fysisk butik. Kortet kan derimod anvendes ved internethandel. Men det er sandsynligt, at ofret spærrer sit

kort, inden sådan en handel forsøges. Et stjålet betalingskort får således først for alvor værdi for en gerningsperson, hvis vedkommende også har den tilhørende pinkode.

Ifølge interviewrespondenten fra Nets er det oftest i forbindelse med, at ofret anvender sit betalingskort, at det stjæles. Pinkoden aflures, og bagefter stjæles kortet. Gerningspersonen slår gerne til på travle steder (stationer, supermarkeder osv.), hvor vedkommende skaber forvirring og snupper kortet (lommetyveri). Danske banker indberetter tredjemandsmisbrug på Dankort og Visa/Dankort til Nets. I ca. 80 procent af tilfældene vurderes det af pengeinstitutmedarbejder, der indberetter misbruget, at pinkoden er afluret i forbindelse med brug af en Dankort-terminal eller en pengeautomat. I 98 procent af tilfældene er Dankortet bortkommet eller stjålet. Kun i enkelte sager er der tale om, at kortet er frarøvet ofret med vold eller trussel om vold.

En anden fremgangsmåde til misbrug af betalingskort er skimming. Skimming foregår således, at gerningspersonen installerer teknik i hæve- eller benzinautomaten, der kan aflæse magnetstriben på kortet. For at få fat i pinkoden sættes et mikroskopisk kamera op, så der kan filmes, når pinkoden indtastes. At holde hånden over tastaturet, når koden tastes, er derfor den letteste måde at forebygge skimming. I Danmark kan oplysningerne ikke bruges, da der er chip på kortet, men det kan de i udlandet. Fx anvendes der i USA ikke chip men magnetstribe. Derfor sendes skimmingsoplysninger til udlandet, så kortet kan misbruges her.[12]

En tredje måde, hvorpå betalingskort kan misbruges, forgår på internettet. Kortoplysninger franarres enten ved hjælp af phishing (se også afsnit 3.3), aflures med spyware (se også afsnit 3.2), skimmes eller købes i internettets undergrundsøkonomi. Kortoplysninger, som stjæles ved et (stort) dataindbrud i en virksomhed, sælges ofte for et par dollars på nettet. På Tellers hjemmeside peges der i denne sammenhæng på hotelbookingssystemer:

> I hotellernes bookingsystemer bliver kortdata gemt i forbindelse med booking (for at sikre hotellet betaling, hvis gæsten tager af sted uden af betale). Disse data bliver oftest gemt i det lokale IT-system i klartekst bag et svagt kodeord til bookingdatabasen. Dermed er det nemt for svindlerne at få adgang til de gemte kortdata. (...) Et hotel i Jylland, der fik stjålet ca. 2.000 kreditkortnumre og efterfølgende måtte betale for undersøgelse og oprydning i deres IT-systemer. Den samlede regning kendes ikke, men eksperter vurderer, at det har kostet et 6-cifret beløb.

[12] Denne praksis har medført, at fx Rabobank (en hollandsk bank) ikke tillader brug af betalingskort uden for EU, medmindre kunden søger dispensation herfra.

5.3 Gerningsmandsprofil af skimmere

Skimming er et kendt fænomen, og journalisterne beretter ofte om det i avisartikler. Men jeg har søgt uden held efter en mere systematisk beskrivelse af skimmere. Et eksempel fra en avisnyhed i forbindelse med skimming er følgende:

> En 49-årig rumænsk mand fremstilles i dag ved retten i Kolding, da han i går blev afsløret i at sætte skimmingudstyr op på en tankstation i Vonsild. Tankens indehaver havde opdaget udstyret, og kontaktede derfor politiet, der valgte at overvåge tankstationen indtil gerningsmanden dukkede op. Det skete klokken 19, hvor den 49-årige rumæner blev anholdt (JydskeVestkysten, 30. december 2012).

I overstående eksempel fremgår det, hvordan skimmere kan blive anholdt af politiet. Datafilen, som Rigspolitiet har stillet til rådighed for denne undersøgelse, indeholder oplysninger om 52 personer, som er sigtede for skimming. De er enten anholdt i forbindelse med opsætning eller afhentning af skimmingudstyr, eller i forbindelse med at politiet har fundet udstyr ved ransagning af deres bil eller beboelse.

I det hollandske politifagblad *Blauw* beskrives skimming som organiseret kriminalitet. Ifølge Ralph Nagelkerke – projektleder af den hollandske skimming efterforskningsenhed – er skimmingbanderne hierarkisk organiseret, og de stammer fra Rumænien og Bulgarien. Blandt lederne af banderne er der folk med teknisk kendskab og fornuft til at udvikle skimming-udstyr, mens fodfolket rejser rundt i Europa og opsætter udstyret, kopiere kortoplysninger og aflure pinkoder. Ifølge Nagelkerke har banderne et tæskehold for at sikre sig, at pengene afleveres. Udbytte investeres i narkotikahandel, menneskesmugling mm. (Ruiter, 2013).

Køn, alder og nationalitet

I eksemplet fra Vonsild er gerningspersonen en 49-årig mand med rumænske nationalitet. Denne profil stemmer godt overens med oplysningerne på de 52 personer, der er sigtede i Danmark for skimming i perioden 2010-2012. På nær en er alle mænd, og mere end tre ud af fire af de sigtede er af rumænsk nationalitet. Derudover er der otte sigtede af udenlandsk nationalitet, og de er alle fra et europæisk land lig Danmark. Kun tre af de sigtede har dansk statsborgerskab, og to af disse har arbejdet sammen med en rumæner i deres skimmingsag. I eksemplet fra Vonsild er gerningsmanden 49 år, og denne alder er i den øvre del af aldersspektret blandt de 52 sigtede personer. De er nemlig alle mellem 21 og 49 år. Lidt over halvdelen af de sigtede er i tyverne, mens en tredjedel er i trediverne.

Tabel 5.1 Køn, alder og nationalitet blandt de sigtede for skimming (n=52)

	Antal personer	Procentdel
Mand	51	98 %
Kvinde	1	2 %
20 – 29 år	27	52 %
30 – 39 år	18	35 %
40 – 49 år	7	13 %
Rumænien	41	79 %
Danmark	3	6 %
Europa	8	15 %

Samarbejde i grupper

Mange skimmere har en makker eller arbejder sammen i grupper. Eksempelvis er en gruppe bestående af fire rumænske mænd sigtet for i alt 117 forhold i forbindelse med opsætning af skimmingudstyr og afluring af kortoplysninger i en af Danske Banks hæveautomater. Det er blevet til 117 forhold for hver enkelt identificeret kort, der er skimming er et forhold. Herudover indeholder datafilen en sag hvor syv mænd af rumænske nationalitet er sigtet for skimming. De har nemlig opholdt sig i et sommerhus, hvor politiet har fundet en betalingsenhed fra en ubemandet tankstation og et par briller med indbygget videokamera. Desuden er to mænd med henholdsvis fransk og belgisk nationalitet sigtet for i alt 39 forhold vedrørende skimming ved hæveautomater på Fyn.

Tabel 5.2 Gruppestørrelse ud fra antal sigtede

	Antal grupper	Antal sigtede	Procentdel
Solo	9	9	17 %
2 personer	3	6	12 %
3 personer	2	6	12 %
4 personer	3	12	23 %
5 personer	1	5	10 %
7 personer	2	14	27 %
I alt	**20**	**52**	**100 %**

5.4 Misbrug af Dankort

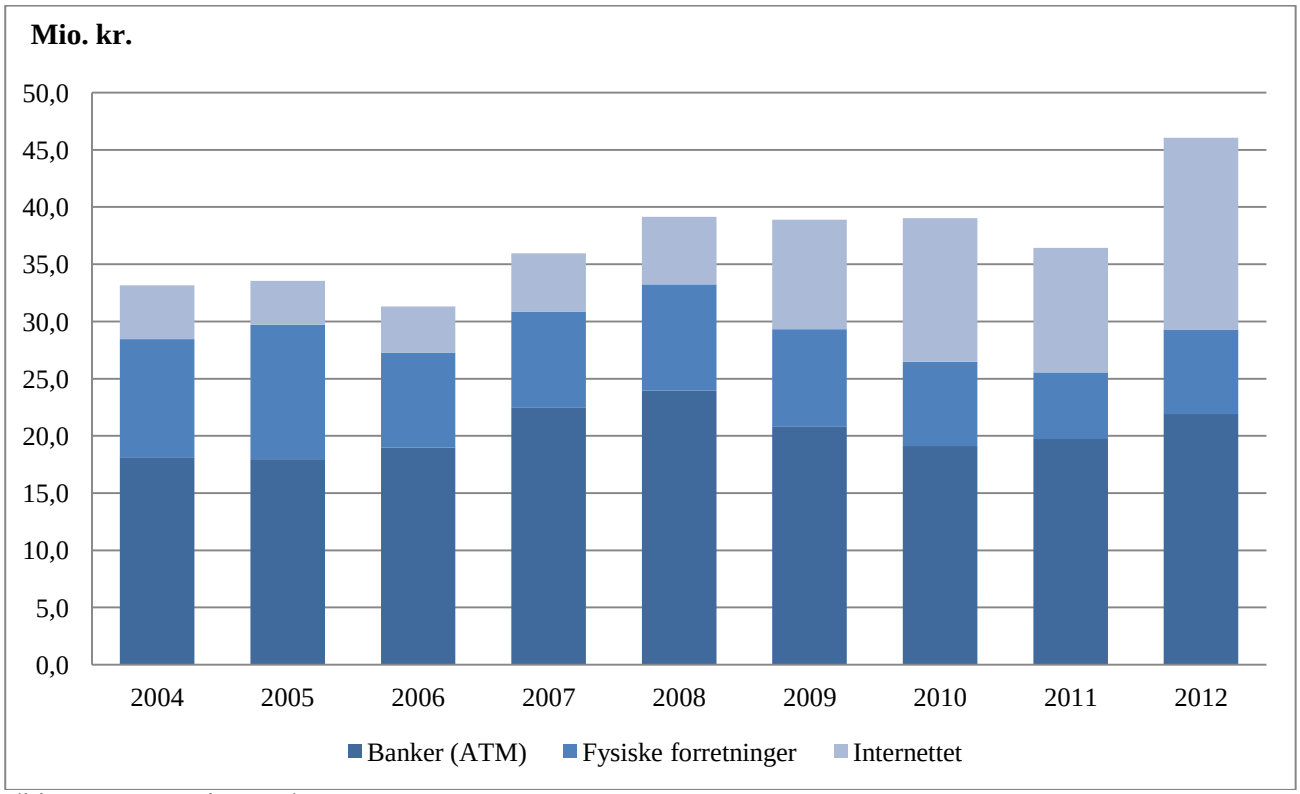
Nets indsamler data om misbrug af Dankort og offentliggør nogle af disse oplysninger på deres hjemmeside. Når et Visa/Dankort anvendes i Danmark, er det Dankort-delen af kortet, der benyttes. Når kortet derimod anvendes i udlandet, træder Visa-delen af kortet i kraft. Nets offentliggør kun tal vedrørende Dankort-delen, med andre ord: Misbrug på det danske marked. De tal, der offentliggøres, knytter sig til omfanget af tab på grund af misbrug og antal sager/transaktioner, hvori Dankort er misbrugt. I forbindelse hermed deler Nets misbrug op i tre hovedkategorier: tabt/stjålet,

falsk og fjernsalg. Imidlertid anvender Nets også et sæt underkategorier, der skelnes således mellem følgende tre steder, hvor misbrug af Dankort kan finde sted:

- Banker: Ved hæveautomater (ATM) med pinkode eller i banken med underskrift
- Fysiske forretninger: Ved Dankortterminaler med pinkode eller nota med underskrift
- På internettet[13]: Indtastning af kortnummer, kontrolcifre og udløbsdato

Figur 5.1 viser tabet i perioden 2004 til 2012. Det samlede tab stiger i denne periode fra 33,2 mio. kr. i 2004 til 46,1 mio. kr. i 2012. Det svarer til en stigning på 39 procent. Figuren viser desuden, at internettet benyttes oftere og oftere ved misbrug af Dankort i perioden fra 2004 til 2012. I 2004 står internethandel således for 14,2 procent af det samlede tab, mens andelen stiger til 36,4 procent i 2012. Det er ikke overraskende, at internettet tegner sig for en voksende del af Dankortmisbrug, da internethandel er i kraftig vækst.

Figur 5.1 Samlede tab på grund af Dankortmisbrug



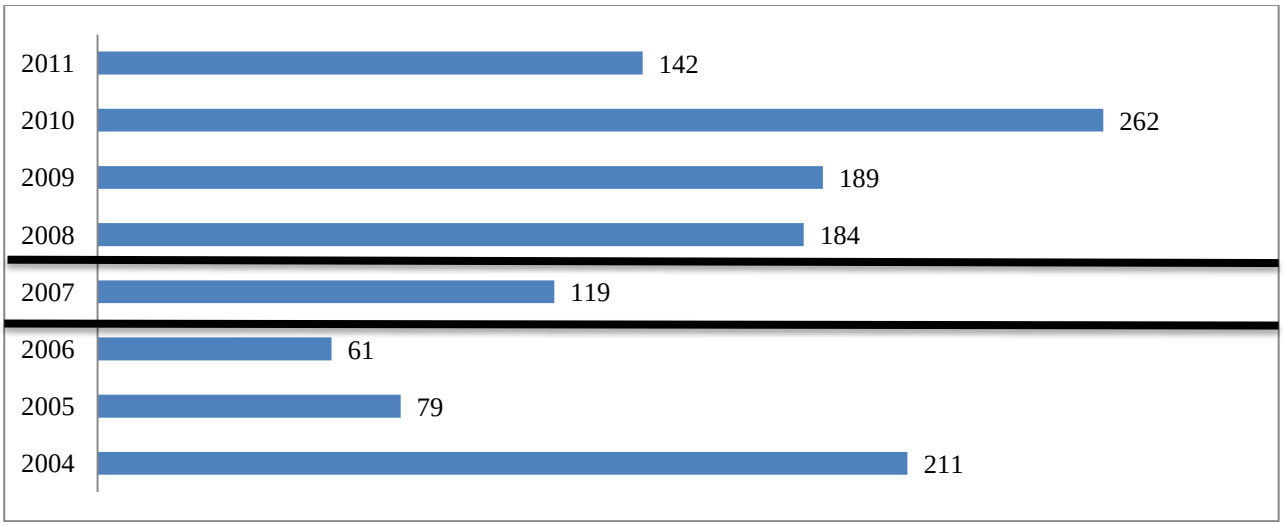
Kilde: Nets (egne beregninger)

[13] Denne kategori omfatter også post- og telefonordre og betalingsautomater uden pinkode. Det antages imidlertid, at internettet står for langt de fleste sager indenfor denne kategori.

I forbindelse med handel i offline verdenen er forholdet mellem antal misbrugssager med Dankort og antal Dankort-transaktioner nogenlunde konstant i perioden fra 2004 til 2011 ifølge Konkurrence- og Forbrugerstyrelsen. Der er således 4-5 sager om året pr. 1 mio. transaktioner.

Antallet af misbrugssager pr. 1 mio. transaktioner er i forbindelse med internethandel markant højere. Figur 5.2 viser et fald i antallet af misbrugssager pr. 1 mio. Dankort-transaktioner på internettet i perioden fra 2004 til 2006. En mulig forklaring herpå er, at PBS (det nuværende Nets) i 2005 indfører et krav om, at forretningerne i forbindelse med brug af betalingskort på internettet skal spørge om kortets kontrolcifre. Det ser dog ikke ud til, at dette tiltag har en længerevarende effekt. Allerede i 2007 stiger antallet af misbrugssager pr. 1 mio. transaktioner igen. Dette er imidlertid en fejlfortolkning af tallene. Nets skriver i deres vejledning, at misbrugsstatistikken i forbindelse med internethandel ændres i 2007: Fra andet halvår af 2007 baserer misbrugstallet sig på antal Dankort-transaktioner og således ikke længere antal sager. Et kort kan misbruges i flere omgang, før det spærres, og flere transaktioner med et kort tæller som en sag. Selvom Konkurrence- og Forbrugerstyrelsens beregning er misvisende, holder deres konklusion, at det stadig er muligt at misbruge et Dankort på internettet blot ved at være i besiddelse af kortet (2012, s. 54).

Figur 5.2 Antal misbrugstransaktioner/sager pr. 1 mio. dankorttransaktioner på internettet



Kilde: Konkurrence- og Forbrugerstyrelsen, 2012, s. 53, Tabel 7.2

5.5 Internationale betalingskort

Det samlede tab på grund af Dankortmisbrug ligger på ca. 40 mio. kr. om året. Men der findes, som beskrevet, også andre betalingskort i Danmark. Den største del af de internationale kort indløses hos Teller – et datterselskab til Nets. Men der er også andre indløser som Swedbank, Valitor og SEB Kort. Ifølge interviewrespondenten fra Nets indløser Teller op til 95 procent af al handlen via internationale betalingskort i fysiske butikker. Ved internethandel er marked i mindre grad domineret af Teller, men også her er Teller den største aktør.

Der mangler et samlet overblik over misbrug af internationale kort i Danmark, da de enkelte kortselskaber ikke offentliggør deres misbrugstal. Ifølge interviewrespondenten fra Nets knytter dette hemmelighedskræmmeri sig til konkurrencen på marked. I rapporten Betalingskortmarkedet (Konkurrence- og Forbrugerstyrelse, 2012) fremstilles dog et skøn over omfanget af misbrug med internationale kort på baggrund af oplysninger fra Mastercard, Visa, Nets, Danske Bank og SEB Bank. I perioden fra 2009 til 2011 ligger tabet i forbindelse med brug af internationale kort således på omkring 50 mio. kr. på årsbasis.

Set ud fra antallet af udstedte kort ligger misbruget af henholdsvis (Visa/)Dankort og internationale betalingskort på nogenlunde samme niveau (der findes lidt flere internationale kort end Dankort). Men set ud fra antallet af transaktioner er misbrug af internationale kort langt mere udbredt end misbrug af Dankortet (Dankort står for ca. 80 procent af alle korttransaktioner).

Der er to markante forskelle mellem misbrug af Dankort og internationale betalingskort. For det første har der siden 2008 ikke været sager med forfalskning (skimming) af Dankort, mens falske kort står for ca. 40 procent af tabet i forbindelse med udenlandske betalingskort. Forskellen kan forklares med, at Dankort er udstyret med chip, der er betydeligt sværere at forfalske. Desuden benyttes der ikke altid pinkode i forbindelse med internationale betalingskort, når transaktionen skal accepteres er en underskrift ofte nok. Den vigtigste forklaring er imidlertid, at internationale betalingskort også kan anvendes i udlandet, og ikke i alle lande benyttes chip til at gennemføre en transaktion. Den anden forskel mellem misbrug af Dankort og internationale kort er, at internationale kort oftere misbruges ved internethandel. Det skønnes, at internethandel står for ca. halvdelen af tabet i forbindelse med misbrug af internationale betalingskort i 2011, hvilket svarer til ca. 25 mio. kr. Dette er et betydeligt højere beløb end de 11 mio. kr., som tabet i forbindelse med misbrug af Dankort ved internethandel ligger på i 2011.

5.6 Misbrug af betalingskort (offerundersøgelse)

Som beskrevet i kapitel 1 er der gennemført en offerundersøgelse som led i Danmarks Statistiks omnibusundersøgelser. Offerundersøgelsen baserer sig på en stikprøve blandt tilfældige danskere i alderen 16-74 år. I forbindelse med undersøgelsen er der stillet spørgsmål omkring betalingskortmisbrug (se bilag 1) til 9.582 respondenter i perioden oktober 2012 til og med juli 2013. Af disse 9.582 respondenter angiver 71 personer eller 0,74 procent, at de har været udsat for kortmisbrug indenfor de sidste 12 måneder.

Stikprøven er repræsentativ for befolkningen som helhed. Der kan dog være en skævhed i bortfaldet. For at teste om der er tale om en sådan skævhed har Danmarks Statistik udarbejdet vægte baseret på personoplysninger. Når disse vægte anvendes falder offerrisikoen for kortmisbrug fra

0,74 procent til 0,71 procent. Ifølge de vægtede data har 29.408 danskere været udsat for kortmisbrug indenfor de sidste 12 måneder. Da opgørelsen er baseret på en stikprøve, medfører dette en vis statistisk usikkerhed. Hvis stikprøven – som antaget – er a-selektiv, kan et 95 % -sikkerhedsinterval beregnes. Intervallet ligger mellem 0,6 – 0,9 procent, eller, når det ganges op til at gælde hele den danske befolkning, mellem 22.463 – 36.353 danskere.

Tabel 5.3 Offerrisiko for kortmisbrug

	Stikprøve	Befolkning (estimat)
Omfang	9.582	4.153.968
Andel af udsatte for kortmisbrug	0,7 %	29.408
95 % -interval	0,6 – 0,9 %	22.463 – 36.353

Online/offline tilegnelse

Gerningspersonen kan tilegne sig udsattes betalingskortoplysninger online eller offline. I offerundersøgelsen er de 71 respondenterne, der har været udsat for kortmisbrug, spurgt, om de har en anelse om, hvordan gerningspersonen har fået fat i deres kortoplysninger. Næsten trefjerdele – 51 ud af de 71 respondenter (72 %) – har en anelse, og to tredjedel mener, at det er sket online. Tabel 5.4 viser en oversigt over de metoder, der efter respondenternes egen vurdering er anvendt til tilegnelse af deres kortoplysninger.

Tabel 5.4 Anvendte metoder i forbindelse med tilegnelse af betalingskortoplysninger

	Antal	Procentdel
Online metoder	*34*	*67 %*
I forbindelse med handel på nettet	21	41 %
Hacking	7	14 %
Phishing/pharming	5	10 %
Selv lagt på nettet	1	2 %
Offline metoder	*17*	*33 %*
Ved anvendelse i udlandet	10	20 %
Stjålet (indbrud, lommetyveri mm)	7	14 %
I alt	**51**	**100 %**

Note: 20 respondenter har ingen anelse om, hvordan deres betalingskortoplysninger er stjålet.

Hensigten med kortmisbruget

Misbruget af forurettedes betalingskortoplysninger knytter sig i halvdelen af tilfældene til, at gerningspersonen ønsker at købe noget – for det meste online. Herudover misbruges kortet til at hæve eller overføre penge for forurettedes konto. Tabel 5.5 viser en oversigt over gerningspersonens hensigt med kortmisbruget.

Tabel 5.5 Gerningspersonens hensigt med misbruget af betalingskortoplysninger

	Antal	Procentdel
Købe online	30	42 %
Købe offline	6	8 %
Hæve penge	17	24 %
Overføre penge	10	14 %
Andet misbrug	8	11 %
I alt	**71**	**100 %**

5.7 Tabsfordeling mellem parterne

Retsgrundlaget for internethandel er betalingstjenesteloven. § 74 af denne lov regulerer den såkaldte *charge back* ved fjernsalgstransaktioner (Karstoft, 2012): Betalerens udbyder er forpligtet til at undlade at gennemføre en betalingstransaktion eller at tilbageføre et beløb, der allerede er debiteret betalerens konto, såfremt betaleren fremsætter en (eller flere) af de indsigelse(r), der er opregnet i § 74, stk. 1, nr. 1-3:

- Nr. 1: debiterede beløb er højere end det beløb, der er aftalt med betalingsmodtageren.
- Nr. 2: en bestilt ydelse er ikke leveret.
- Nr. 3: betaleren har udnyttet en fortrydelsesret.

Betalingstjenesteloven regulerer også hvem, der hæfter for tab ved misbrug af betalingskort. § 62 handler således om tabsfordelingen mellem betaleren og udbyderen. Når der er tale om misbrug, skal betaleren melde misbruget til udbyderen. Da det er svært at bevise, at betaleren ikke selv har anvendt sit betalingskort, er en tro og lov erklæring nok. Betaleren har en indsigelsesfrist. Det skal meldes snarest, men senest 13 måneder efter debiteringen. Passivitet kan føre til, at retten til at gøre indsigelsen tabes inden for 13-måneders fristen. Når kortindehaveren erklærer, at betalingskortet er misbrugt, skal udbyderen bære tabet ifølge betalingstjenesteloven. Men indehaveren kan hæfte for en selvrisiko. Selvrisikoen beskrives i betalingstjenesteloven § 62, stk. 2. Der skelnes mellem tre størrelser knyttet til selvrisikobeløbet (Karstoft, 2012):

- 1.100 kr. hvis pinkoden er mistet, uanset om det kan bebrejdes indehaveren af kortet (undtagelse: vold eller trussel om anvendelse af vold).
- 8.000 kr. hvis det er undladt at underrette udbyder af kortet snarest muligt; hvis indehaveren overgiver pinkode, mens den kunne/burde indse, at der er risiko for misbrug; hvis groft uforsvarlig adfærd ved opbevaring af pinkoden.
- Ubegrænset. Selv oplyst pinkoden.

Reglerne for selvrisiko gælder ikke, hvis der ikke benyttes en personlig sikkerhedsforanstaltning, fx en pinkode. Ved internethandel med Dankort findes der ikke sådan en foranstaltning, og dette be-

tyder, at indehaveren af kortet ikke hæfter for en selvrisiko. Det er anderledes, når internethandel betales med et internationalt betalingskort. Både Visa og Mastercard benytter den såkaldte 3D Secure. Ved siden af kortnummer, udløbsdato og kontrolcifre skal betaleren indtaste en selvoprettet kode, før betalingen gennemføres.

Når et Dankort bruges – i en ATM, butik eller på internettet – kontrolleres kortoplysningerne af Nets. Hvis kortet ikke er spærret, eller kortbrugen ikke virker mistænksom (fx brug af kortet inden for meget kort tid), gennemføres betalingen uden at tjekke ved kortudstederen (banken), om der er dækning på kortet. Der er i princippet ikke et maksimum beløb, som kan trækkes på Dankortet, men en butik hæfter for tab over 4.000 kr. i forbindelse med en handel i offline verdenen. Når en butiksejer tillader en kunde at betale et beløb over 4.000 kr., er det således på egen risiko. I praksis reagerer butiksejerne forskelligt, når en kunde med et Dankort vil betale en vare, som overstiger 4.000 kr. Nogle butikker spørger om legitimation, mens andre ikke gør. Ved internetkøb hæfter forretningen for tabet, når beløbet overstiger 1.000 kr., og der ikke er dækning.

Bankernes tab knytter sig hovedsagligt til Dankortmisbrug i hæveautomater. Kundernes tab skyldes først og fremmest selvrisikoen, når andre benytter deres pinkode. Mens forretningernes tab hovedsagligt skyldes internethandel. Tabel 5.6 viser en oversigt over årene 2010 til 2012. I tabellen er betalerens (kundernes) del af tabet beregnet ud fra en selvrisiko på 1.100 kr. Det antages, at hver misbrugssag, hvor Dankortet tabes eller stjæles, udløser denne selvrisiko, og at beløbet inkasseres af udstederen (banken).

Tabel 5.6 Tabsfordeling ved Dankortmisbrug i mio. kr.(2010-2012)

	2010		2011		2012	
	beløb	andel	beløb	andel	beløb	andel
Banker	21,3	55 %	21.4	59 %	25,1	54 %
Kunder	3.0	8 %	3.1	9 %	2,9	6 %
Forretninger	14.7	37 %	11.9	33 %	18,1	39 %
Samlet tab	**39.0**	**100 %**	**36.4**	**100 %**	**46.1**	**100 %**

Kilde: Nets (egne beregninger)

Ved brug af et internationalt betalingskort er indløserens procedure anderledes. I forbindelse hermed kontrolleres kortoplysningerne også, men herudover er der desuden kontakt med kortudstederens datacentral for at tjekke, om der er tilstrækkelig dækning på kortet. Denne procedure medfører, at forretninger ikke hæfter for tab i tilfælde af misbrug. Ulempen ved denne fremgangsmåde er, at omkostningerne ved betaling med et internationalt kort er væsentligt højere end ved Dankort. Ved internethandel er disse omkostninger synlige for kunden, og ofte kan kunden vælge hvilken betalingsform, der skal benyttes – med en forskellig gebyrtarif.

5.8 Offerprofil i forbindelse med betalingskortmisbrug

Offerundersøgelsen viser, at risikoen for at blive udsat for betalingskortmisbrug er størst for aldersgruppen 30-49 år. Det gælder både for mænd og kvinder. Offerrisikoen for mænd er dog generelt højere end for kvinder. Det betyder, at mænd i alderskategorien 30-49 år er den mest udsatte gruppe.

Tabel 5.7 Offerrisiko for betalingskortmisbrug efter køn og alder

	Mand	Kvinde	I alt
Under 30 år	0,9 %	0,4 %	0,6 %
30 – 49 år	1,1 %	0,8 %	0,9 %
50 år og ældre	0,7 %	0,6 %	0,6 %
I alt	**0,9 %**	**0,6 %**	**0,7 %**

Note: Antal ofre er 71, og stikprøven omfatter 9.582 respondenter.

Der er en sammenhæng mellem erhverv og offerrisiko, hvilket tabel 5.8 viser. Respondenter uden arbejde har således en anelse højere offerrisiko. Modsat de øvrige undersøgte internetkriminalitetsformer er pensionister ikke underrepræsenterede blandt ofrene. Det kan formentlig forklares med udgangspunkt i det faktum, at pensionister også har et betalingskort, og misbrug af et betalingskort på internettet forudsætter ikke nødvendigvis, at kortoplysningerne er mistet online.

Tabel 5.8 Offerrisiko for betalingskortmisbrug efter erhverv

	Antal ofre	Antal resp.	Offerrisiko
Med arbejde	40	5.461	0,7 %
Uden arbejde	10	898	1,1 %
Studerende	9	1.286	0,7 %
Pensionister	12	1.928	0,6 %
I alt	**71**	**9.573**	**0,7 %**

Note: Uden erhverv omfatter også førtidspensionister, mens efterlønsmodtagere hører til kategorien pensionister.

5.9 Gerningsmandsprofil af betalingskortmisbrugere

I datafilen, som Rigspolitiet har stillet til rådighed for denne undersøgelse, knytter alle sigtelserne i forbindelse med misbrug af betalingskortoplysninger sig til køb på nettet. Det kan være køb af varer/ydelser (fx taletid) eller misbrug i et online kasino. Det afhænger af fremgangsmåden, hvordan politiet registrerer disse sager. I perioden 2010-2012 er der sigtet 344 unikke personer for 1.145 forhold i forbindelse med misbrug af betalingskort. De fleste sigtes efter databedrageri (§ 279a) eller bedrageri (§ 279) bestemmelserne. Tabel 5.9 viser en oversigt.

Tabel 5.9 Lovovertrædelse som betalingskortmisbrugere er sigtet for (2010-2012)

	Antal forhold	Antal sigtede	Antal forhold pr. sigtede
Bedrageri	417	130	3,2
Databedrageri	662	164	4,0
Dokumentfalsk	66	50	1,3
I alt	**1.145**	**344**	**3,3**

Som skrevet er der sigtet 344 personer for misbrug af betalingskortoplysninger i perioden 2010-2012. Blandt de sigtede er kønsfordelingen skæv, eftersom 82 ud af de 344 (24 procent) er kvinder. Andelen af sigtede kvinder er således større sammenlignet med andelen af sigtede for henholdsvis hacking, id-misbrug og skimming (jf. afsnit 3.5, 4.5 og 5.3). Desuden er godt tre ud af fire sigtede af dansk nationalitet. De 80 sigtede med udenlandsk nationalitet kommer fra 34 forskellige lande. Størstedelen er fra Østeuropa, Mellemøsten eller Afrika. Den yngste person, der er sigtet for misbrug af betalingskortoplysninger, er 12 år, og den ældste er 62 år. Mere end halvdelen af de sigtede er 15-24 år. Desuden er 63 af de sigtede under 18 år (18 procent). Tolv af dem er under den kriminelle lavalder, mens de resterende er 15, 16 eller 17 år gammel.

Tabel 5.10 Aldersfordelingen blandt sigtede betalingskortmisbrugere i Danmark (2010-2012)

	Antal	Procentdel
14 år eller yngre	12	4 %
15-24 år	185	54 %
25-34 år	85	25 %
35-44 år	38	11 %
45-54 år	22	6 %
55-64 år	2	1 %
I alt	**344**	**100 %**

Kriminel løbebane

Blandt de 344, som sigtes for betalingskortmisbrug i perioden 2010-2012, er 207 også sigtede for en eller flere lovovertrædelser i perioden 2001-2009. Det svarer til en recidivprocent på 60. 36 procent af recidivisterne sigtes en eller to gange i 2001-2009, mens 64 procent af recidivisterne tegner sig for tre eller flere sigtelser.

Tabel 5.11 Antal sigtelser for lovovertrædelser i perioden 2001-2009

	Antal personer	Også ligeartet
Ingen sigtelser	137	
1 sigtelse	51	6
2 sigtelser	23	3
3-10 sigtelser	66	16
Mere end 10 sigtelser	67	34
I alt	**344**	**59**

59 ud af de 207 personer, der betegnes som recidivister, begår ligeartet kriminalitet i perioden 2001-2009 (se også afsnit 1.4.5). Mere end halvdelen (58 procent) af dem falder i kategorien 'meget kriminel aktiv', hvilket svarer til mere end 10 sigtelser. Et eksempel herpå er en 50-årig mand fra København, der registreres for 133 sigtelser i perioden 2001-2009. 23 af disse er for ligeartet kriminalitet. I perioden 2010-2012 sigtes han for 30 forhold i forbindelse med misbrug af kortoplysninger, idet han køber varer på nettet med aflurede kortoplysninger. Et andet eksempel er en 22-årig kvinde fra Randers, der i 2010-2012 sigtes for at købe cigaretter og booke et hotelværelse med et stjålet Dankort. Depositummet for hotelværelset tilbagebetales dog efter annullering den efterfølgende dag. Hun sigtes i perioden 2001-2009 for 98 forhold, og 28 af disse er ligeartet kriminalitet.

5.10 Kortmisbrug i Danmark internationalt set

Den Europæiske Central Bank (ECB) publicerer tal om kortmisbrug i eurolandene.[14] I denne opgørelse anvendes samme opdeling, som Nets benytter i forbindelse med Dankortmisbrug statistik: banker (ATM), fysiske forretninger (POS) og internettet (CNP). Det viser sig, at kortmisbrug forgår i mindre grad på internettet i Danmark sammenlignet med eurolandene. En del af forklaringen er, at mange internetforretninger har en fælles server og hjemmesider for Europa, der administreres fra et enkelt land. Disse sider frekventeres også af danske kortindehavere, men er ikke med i opgørelsen over Dankort, da betalingen typisk sker med Visa.

Tabel 5.12 Kortmisbrug i Danmark vs. Eurolandene

	Dankort	Internationale kort i Danmark	Eurolande
Banker (ATM)	49 %	57 %	16 %
Fysiske forretninger (POS)	19 %		32 %
Internettet (CNP)	32 %	43 %	52 %

Kilde: Nets, ECB

[14] SEPA: Single Euro Payments Areas

Som beskrevet tidligere er der ca. 5 misbrugssager pr. 1 mio. Dankort-transaktioner i forbindelse med handel i offline verdenen. Dette svarer til 0,0005 procent. Ses der i stedet på internethandel, er der ca. 200 misbrugssager pr. 1 mio. dankorttransaktioner, altså 0,02 procent. I ECB-rapporten relateres kortmisbrug også til antal transaktioner, men her skelnes der ikke mellem handel offline og online. Den samlede andel af misbrug i forhold til antal transaktioner ligger i eurolandene på 0,02 procent i årene 2007 til 2010 ifølge ECB-rapporten. Det er samme niveau som ved internethandel, hvor der anvendes Dankort.

Ifølge ECB er 1,2 procent af alle fysiske kort udstedet i eurolandene udsat for misbrug. Det vil sige, at 12 ud af 1.000 betalingskort misbruges (ECB, 2012, s. 8). Det kunne være interessant at beregne dette procenttal for betalingskort udstedet i Danmark. Men det er umuligt, så længe danske kortudstedere ikke åbner op for informationsdeling.

6 Bedrageri ved internethandel

6.1 Internethandel

Der handles mere og mere på internettet. I 2012 gennemfører danskerne således 90 mio. handler, viser en analyse fra FDIH (2012b). Køb af tøj og sko er i vækst, mens køb af bøger, tidsskrifter og aviser aftager. De fleste kunder er tilfredse med leveringen af de købte vare, og de anvender hyppigst Dankort i forbindelse med betalingen (FDIH, 2012b). Det er imidlertid ikke kun via internetbutikker, at der handles på internettet. Privatpersoner sælger også ud, fx via dba.dk, qxl.dk og lauritz.com.

Hvor der handles for så mange penge, findes kriminelle, der forsøger at få fat i en del af pengene. Derfor er der blandt andet indført et e-mærke for at beskytte danskere, der handler på internettet. E-mærket er en mærkningsordning for sikker nethandel. Den administreres af handelsfonden, der er en non profit organisation, som stiftes i 2000 af en række brancheorganisationer. Der er i alt 1.569 e-mærkede internetbutikker (pr. 20. september 2013). Men e-mærket misbruges også. På e-mærkets internetside opfordres forbrugere til at spotte falske internetbutikker, og alene i 2012 anmeldes 298 sager (emaerket.dk). På e-mærkets internetside påpeges det, at udenlandske svindlere i stigende grad misbruger e-mærket og andre troværdighedsskabende brands, når de opretter falske internetbutikker.

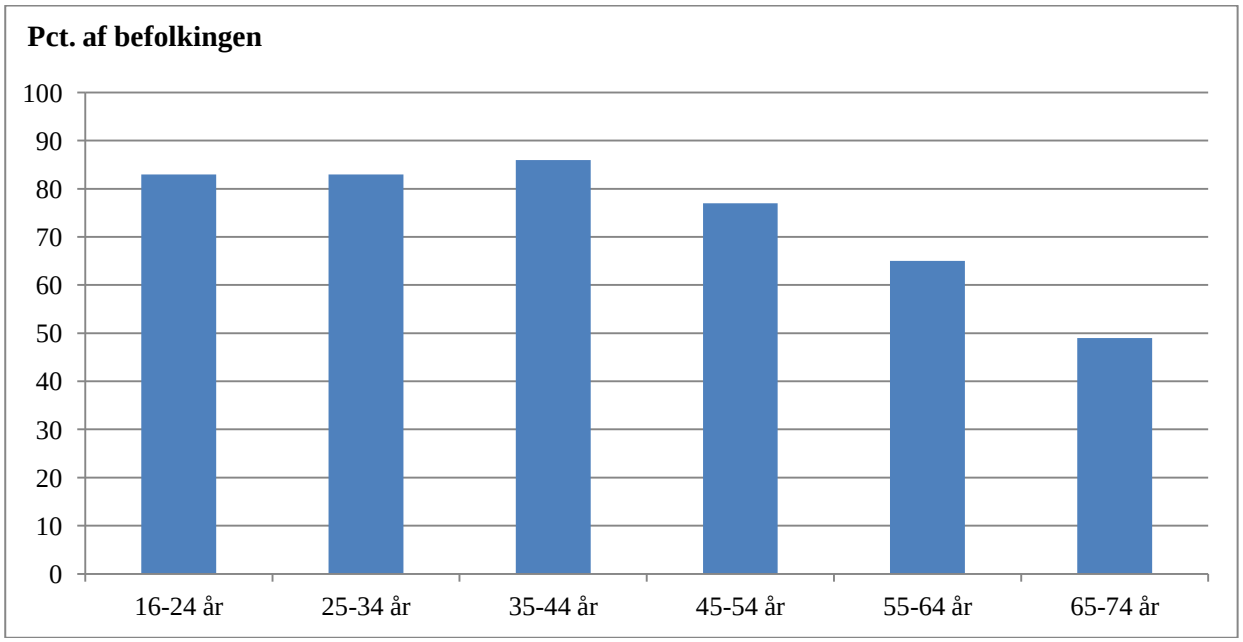
Internetbutikker

Den danske internethandel udgør i 2012 54,7 mia. kr., hvoraf 12,5 mia. ligger i udenlandske internetbutikker (FDIH, 2012b). Internethandlen udgør ca. 18 procent af detailhandlens samlede omsætning på 283 milliarder kroner. Det skal imidlertid ses i den sammenhæng, at 45 procent af detailhandlen udgøres af dagligvarer, og for denne varekategori udgør internethandel blot en lille del af det samlede salg. Der er derfor brancher, hvor internethandlen udgør langt mere end de 18 procent, som gennemsnittet lyder på. Internethandel repræsenterer både rene internetbutikker og fysiske butikker, der opretter sig på internettet for at modstå konkurrencen og imødekomme forbrugernes ønsker (Sørensen, 2013).

Ifølge FDIHs årsrapport for 2011 består ca. halvdelen af internethandlen af fysiske varer (med computerhardware og elektronik øverst på listen), mens den anden halvdel består af ikke-fysiske varer, som rejser, flybilletter og underholdning.

Syv ud af ti danskere i alderen 16-74 år køber varer eller tjenester på internettet i 2011. Det er markant flere end gennemsnittet i de 27 EU-lande, der ligger på godt fire ud af ti indbyggere (Danmarks Statistik, 2012). Set i et historisk perspektiv er internetkøb i EU-landene mere end fordoblet i perioden fra 2004 til 2011. Ses der specifikt på Danmark er andelen steget fra lidt over 40 procent i 2004 til 70 procent i 2011. I Danmark er internetkøb en anelse mere udbredt blandt mænd (72 procent) end kvinder (68 procent). Desuden aftager internethandel med alderen, hvilket er forventeligt. Dog køber knap halvdelen af aldersgruppen 65-74 år varer og/eller ydelser på internettet.

Figur 6.1 Internetkøb i Danmark fordelt på alder (2011)



Kilde: Danmarks Statistik, 2012, Figur 31, s. 24

Det er en bred vifte af varer og ydelser, der købes på internettet. Eksempelvis køber en stor del af danskerne (67 procent) billetter til teater, koncerter mv., og også overnatninger i forbindelse med rejser anskaffes flittigt over internettet (60 procent). Desuden køber halvdelen af danskerne tøj på internettet, mens en tredjedel anskaffer elektronik (Danmarks Statistik, 2012). Langt de fleste danskere, der køber over internettet, benytter sig af nationale forhandlere (82 procent). Men en betydelig mindre andel handler også i andre EU-lande (40 procent). Handler uden for EU er mindre udbredt blandt danskere (17 procent). Den samme tendens gør sig gældende i de øvrige EU-lande. Ved internetbetalinger benytter de fleste danskere Dankort. Ifølge nationalbankens beregninger står Dankort således for 72 procent af internetbetalinger, mens andre betalingsmetoder står for de resterende 28 procent (Wix Wagner, 2012).

Private handler på internettet

Danskere handler også privat på internettet, og der er utallige sider, hvor der kan opslås en salgs- eller købsannonce. Mange af disse internetsider retter sig mod et bestemt publikum. Fx er der heste-nettet.dk, hestegalleri.dk og youngrider.com for folk, der interesserer sig for heste. De mest

kendte almene handelssider på nettet er: dba.dk (Den Blå Avis), qxl.dk og lauritz.com. Den Blå Avis fungerer som en opslagstavle, mens QXL og Lauritz.com er auktionssider. På dba.dk er der mange private sælgere, der annoncerer, og som udgangspunkt er der ingen fortrydelsesret i handler private imellem. Men der er også mange erhvervsdrivende, der benytter dba.dk som platform, og indgås der handler med disse, gælder 14 dages returret ifølge forbrugeraftaleloven. I princippet blander dba.dk – som er en del af eBay – sig ikke i handler, men på siden står der gode råd til, hvordan der købes sikkert. Bl.a. er der advarsler mod falske annoncer og hælervare:

> Oplever du en billig iPhone, iPad eller bil, hvor prisen næsten er for god til at være sand, skal du som udgangspunkt være skeptisk. Mange steder på nettet florerer der falske annoncer, hvor svindlere forsøger at få dig til at forudbetale for en vare som ikke eksisterer. Kendetegnene for disse falske annoncer er: annonceteksten er på dansk, men dialogen er efterfølgende på engelsk; prisen på varen er billigere end tilsvarende; beløbet skal forudbetales til en udenlandsk bankkonto (dba.dk).

For at øge sikkerheden ved køb tilbyder dba.dk cpr- eller nemID-validering af sælgeren. Dette er udelukkende et tilbud og således ikke et krav. Ellers rådes køberen til at benytte PayPal i forbindelse med betaling. Herved kan køberen nemlig i visse tilfælde få pengene tilbage: Hvis varen ikke modtages, eller hvis varen afviger væsentligt fra beskrivelsen. Servicen er dog ikke gratis. Det koster sælgeren 2,60 kr. pr. handel plus 3,4 procent af salgsprisen.

Lauritz Christensen Auktioner er et af Danmarks ældste auktionshuse, og med konverteringen til lauritz.com i slutningen af 1999 er Lauritz det første auktionshus, der går over til internetauktioner. I marts 2013 køber Lauritz.com QXL Danmark og QXL Norge. QXL er Danmarks største online auktions- og handelsplads med ca. en halv mio. registrerede medlemmer. Her sættes hver uge op mod 1,3 mio. varer til salg af private, virksomheder og andre organisationer. Køberen på QXL er beskyttet på lige fod som ved en butikshandel. I QXLs generelle vilkår og regler står blandt andet følgende:

> Som sælger (uanset om du er registreret som privat eller erhvervsmedlem) på QXL, vil du oftest skulle yde fortrydelsesret til dine købere, ligesom du er forpligtet til at overholde Forbrugeraftalelovens regler om forbrugerbeskyttelse, herunder fortrydelses- og reklamationsret. Derudover skal du oplyse om eventuel fortrydelsesret i varebeskrivelsen, og skal også skriftligt oplyse køber om eventuel fortrydelsesret, når du kontakter vedkommende, efter at auktionen er afsluttet (§ 6.8.1 Fortrydelsesret).

6.2 Bedrageri ved internethandel

Som beskrevet i kapitel 1 er der gennemført en offerundersøgelse som led i Danmarks Statistiks omnibusundersøgelser. Offerundersøgelsen baserer sig på en stikprøve blandt tilfældige danskere i alderen 16-74 år. I forbindelse med undersøgelsen er der stillet spørgsmål omkring bedrageri ved internethandel (se bilag 1) til 9.582 respondenter i perioden oktober 2012 til og med juli 2013. Af disse 9.582 respondenter angiver 233 personer eller 2,4 procent, at de har været udsat for bedrageri indenfor de sidste 12 måneder. Da opgørelsen baserer sig på en stikprøve, medfører dette en vis statistisk usikkerhed.[15]

Offerundersøgelsen viser altså, at risikoen for bedrageri ved internethandel er 2,4 procent. Når dette procenttal skal ganges op til at gælde antallet af danskere, der udsættes for bedrageri ved internethandel, er et væsentligt spørgsmål: Hvorvidt e-handel skal anses som en personlig aktivitet eller en husstandsaktivitet. Formentligt afhænger svaret på dette spørgsmål (til dels) af hvilket produkt, der tales om. Er det en vare eller ydelse til personlig brug fx tøj, svarer manden antageligt 'nej' på spørgsmålet om bedrageri ved internethandel, hvis konen er blevet snydt ved køb af et par sko på internettet. Men hvis der derimod er tale om snyd i forbindelse med køb af billetter til en koncert, som kone og mand sammen skal til, svarer begge formentligt 'ja' på spørgsmålet, om de er blevet udsat for bedrageri ved internethandel. I tabel 6.1 sættes de 2,4 procent derfor både i relation til personer og til husstande. I forbindelses med personer svarer procenttallet således til 100.000, mens det drejer sig om 62.000 husstande. Formentligt placerer det virkelige tal sig mellem disse to resultater, og dermed er et godt bud, at ca. 80.000 udsættes for bedrageri ved internethandel.

Tabel 6.1 Offerrisiko for bedrageri ved internethandel i Danmark

	Butikshandel	Privathandel	I alt
Omfang stikprøve	9.582	9.582	9.582
Antal udsatte	159	74	233
Andel af udsatte for e-bedrageri	1,7 %	0,8 %	2,4 %
95 % -interval	1,4 – 2,0 %	0,6 – 1,0 %	2,1 – 2,7 %
Antal udsatte i Danmark (personer)	70.000	30.000	100.000
Antal udsatte i Danmark (husstande)	42.000	20.000	62.000

Tabel 6.1 viser desuden, at ca. to ud af tre personer, der har oplevet bedrageri, handlede i en (falsk) internetbutik, mens en ud af tre handlede privat. Når en person snydes i forbindelse med en butikshandel, omhandler det, at varen eller ydelsen ikke leveres. Bedrageri i forbindelse med en privat

[15] Stikprøven er repræsentativ for befolkningen som helhed. Men der kan være en skævhed i bortfaldet. For at teste om der er tale om sådan en skævhed udarbejder Danmarks Statistik vægte baseret på personoplysninger. Når disse vægte anvendes stiger offerrisikoen for bedrageri ved internethandel fra 2,4 procent til 2,6 procent. På grund af denne marginale forskel gennemføres analysen uden vægte.

handel er også knyttet til dette forhold, men denne kategori inkluderer desuden, at sælgeren ikke modtager sin betaling. Ved de 74 private handler, der er registreret i undersøgelse i forbindelse med bedrageri, har 58 personer ikke modtaget varen eller ydelsen, mens 16 personer oplyser, at de ikke har modtaget betaling fra køberen.

Butikshandel

Varekategorien 'tøj, sko og smykker' placerer sig øverst på listen over produkter, som der snydes med i forbindelse med køb via (falske) internetbutikker (ifølge købernes egne oplevelser). Der er således 26 procent, der har oplevet snyd i forbindelse med køb indenfor denne varekategori, hvilket er langt over kategoriens andel i nethandelomsætningen. En anden kategori, som skiller sig negativt ud i forhold til dens andel af omsætningen, er 'kosmetik, medicin og kosttilskud'. Denne kategori står for 21 procent af bedragerierne med vare i en (falsk) internetbutik, mens dens andel af nethandelomsætningen kun udgør omkring 5 procent. Tabel 6.2 viser hele oversigten.

Tabel 6.2 Butikshandel og e-bedrageri: varekategorier

	Antal	Procentdel	Nethandel*
Tøj, sko og smykker	37	26 %	16 %
Kosmetik, medicin og kosttilskud	29	21 %	5 %
IT, tele og foto	29	21 %	13 %
Bolig, have og blomster	15	11 %	6 %
Sports- og fritidsudstyr	11	8 %	4 %
Auto-, både- og cykeludstyr	5	4 %	3 %
Film, musik, bøger, spil og legetøj	5	4 %	17 %
Rejser og kulturoplevelser	5	4 %	17 %
Elektronik og hvidevarer	4	3 %	9 %
I alt	**140**	**100 %**	

19 respondenter giver ikke (klare) oplysninger om den vare/ydelse, de er snydt for.
* FDIH handelsanalyse 2012 (FDIH 2012b, s. 17)

Privat handel

I forbindelse med handel privatpersoner imellem, hvor en af parterne udsættes for e-bedrageri, placerer varekategorien 'tøj, sko og smykker' sig også højt på listen over produkter, som der snydes med. Varekategorien 'IT, tele og foto' fører imidlertid an ved privathandel. Tabel 6.3 viser oversigten.

Tabel 6.3 Privathandel og e-bedrageri: varekategorier

	Antal	Procentdel
IT, tele og foto	19	31 %
Tøj, sko og smykker	15	24 %
Bolig, have og blomster	9	15 %
Auto-, både- og cykeludstyr	5	8 %
Rejser og kulturoplevelser	4	6 %
Sports- og fritidsudstyr	3	5 %
Film, musik, bøger, spil og legetøj	3	5 %
Kosmetik, medicin og kosttilskud	3	5 %
Elektronik og hvidevarer	1	2 %
I alt	**62**	**100 %**

12 respondenter giver ikke (klare) oplysninger om den vare/ydelse, de er snydt for.

6.3 Tab på grund af bedrageri ved internethandel

Blandt respondenterne har i alt 19 personer privat solgt noget på nettet uden at modtage betalingen. I 7 af tilfældene er der tale om mindre beløb fra 1.000 kroner eller mindre. Men, der er også respondenter, der beretter om store beløb; fx en respondent har lidt et tab på 95.000 kr. i forbindelse med et bilsalg, mens en anden respondenter har tabt 100.000 kr. til en ejendomsmægler.

De øvrige 202 respondenter, der har været udsat for e-bedrageri, har købt noget på nettet: 149 af dem i en (falsk) internetbutik og 53 hos en privat sælger. Respondenterne, der har købt hos en privat sælger, taber i 46 ud af de 53 tilfælde deres penge. Blandt respondenterne, der har købt i en (falsk) internetbutik, har flere fået dækket deres tab. Men også her hæfter flertallet selv for tabet. En respondent som tilkendegiver, at han har købt smykker for 100.000 kr., har fået dækket sit tab.

Tabel 6.4 Tabsfordeling ved e-bedrageri

	Antal ofre	Tabet (i alt)	Tabet (gennemsnit)
Butikshandel			
Købt, hæfter selv	111	174.020	1.568
Købt, tabet dækket	38	119.150	3.136
Solgt til butik	3	105.250	35.083
Butikshandel i alt	*152*	*398.420*	*2.621*
Privat handel			
Købt, hæfter selv	46	203.850	4.432
Købt, tabet dækket	7	46.099	6.586
Solgt på nettet	16	131.120	8.195
Privat handel i alt	*69*	*381.069*	*5.523*
I alt	**221**	**779.489**	**3.527**

12 respondenter oplyser ikke deres tab i offerundersøgelsen

Tabel 6.4 viser, at det samlede tab ligger på 779.489 kr. Det svarer til et gennemsnit på 3.527 kr. Det gennemsnitlige tab ved butikshandel ligger på et lavere beløb (2.621 kr.) end ved handel mellem private personer (5.523 kr.). Det gennemsnitlige beløb er dog 'kunstigt' højt på grund af enkelte store beløb. I mere end halvdelen af e-bedrageri sagerne er tabsbeløbet under 1.000 kr. Det mediane tab ligger ved 800 kroner. Tabel 6.5 viser oversigten.

Tabel 6.5 Tabsbeløb ved e-bedrageri

	Butikshandel	Privat handel	I alt
Under 1.000 kr.	91	27	118
1.000 – 4.999 kr.	46	28	74
5.000 – 9.999 kr.	7	7	14
10.000 kr. eller mere	8	7	15
I alt	**152**	**69**	**221**

12 respondenter oplyser ikke deres tab i offerundersøgelsen

6.4 Offerprofil i forbindelse med bedrageri ved internethandel

Offerundersøgelsen viser, at risikoen for at blive udsat for bedrageri ved internethandel hænger sammen med alder. Ældre danskere har således en mindre risiko for at blive udsat herfor. Dette hænger formentligt sammen med, at ældre mindre hyppigt køber varer og ydelser på internettet. Der er ingen forskel i offerrisikoen for mænd og kvinder, når alderen ikke tages med i betragtning. Men når sammenhængen mellem offerrisiko, køn og alder undersøges, ses det, at offerrisikoen for kvinder under 50 år er større sammenlignet med jævnaldrene mænd. Det forholder sig omvendt for dem over 50 år. Tabel 6.6 viser, at kvinder under 30 år er den gruppe, som har den største offerrisiko for bedrageri ved internethandel.

Tabel 6.6 Offerrisiko for e-bedrageri efter køn og alder

	Mand	Kvinde	I alt
Under 30 år	3,5 %	4,5 %	4,0 %
30 – 49 år	2,7 %	3,4 %	3,1 %
50 år og ældre	1,7 %	1,1 %	1,4 %
I alt	**2,4 %**	**2,5 %**	**2,4 %**

Note: Antal ofre er 233, og stikprøven omfatter 9.582 respondenter.

Offerrisikoen for at blive udsat for bedrageri ved internethandel afhænger af respondenternes uddannelsesniveau. Men der er ingen klar tendens. Det hænger således ikke sådan sammen, at jo lavere uddannelse, desto højere risiko, eller omvendt. Men dem, der har afrundet en erhvervsfaglig uddannelse, har den laveste offerrisiko. I tabel 6.7 kan oversigten ses.

Tabel 6.7 Offerrisiko for e-bedrageri efter højest afsluttede uddannelse

	Antal ofre	Antal respondenten	Offerrisiko
Folkeskolen	45	1.899	2,4 %
Gymnasium	33	876	3,8 %
Erhvervsfaglig uddannelse	53	2.959	1,8 %
Kortere videregående uddannelse	22	646	3,4 %
Mellemlang videregående uddannelse	44	1.915	2,3 %
Lang videregående uddannelse	33	1.033	3,2 %
Andet	3	254	1,2 %
I alt	**233**	**9.582**	**2,4 %**

Risikoen for at blive udsat for bedrageri ved internethandel afhænger desuden af ens erhverv, og i forbindelse hermed er mønsteret mere klart. Pensionister har således den laveste offerrisiko, hvilket utvivlsomt hænger sammen med deres alder og mindre færden på internettet (se også figur 6.1). I modsætning hertil har studerende - den yngste erhvervsgruppe - og selvstændige den højeste offerrisiko. Der er en fare for, at de selvstændige blander deres erhvervsmæssige internetkøb sammen med deres private, når de svarer på spørgsmålene vedrørende bedrageri ved internethandel.

Tabel 6.8 Offerrisiko for bedrageri ved internethandel efter erhverv

	Antal ofre	Antal respondenten	Offerrisiko
Funktionær	85	3.222	2,6 %
Arbejder	29	1.657	1,8 %
Selvstændig	23	582	4,0 %
Uden arbejde	27	907	3,0 %
Studerende	51	1.286	4,0 %
Pensionist	18	1.928	0,9 %
I alt	**233**	**9.582**	**2,4 %**

Note: Kategorien 'uden arbejde' omfatter også førtidspensionister, mens efterlønsmodtagere hører til kategorien pensionister.

6.5 Gerningsmandsprofil af bedragere ved internethandel

I datafilen fra Rigspolitiet fremgår det, at i forbindelse med sagerne i perioden 2010-2012 hvor en er sigtet for bedrageri ved internethandel, har forurettede oftest betalt for en bestilling uden at få leveret varen. I de fleste sager er der tale om private handler gennem dba.dk, og det er typisk mobiler (iPhone) eller andet IT-udstyr, som er forsøgt handlet.

I perioden 2010-2012 er der sigtet 53 unikke personer i Danmark for bedrageri ved internethandel. De fleste (60 procent) er i alderen 15-24 år. To tredjedel af bedragerne er mænd, mens en tredjedel er kvinder. Blandt de sigtede over 25 år er andelen af kvinder mindre, nemlig 1 ud af 7 (14 procent).

Tabel 6.9 viser oversigten. På nær et tilfælde er alle sigtede bedragere ved internethandel af dansk nationalitet.

Tabel 6.9 Aldersfordeling blandt sigtede bedragere ved internethandel (2010-2012)

	Mænd	Kvinder	I alt	Procentdel
15-24 år	21	11	32	60 %
25-34 år	12	1	13	31 %
35-44 år	5	2	7	24 %
45-54 år	1	-	1	7 %
I alt	**39**	**14**	**53**	**100 %**

Kriminel løbebane

Blandt af de 53, som sigtes for e-bedrageri i perioden 2010-2012, er 39 også sigtede for en eller flere lovovertrædelser i perioden 2001-2009. Det svarer til en recidivprocent på 74. Ca. en tredjedel af recidivister sigtes en eller to gange i denne periode, mens to tredjedel af recidivister tegner sig for tre eller flere sigtelser i perioden 2001-2009.

Tabel 6.10 Antal sigtelser for lovovertrædelser i perioden 2001-2009

	Antal personer	Også ligeartet
Ingen sigtelser	14	
1 sigtelse	6	1
2 sigtelser	8	-
3-10 sigtelser	11	1
Mere end 10 sigtelser	14	7
I alt	**53**	**9**

9 ud af de 39 recidivister har begået ligeartet kriminalitet i perioden 2001-2009 (se også afsnit 1.4.5), og 7 af dem falder i kategorien 'meget kriminel aktiv' (mere end 10 sigtelser). Blandt disse er en 29-årig mand fra Randers, og han har i perioden været den mest kriminelle aktive. I perioden 2001-2009 er han således sigtet 216 gange. I 2011 sigtes han igen for at ville sælge en Playstation 3 gennem Den Blå Avis. Den 18-årige forurettede betaler, men modtager aldrig varen. Det samme oplever en 30-årig mand, der betaler 3.200 kr. for en iPad3 til en person, der annoncerer på Den Blå Avis. Det viser sig at være en 25-årig mand fra Nivå, som har været sigtet 57 gange i perioden 2001-2009.

Der er en sammenhæng mellem recidiv og alder. De yngre bedragere er således mindre hyppigt sigtede i perioden 2001-2009, hvilket også måtte forventes. De ældre bedrageres recidivprocent er på 100.

Tabel 6.11 Recidiv og alder

	Antal sigtede	Antal recidivister	Andel recidivister
15-24 år	32	20	63 %
25-34 år	13	11	85 %
35-44 år	7	7	100 %
45-54 år	1	1	100 %
I alt	**53**	**39**	**74 %**

7 Forebyggelse og overvågning

7.1 Sikring af computere

En søgning på internettet på forholdsregler i forbindelse med internetsikkerhed giver mange resultater, og det er både myndigheder og private aktører (sikkerhedsfirmaer), som står bag de sider, der henvises til ved søgningen. Bl.a. skriver Det Kriminalpræventive Råd på deres internetside ti gode råd til at undgå identitetstyveri. Disse færdselsregler for sikker trafik på internettet er udarbejdet i samarbejde med Rigspolitiet og Digitaliseringsstyrelsen. Rådene retter sig på den ene side mod teknisk sikring af computeren, såsom opdatering af programmer, brug af antivirusprogram og firewall, kryptering af det trådløse netværk, brug af passwords og sikring af bærbare enheder. På den anden side understreges vigtigheden af forsvarlig adfærd på nettet. Folk rådes således til at være tilbageholdende med at videregive personlige oplysninger på mail, sociale medier, internetsider og så videre. Den tekniske sikring retter sig mod at undgå malware, mens den varsomme adfærd retter sig mod at hindre phishing.

Selvom råd magen til de, der optræder på Det Kriminalpræventive Råds internetside, er tilgængelige flere steder, findes der mange private computere, som ikke er optimalt sikrede. Myndighederne er dog nu så småt begyndt at hjælpe borgerne med at opdatere deres softwareprogrammer. Når man logger ind med NemID på Skats hjemmeside, og den nyeste version af Java ikke er installeret på computeren, kræves en opdatering, før man kan gennemføre login-processen. Det samme gælder for virk.dk fra Digitaliseringsstyrelsen.

Det er ikke til at sige nøjagtigt hvor mange (danske) computere, der er inficerede med malware. Sikkerhedsfirmaet CSIS anslår, at 80.000 danske computere er smittet i 2012. CSIS overvåger spionsoftware, og når en inficeret computer melder tilbage til en server (i udlandet), registreres kontakten. I interviewet med lederen af NITES udtrykkes skepsis over for dette tal. Han påpeger, at ingen ved hvor mange inficerede computer, der findes i Danmark, man at sikkerhedsfirmaer har en kommerciel interesse i at understrege problematikken. Der er dog ingen tvivl om, at en del af de danske computere er inficerede med malware.

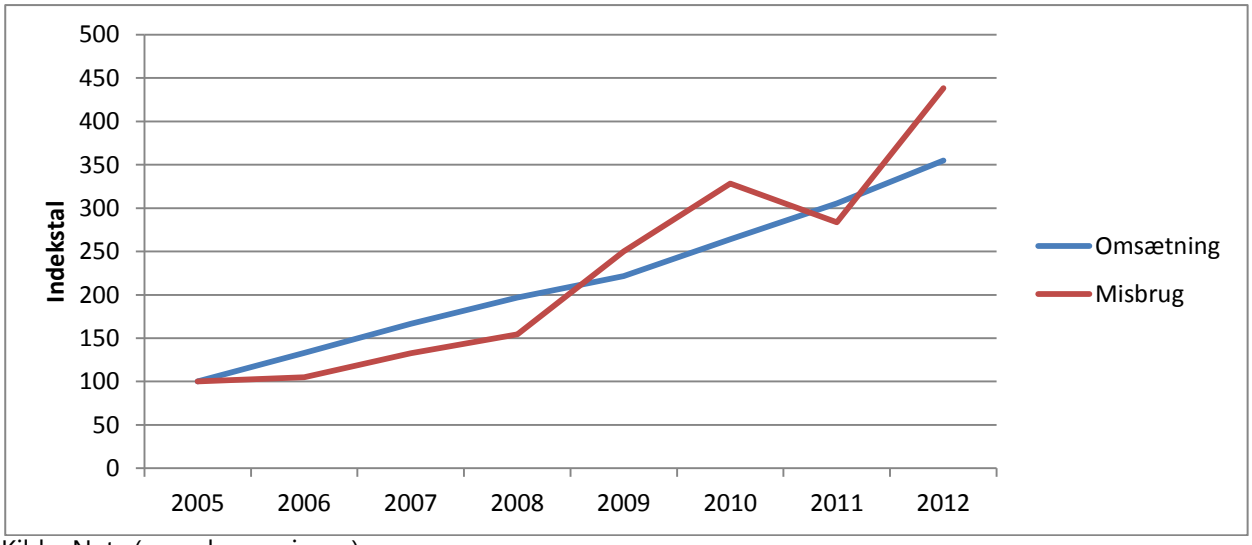
7.2 Betalingskortsikring

Misbrug af Dankort på nettet kan ske, når gerningspersonen har oplysninger vedrørende kortnummer, udløbsdato og kontrolcifre. Visa og Mastercard har introduceret den såkaldte 3D Secure:

Udover kortnummer, udløbsdato og kontrolcifre skal betaleren indtaste en selvoprettet kode, før betalingen gennemføres. Det er op til den enkelte internetforretning, om de vil anvende den ekstra sikring. Langt de fleste danske internetforretninger vælger denne løsning fra. Grunden hertil er, at forretningerne vægter brugervenligheden højere end sikkerheden. De vil hellere tage et eventuelt tab på grund af kortmisbrug end at 'skræmme' kunderne væk. Ifølge interviewrespondenten fra Nets overvejes det – nu hvor NemID mere eller mindre er udrullet i Danmark – at benytte dette instrument i forbindelse med Dankort-internetbetaling.[16] Herved lægges en ekstra teknisk hindring, før misbrug kan finde sted. Et tidligere initiativ til at gøre internethandel mere sikker, e-dankortet, bliver dog aldrig en succes. Med e-dankortet betales der over netbank i stedet for betalingskort. Danske forretninger afviser i stor stil denne form for internetbetaling, igen på grund af manglende brugervenlighed.

I den kriminologiske litteratur peges der ofte på den begrænsede levetid for præventive tiltag (se fx Graham, 1990). Det ligner et kapløb mellem kriminelle, der forsøger at uskadeliggøre tiltagene, og samfundet/virksomhederne, som arbejder på at finde nye forhindringer. Et andet kendt kriminologisk fænomen er forskydning (se fx Reppetto, 1976). Ideen bag denne teori er, at præventive forhindringer for en slags kriminalitet gør, at kriminelle søger lykken i andre retninger. Begge fænomener – uskadeliggørelse og forskydning – gør sig gældende inden for kortsvindel. Men i det lange løb holder finanssektoren og kortsvindlerne hinanden mere eller mindre i skak, når forholdet mellem udviklingen af henholdsvis omsætning og misbrug af Dankort betragtes som målestok (se figur 7.1).

Figur 7.1 Indekseret udvikling af omsætning og misbrug af Visa/Dankort ved internethandel i Danmark (2005 = indeks 100)



Kilde: Nets (egne beregninger)

[16] Interviewet finder sted i slutningen af 2012. NemID nedlægges fra d. 24. til d. 25 marts og igen i starten af april 2013 af et DDoS-angreb.

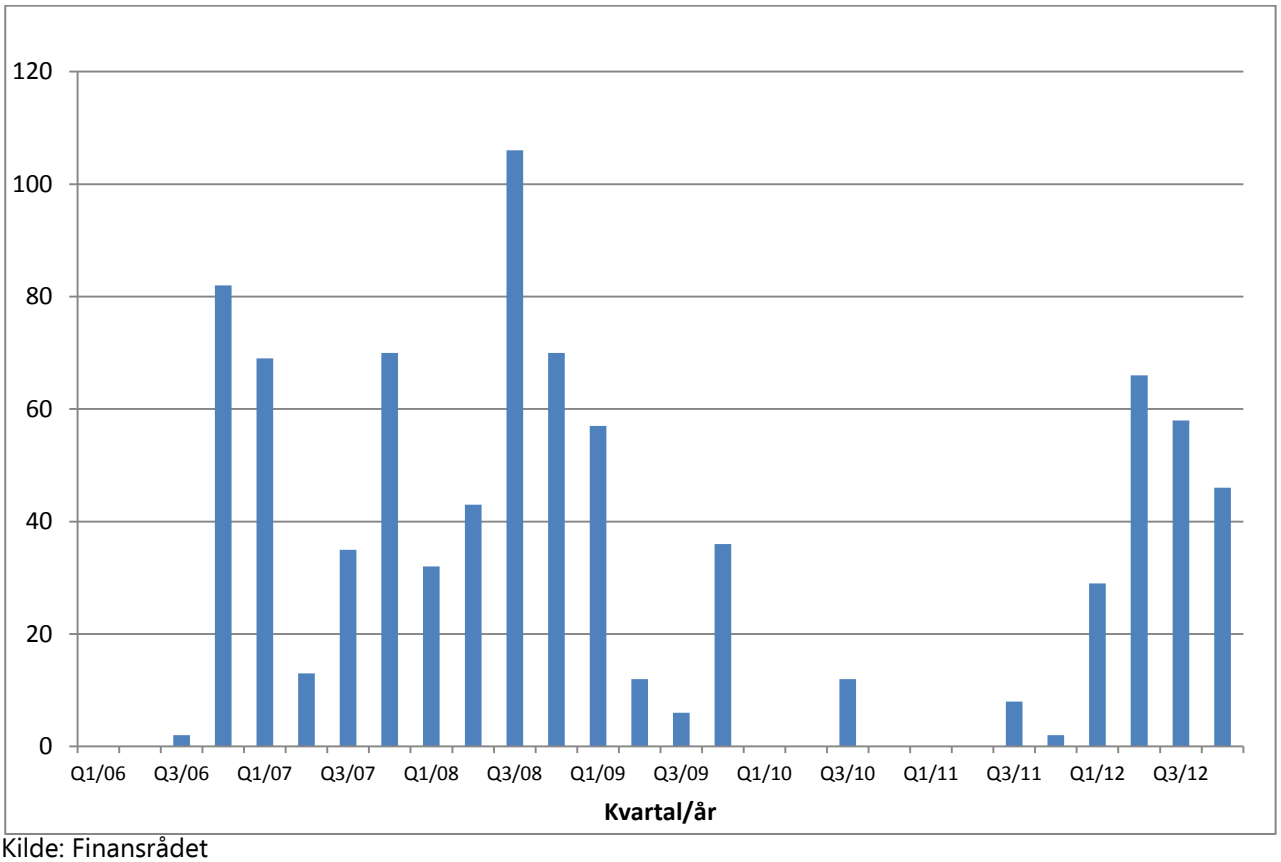
7.3 NemID som to-trins sikring

NemID introduceres d. 1. juli 2010 og er Danmarks digitale signatur. Den gælder ikke kun, når der skal opnås adgang til netbank, men også til offentlige services, fx Skat. Videnskabsminister Charlotte Sahl-Madsen udtaler ved introduktionen af NemID:

> For 42 år siden fik vi CPR-nummer. For 25 år siden fik vi Dankort. I dag, den 1. juli 2010, tager vi næste skridt op af stigen mod et fuldt digitaliseret Danmark. I dag får vi NemID.

Den afgørende forskel mellem NemID og den tidligere opkobling[17] til netbank er nøglekortet eller nøgleviseren. Hver gang en kunde logger ind på sin netbank kræves en unik sekscifret nøgle, som aflæses på kortet/viseren. Dermed er der lagt en væsentlig ekstra teknisk forhindring til at forebygge netbankindbrud.

Figur 7.2 Antal netbankindbrud (inkl. forsøg) pr. kvartal i perioden 2006-2012



Kilde: Finansrådet

[17] Før introduktionen af NemID krævede adgang til netbank en logfil på computeren samt brugernavn og password. Adgang til computeren og afluring af id-oplysninger var således nok for it-kriminelle til at kunne begå netbankindbrud.

Figur 7.2 viser udvikling i netbankindbrud pr. kvartal i perioden 2006 til 2012. Ved første øjekast ser det ud til, at introduktionen af NemID har en positiv effekt. Men ses der lidt nærmere efter, opdages det, at antallet af netbankindbrud allerede falder til nul i det første halvår af 2010 – perioden umiddelbart før introduktionen af NemID. Interviewrespondenten fra Finansrådet forklarer:

> I 2010 er der et meget lille tab, men det er faktisk først i løbet af 2010, at NemID er introduceret. Hvad der faktisk er sket er, at man i løbet af 2009 lukkede nogle dataservere ned, som hackere brugte ret aktivt. Det var det, der gav effekten.

Dermed ikke sagt, at NemID ikke gør det mere besværligt for it-kriminelle at begå netbankindbrud i Danmark. Men som allerede påpeget vender kurven i løbet af 2012. Via specifikke malware kan it-kriminelle nemlig franarre en bankkunde sin NemID nøgle. Det kaldes *real time phishing* og finder sted, mens kunden er logget på sin netbank. Denne handling kræver, at:

- bankkundens computer er inficeret med malware;
- bankkunden er logget ind på sin netbank;
- hackeren observerer, at kunden er logget ind på sin netbank;
- bankkunden afgiver en ny NemID nøgle.

Kunden lokkes til at afgive en ny NemID nøgle ved, at der eksempelvis simuleres en teknisk fejl på netbanken. Denne fejl sker i realiteten også, men det er ikke banken, der beder om, at der indtastes en ny nøgle.

7.4 Overvågning af finansielle transaktioner

Sikring af netbank sker ikke kun ved at sikre adgangen, men også ved overvågning af betalinger. Overvågning finder sted ved bankernes datacentraler. Danske Bank og Nordea har hver deres datacentral, mens landets andre banker er slået sammen i tre datacentraler:

- Bankdata i Fredericia
- BEC (Bankernes EDB Central) i Roskilde
- SDC (Skandinavisk Data Center) i Ballerup

Disse datacentraler dannes i 1960'erne, og ved de tre fælles datacentraler arbejder der ca. 500 medarbejder pr. central. Datacentralerne kan spotte et formentligt netbankindbrud ved, at der sker en usandsynlig overførsel, eller deres opmærksomhed vækkes på anden vis. I forbindelse med netbankindbrud overføres penge typisk til udlandet. Ifølge interviewrespondenten fra Finansrådet sker overførslen sjældent – som man ellers skulle forvente – til et fjernt land, men derimod til fx England. Når der er tale om en pengeoverførsel til udlandet, sker den reelt set ikke med det samme,

der er en såkaldt clearingsperiode – typisk på et par timer. Datacentralerne har dermed et par timer til at stoppe pengeoverførslen. Tal fra Finansrådet (se tabel 3.10) viser, at det lykkes datacentralerne at stoppe pengeoverførslen i clearingsperioden i forbindelse med mere end halvdelen af netbank-indbruddene.

Alle fem datacentraler er med i et IT-sikkerhedsforum under Finansrådet. Dette forum mødes en gang i kvartalet, medmindre der er nye træk fra hackernes side, fx ny malware. I så fald indkaldes til møde for at dele viden med de andre aktører. For at finde ud af hvilke malware, der bruges ved netbankindbrud, spørges de udsatte, om de vil udlevere deres computer. Computeren undersøges efterfølgende for malware af CSIS, der er et IT-sikkerhedsfirma.

Nets fungerer som indløser af (Visa/)Dankort. De sørger således for, at betalingen overføres fra køberens konto til forretningens konto. Dermed er Nets den mest centrale aktør i forbindelse med overvågningen af Dankortbetalinger, og overvågningen sker ved Nets' datacentral i Ballerup. Idéen bag overvågningen er at spotte unormale betalingsmønstre, og kriterierne herfor er erfarings-baserede og justeres løbende. Det kan fx være en såkaldt hurtigløbsovervågning: Et kort brugs inden for en (meget) kort tidsperiode ved kortudstedernes egen bank, en anden bank, og der købes også for op til 4.000 kr. i en butik. I sådan et tilfælde spærres kortet præventivt. Der kan også ske præventiv spærring, når et kort bruges i en periode, hvori en hæveautomat udsættes for skimming. Nets forsøger at finde den rette balance ved præventiv spærring og unødvendige gener for kunderne. Når et kort spærres præventivt, kontakter Nets banken, som efterfølgende informerer deres kunde. Specielt når spærringen foregår i udlandet, kan det være generende, hvis det senere viser sig, at spærringen er unødvendig. Nets kan ikke sætte tal på antallet af (unødvendige) præventive spærringer af (Visa/)Dankortet.

7.5 Forebyggende tiltag under opsejling

Præventive tiltag justeres løbende i takt med kriminalitetens udvikling. Herunder beskrives enkelte tiltag, som er under opsejling ifølge de forskellige interviewrespondenter.

Netbankindbrud

Ved netbankindbrud overføres pengene som regel til udlandet. Denne viden anvender Nordea allerede i sikringen af deres netbanksløsning ved at spørge om en ekstra godkendelse fra kunden i forbindelse med en overførsel til udlandet. Nordea sender således en sms til kunden for bekræftelse af ordren. Der kan tænkes flere tekniske forhindringer. Men der er en væsentlig balancegang mellem sikkerhed på den ene side og brugervenlighed på den anden, ifølge interviewrespondenten fra Finansrådet. Et begrænset antal netbankindbrud skader ikke meget. Det er dog vigtigt for bankerne, at danskerne har tillid til netbankssystemet, da hele bankkonceptet i højere og højere grad bygger på betjening over nettet - med lukning af filialer til følge. Indtil videre sker netbankindbrud

kun gennem traditionelle computere, men det må antages, at mobilbanken (smartphone eller tablet) også benyttes hertil i den nære fremtid.

Dankortsikring

Betaling med kort skal på den ene side være nemt og hurtigt og på den anden side sikkert. Det betyder i praksis en konstant proces af tilpasning. Interviewrespondenten fra Nets forventer, at der på sigt skrues ned for sikkerheden ved 'små betalinger'. I dag skal der fx kun indføres kort ved betaling i forbindelse med Storebæltsbroen og parkeringsautomaterne i København, pinkoden skal ikke indtastes. Det går hurtigere og er nemmere. Det kan tænkes, at små betalinger i butikker også kommer til at foregå på denne måde i fremtiden. Muligvis erstattes dankortterminalen af et scanningsapparat, som vi kender det fra fx rejsekortet. Interviewrespondenten fra Nets forventer samtidig, at der skrues op for sikkerheden, når det gælder internethandel: Indtastning af en NemID-kode som 3D Secure løsning for Dankortet. Desuden begrænses anvendelsen af betalingskort muligvis i lande uden for EU for at komme skimming til livs. Han forestiller sig ikke – på kort sigt – at betalingskort udstyres med biometriske kendetegn. Derimod er der flere og flere virksomheder, der udstyrer deres kunder med en personlig kode, hvilket betyder, at kreditkortoplysninger kun behøves oplyst en enkelt gang. Eksempler herpå er Apples AppStore og en konto på Skype. Denne betalingsmetode anvendes formentlig oftere i fremtiden.

8 Anmeldelse, efterforskning og strafudmåling

8.1 Politiets anmeldelsesstatistik

Politiets sagsstyringssystem – Polsas – bruger gerningskoder, som er inspireret af straffeloven. Det kan derfor være svært at genkende nye kriminalitetsfænomener. I Danmark er der ikke tradition for at have specielle straffebestemmelser for forbrydelser, der begås ved hjælp af tekniske indretninger – det gælder telefonen, men også computeren (Bagger Tranberg & Langsted, 2012). Der er imidlertid undtagelser. I 1985 indføres straffebestemmelsen om databedrageri (straffelovens § 279a), da almindeligt bedrageri kræver, at nogen lider under en 'vildfarelse'. Ifølge lovgiveren kan det ikke være en maskine, der står bag denne. Hvis et offer derimod narres med en løgnehistorie i en e-mail, dømmes dette som traditionelt bedrageri efter straffelovens § 279. Det samme gælder for trusler på internettet (§ 266) og børnepornografi på internettet (§ 235).

I dette afsnit ses der nærmere på, hvordan og hvor ofte politiet registrerer angreb på og uberettiget adgang til computere samt betalingskortmisbrug.

Hacking

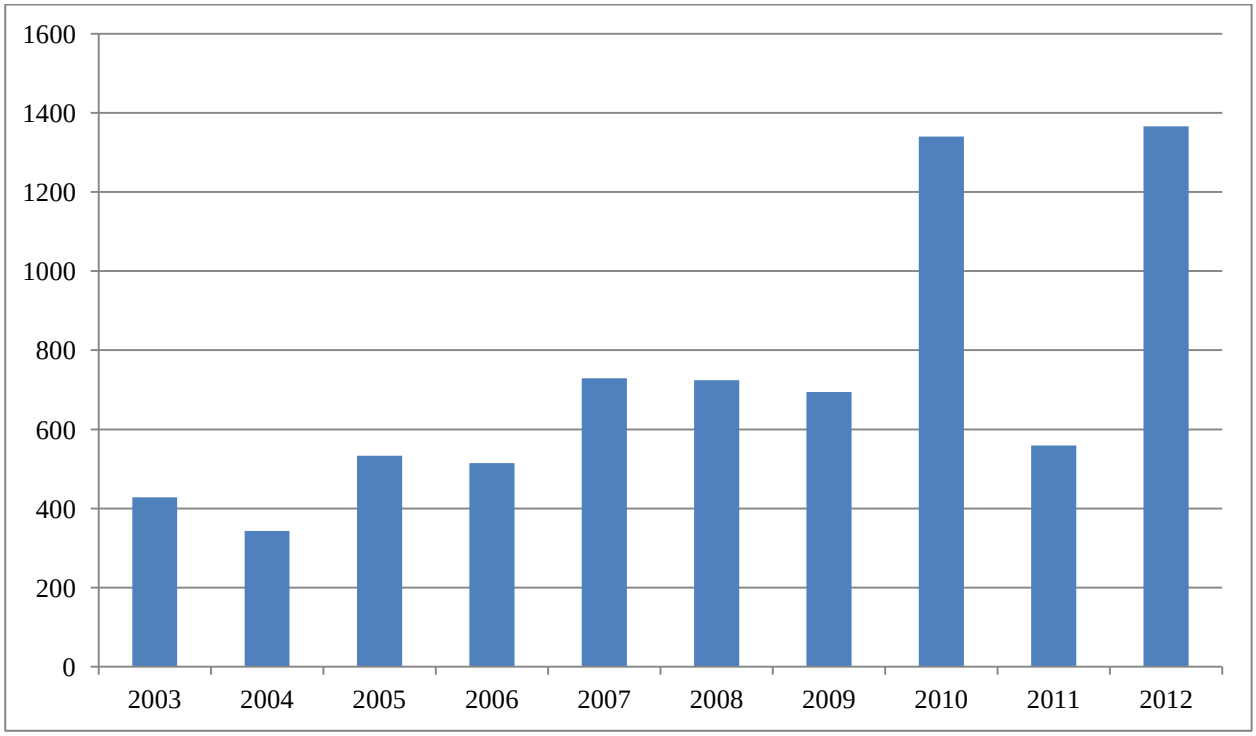
Uberettiget adgang til computere og informationssystemer er kendt under begrebet hacking og er kriminaliseret i straffelovens § 263, stk. 2: "Den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem, straffes med bøde eller fængsel i indtil 1 år og 6 måneder". Ifølge politiets kriminalstatistik anmeldes 40-50 sager vedr. hacking om året. Politiets anmeldelsesstatistik afspejler imidlertid ikke det reelle niveau. Ifølge respondenten fra politiet optages altid en anmeldelse, når en borger eller virksomhed henvender sig, men det er sjældent, at politiet modtager anmeldelser vedrørende hacking. De forurettede er nemlig langt fra altid klar over, at deres computer er hacket, og hvis de oplever problemer, så klarer de dem enten selv, eller de henvender sig til et computerfirma. Desuden anmelder virksomheder også sjældent hacking til politiet. En vigtig forklaring herpå er, at de ofte gerne vil undgå negativ omtale.

Databedrageri

Som beskrevet indledningsvis i dette afsnit knytter bedrageri på internettet sig til den almene bedrageribestemmelse (§ 279), men også databedrageri (§ 279a). Phishing, skimming, misbrug af betalingskort på nettet og netbankindbrud er forbrydelser, som typisk hører hjemme under databedrageri. Figur 8.1 viser udviklingen i disse anmeldelser. Som det ses er antallet af anmeldelser sti-

gende i perioden fra 2003 til 2012. Året 2011 adskiller sig dog fra tendensen, jeg er ikke bekendt med forklaringen på det lave antal anmeldelser.

Figur 8.1 Antal af politianmeldte databedragerisager (2003-2012)



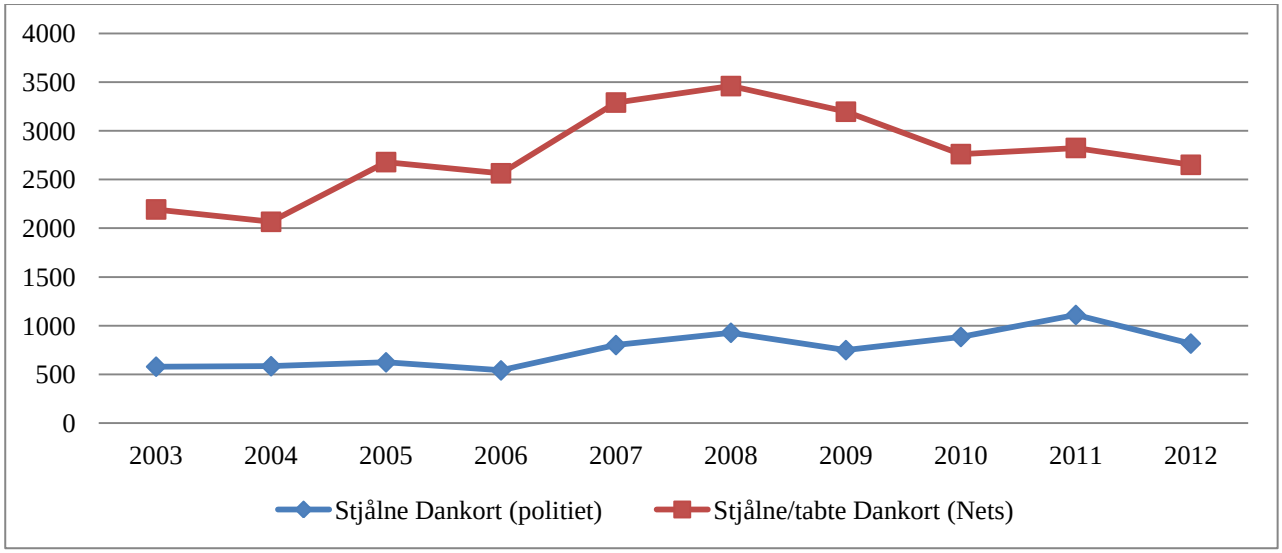
Kilde: Danmarks Statistik/ Rigspolitiet

Bankernes politik er, at netbankindbrud anmeldes til politiet. Anmeldelsen sker til det lokale politi, og Finansrådet anbefaler, at Rigspolitiets IT-specialister (NITES) informeres samtidig. Ifølge interviewrespondenten fra Finansrådet er bankerne ikke altid lige gode til at anmelde netbankindbrud til politiet. Forventningerne til politiets efterforskning er nemlig ikke store. Det formodes, at ansatte i politikredsene som oftest ikke har nok kendskab til den digitale verden til at efterforske sager knyttet hertil. Efterforskere fra NITES er, ifølge respondenten fra Finansrådet, bedre gearet til sådanne opgaver. Men de har begrænset kapacitet, hvorfor det kun er, hvis der sker noget usædvanligt, at de tropper op, fx da NemID'et var 'knækket' i starten af 2012.

Betalingskortmisbrug

Det afhænger af forbrydelsen, hvem der anmelder betalingskortmisbrug til politiet. Når der er tale om tyveri af betalingskort, så er det i princippet kortindehaveren, der anmelder tyveriet. Figur 8.2 viser, at der findes langt flere misbrugssager med stjålne Dankort i Nets' statistik end i politiets anmeldelsesstatistik. Det skyldes (delvist), at politiet både registrerer et stjålent Dankort under tyveri, men også under betegnelsen bedrageri. En anden forklaring på forskellen mellem Nets' og politiets tal er, at en anmeldelse til politiet kan indeholde flere tabte kontooplysninger.

Figur 8.2 Antal af anmeldte bedragerisager med stjålne Dankort (politiet vs. Nets)

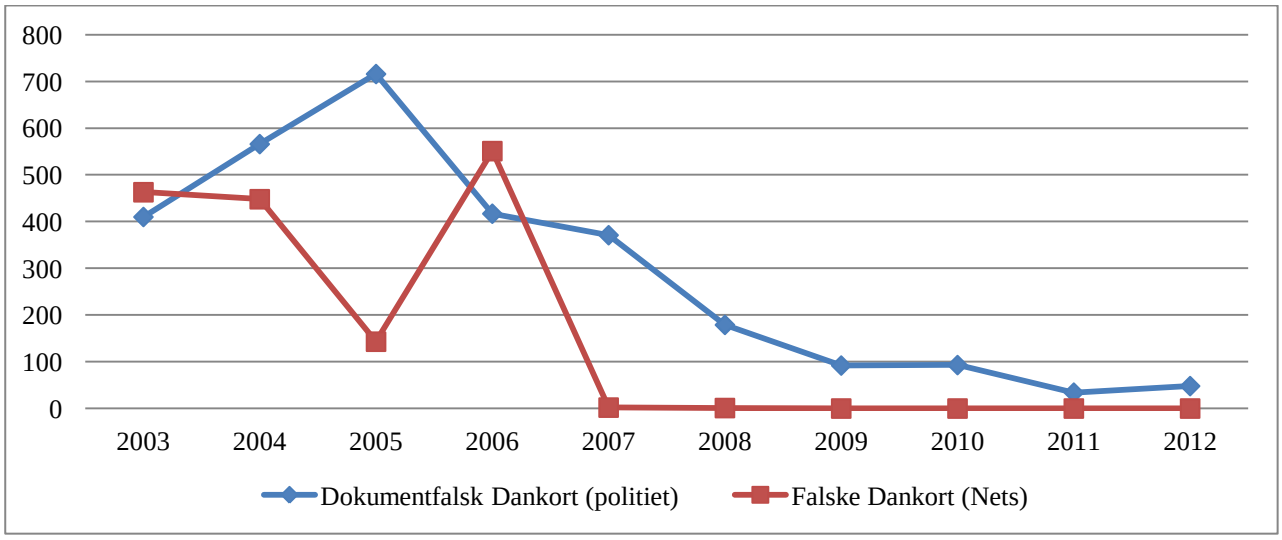


Kilde: Danmarks Statistik/Rigspolitiet og Nets

Når der er tale om skimming, er det typisk Nets, der anmelder sagen til politiet. Nets står nemlig oftest for anmeldelsen, når der er tale om en række af sager. Men det kan også være banken, der står for anmeldelsen. Dette sker oftest i forbindelse med enkelte sager. Både Nets og den respektive bank anmelder til den politikreds, hvori skimmingen finder sted.

Når et falsk Dankort anvendes, er der tale om dokumentfalsk (straffelovens § 171). Her stemmer politiets statistik heller ikke overens med opgørelsen fra Nets. En forklaring herpå kan være, at politiet muligvis anser det som dokumentfalsk, når et skimmet Visa/Dankorts Visa-del anvendes i udlandet. Dette kan forklare, at der ifølge politiets statistik stadig sker anmeldelse af dokumentfalsk med Dankort, selvom disse sager ikke forekommer længere på grund af chippen.

Figur 8.3 Antal af anmeldte dokumentfalsksager Dankort (politiet vs. Nets)



Kilde: Danmarks Statistik/Rigspolitiet og Nets

8.2 Politiets efterforskning

Når politiet modtager en anmeldelse vedrørende IT-kriminalitet, er det langt fra sikkert, at sagen efterforskes. "Der skal prioriteres" er en sætning, der ofte høres fra politifolk, og også – eller måske specielt – i forbindelse med efterforskning af IT-kriminalitet. Hvis der ikke lides tab, er det usandsynligt, at sagen efterforskes. Det kræver nemlig spejling af den hackede computer, og det er for meget arbejde i en sag, hvor tabet er ringe eller slet ikke findes. Den interviewede politimand fortæller, at jo større tabet er, desto større er sandsynligheden for, at en sag efterforskes. Desuden efterforskes sager også oftere, hvis de er led i en serie af forbrydelser. Politiet modtager imidlertid gerne privatpersoners og virksomheders anmeldelse, så de kan danne sig et indtryk af (omfanget af) IT-kriminalitet.

Politiets efterforskningsberedskab i forbindelse med internetkriminalitet består af tre lage. Det første lag er den almene betjent. Efterforskning af IT-kriminalitet er en integreret del af politiuddannelse, og specielt de yngre betjente har solid basisviden herom ifølge interviewrespondenten fra NITES. Det andet lag er den pågældende politikreds' IT-koordinatorer. Hver politikreds har et par koordinatorer, der findes således i alt ca. 45 i Danmark. IT-koordinatorerne gennemfører en uddannelse, der er udviklet af NITES's medarbejdere, som også står for undervisningen. I princippet anmeldes og efterforskes en internetforbrydelse i politikredsen, men det er muligt at benytte specialiseret viden. NITES er således det tredje lag. NITES er en del af Rigspolitiet og står for National IT-efterforskningssektion. Der arbejder godt 60 personer ved NITES, og ca. 50 af disse er politiuddannede efterforskere med efteruddannelse i datalogi eller computervidenskab (ofte i udlandet). Det betyder, at der findes ca. 100 politiuddannede medarbejdere ved Dansk Politi, som har en mere specialiseret viden om efterforskning af internetkriminalitet (koordinatorer og NITES-ansatte). Dette svarer til ca. 1 procent af politiets styrke.

Digitale spor, muldyr og bagmænd

Internetkriminelle efterlader digitale spor, og disse kan bruges i efterforskningen. Det kan dog besværliggøre efterforskningen, hvis den kriminelle handling udføres i udlandet. Men i princippet er det muligt at spore computeren, som anvendes af gerningspersonen (IP-adressen), medmindre vedkommende anvender et botnet til at gennemføre et DDoS-angreb. I sådanne tilfælde kommer angrebet fra hundrede eller tusinde computere.

Når en computer identificeres er det imidlertid langt fra sikkert, at denne tilhører gerningspersonen. I tilfælde af berigelseskriminalitet – fokusområdet for denne rapport – er der et ekstra efterforskningsspor: Penge (ved et netbankindbrud) eller varer (ved e-bedrageri) sendes nemlig til henholdsvis et kontonummer eller en adresse.

Når penge overføres eller forsøges overført ved et netbankindbrud, må der være et kendt kontonummer, hvor de sluses hen. Kontoen tilhører oftest et såkaldt muldyr. På Finansrådets hjemmeside kan der læses følgende om muldyr:

> Muldyr bliver typisk rekrutteret igennem en spammail-kampagne med et 'jobopslag'. Rekrutteringsforsøget kan være på dansk eller engelsk. Nogle er meget professionelt udført, andre ganske ubehjælpsomme. Jobopslaget kan være kamufleret under overskrifter som 'finansielle assistenter søges', 'hjemmearbejde', 'part-time job' og 'local representation needed for International Company'. Reagerer man på rekrutteringsforsøget viser det sig, at hovedindholdet i jobbet er, at man skal være behjælpelig med at modtage penge og videresende pengene. Som betaling får man ofte en andel på 5-15 procent.

Nets peger på, at internetkriminelle også bruger muldyr for at sikre sig en måde at modtage varer købt med stjålne betalingskortoplysninger:

> Stadig flere danskere lader sig lokke til at være "muldyr" for internationale kriminelle bander, der præsenterer sig som professionelle transportfirmaer. Banderne kontakter typisk private danskere via e-mail og tilbyder dem at tjene en ekstra skilling ved at tage imod og videresende pakkepost med varer købt i danske internetforretninger. Efterhånden foregår svindlen med alle typer varer, svindlerne kan videresende. Nets har i den senere tid registreret en stigning i antallet af sager om danske "muldyr" for udenlandske kriminelle. Det er mest populært at svindle sig til varekategorier, der har en høj værdi ved videresalg. Det er derfor først og fremmest dyre mærkevarer, mobiltelefoner, kameraer og anden forbrugerelektronik. Men svindlen har grebet om sig og andre varekategorier er blevet interessante for svindlerne.

Desuden peger Europol (2011a) på muldyr, som den synlige del af netværket:

> Mules are recruited via employment search websites and social networking sites to help cash in stolen personal and financial information. As the individuals tasked with turning data in hard cash, mules are the visible face of cybercrime.

Muldyr kan spores, men det er tvivlsomt, hvorvidt det altid sker i praksis. Interviewrespondenten fra NITES fastslår, at politiet i princippet går efter muldyr i Danmark men tilføjer, at der ikke ses ret mange muldyr i Danmark for tiden. Når muldyr opholder sig i udlandet – hovedsagelig i England eller Tyskland – informerer politiet deres udenlandske kolleger, men der anmodes sjældent om bistand.

Hvem der står bag internetkriminalitet er mindre synligt. Ifølge interviewrespondenten fra Finansrådet er der tale om en arbejdsdeling mellem dem der *udvikler* malware, og dem der *anvender*

malware til at fiske efter oplysninger for at få adgang til en given netbank. Dette synspunkt bakkes op af litteraturen (fx Smith, 2010). Smith taler således om en digital undergrundsøkonomi, hvor der kan købes malware, bankkontooplysninger og adgang til botnet. Bankkontooplysninger kan købes for 10 – 125 US dollars ifølge Europol (2011a), og Europol karakteriserer den digitale undergrundsøkonomi (digital underground economy) på følgende vis:

> All of this stolen data is retailed in the criminal underworld, which is driving a range of new illegal activities, including crimeware distribution and the hacking of corporate databases. This is backed up by a fully–fledged infrastructure of malicious code writers and hackers, specialist web hosts and leased networks of thousands of compromised computers which carry out automated attacks online, to access and steal personal data. As this underground economy has grown in sophistication, 'service providers' have also emerged who offer payment card verification number generators.

Europol vurderer, at personer der står bag internetkriminalitet er unge (oftest under 25 år) med mange IT-kvalifikationer (oftest universitetsuddannede). Dette er en anderledes profil end den, der knytter sig til folkene bag andre former for grænseoverskridende kriminalitet. Et andet kendetegn ved internetkriminelle er, at de ofte kun kender hinanden online. Europol (2011a) beskriver miljøerne således:

> Online forums are essential tools for the digital underground economy to recruit and make introductions, enabling criminals to swarm together to work on specific projects. These forums are also where crimeware components are advertised and budding cybercriminals learn their trade through tutorials.

8.3 Politianmeldelse og opklaring

I offerundersøgelsen af identitetstyveri og bedrageri ved internethandel spørges der til, hvorvidt de respondenter, der har været udsat for internetkriminalitet, har meldt sagen til politiet, og i så fald om sagen er opklaret. Nets står typisk for anmeldelse af betalingskort, der er spærret på grund af (forsøg på) misbrug. Dermed kan offerundersøgelsen ikke give et praj om anmeldelsestilbøjelighed i forbindelse med misbrug af betalingskort.

Tabel 8.1 viser resultaterne for identitetstyveri. Syv af respondenterne har været udsat for misbrug af både traditionelle og økonomiske identitetsbeviser, de lægges under kategorien økonomiske identitetsoplysninger. Det viser sig, at anmeldelsestilbøjelighed ikke er ens for de tre typer af identitetsoplysninger, der misbruges: Misbrug af digitale identiteter anmeldelse mindst hyppigt.

Tabel 8.1 Anmeldelsestilbøjelighed ved identitetstyveri

	Antal ofre	Anmeldelse	Anmeldelses-procent
Traditionelle ID-oplysninger/beviser	23	6	26 %
Økonomiske ID-oplysninger/beviser	35	10	29 %
Digitale ID-oplysninger	30	3	10 %
Andet	6	1	17 %
I alt	**94**	**20**	**21 %**

I alt svarer 20 respondenter i offerundersøgelsen, at de har anmeldt identitetstyveriet til politiet. Politiet optager i 18 af disse sager anmeldelse. 3 ud de 18 respondenter (17 procent) svarer, at politiet har opklaret sagen. Om politiet har opklaret andre af de 15 sager, ved vi ikke, men respondenterne har i hvert fald ikke kendskab til det.

Tabel 8.2 viser resultaterne for anmeldelsestilbøjeligheden ved e-bedrageri. I alt svarer 18 procent af respondenterne, der har været udsat for e-bedrageri, at de har anmeldt sagen til politiet. Anmeldelse sker betydeligt hyppigere i forbindelse med bedrageri ved privathandel end ved handel gennem en (falsk) internetbutik. I otte af tilfældene afviser politiet anmeldelsen. Det handler i fire sager om et butikskøb: Der er således købt en vare (henholdsvis tæpper, slankepiller, sko og kondomer) over nettet, men aldrig modtaget levering. Det andre fire sager, hvor politiet afviser anmeldelse handler om private handler, henholdsvis bog, mobiltelefon, Louis Vuitton taske og en Ipad, hvor betaling aldrig er modtaget. Hvorfor politiet afviser anmeldelsen er ikke kendt.

Tabel 8.2 Anmeldelsestilbøjelighed ved internethandelbedrageri i Danmark

	Antal ofre	Anmeldelse	Anmeldelses-procent
Butikshandel	159	18	11 %
Privathandel	74	24	32 %
I alt	**233**	**42**	**18 %**

Politiet opklarer 13 af de 34 sager (38 procent), hvori anmeldelse er optaget. 4 af de 14 anmeldte butikshandel bedragerisager er opklaret, mens 9 ud af de 20 anmeldte privathandel bedragerisager er opklaret.

8.4 Strafudmåling

Polsas filen med oplysninger om sigtede hackere, identitetstyve, skimmere, betalingskortmisbrugere og bedragere på det private marked indeholder også oplysninger om afgørelsen. Afgørelsen kan træffes af anklagemyndigheden eller domstolen. Anklageren kan afgøre en sag med:

- Påtaleopgivelse (retsplejelovens § 721). Denne afgørelse bliver for det meste anvendt når anklageren skønner således, at videre forfølgning ikke kan føre til, at sigtede findes skyldig. Det vil sige, at beviset er ikke tilstrækkeligt i anklagerens øjne og sigtede anses for ikke-skyldigt.
- Tiltalefrafald (retsplejelovens § 722). Denne afgørelse bliver anvendt ved bagatelagtige lovovertrædelser eller på grund af sigtedes unge alder eller sociale vilkår. Tiltalefrafald indebærer, at sigtede er fundet skyldigt.
- Bødeforlæg (retsplejelovens § 832). I sager om lovovertrædelser, der ikke skønnes at ville medføre højere straf end bøde, kan anklagemyndigheden i et bødeforelæg tilkendegive sigtede, at sagen kan afgøres uden retssag. Sigtede erklærer sig skyldig i overtrædelsen.

Domstolen kan afgøre en lovovertrædelse med ubetinget eller (delvis) betinget frihedsstraf, bøde, en anden type afgørelse, fx en foranstaltningsdom, eller frikendelse.

Tabel 8.3 Afgørelse i forbindelse med sigtelser for former af internetkriminalitet

	Hackere	ID-tyve	Skimmere	Kort-misbrugere	Bedragere ved handel
Under kriminelle lavalder	5 %			5 %	
Påtaleopgivelse	34 %	28 %	23 %	30 %	9 %
Tiltalefrafald	16 %	2 %		6 %	11 %
Bødeforlæg/dom	17 %	2 %		8 %	9 %
Betinget dom	21 %	30 %		24 %	31 %
Dom	5 %	33 %	66 %	22 %	37 %
Frifindelse	2 %	5 %	11 %	5 %	3 %
Ikke beviselig skyldigt	36 %	33 %	34 %	35 %	12 %
Fundet skyldigt	59 %	67 %	66 %	60 %	88 %

Tabel 8.3 viser for det første, at i ca. en tredjedel af sagerne opgives sigtelsen eller tiltalte frifindes. Det vil sige, at der i en tredjedel af sager mangler beviser i forhold til skyldspørgsmålet. Der er dog en undtagelse i forbindelse med sigtede for bedrageri ved internethandel, 9 ud af 10 dem findes skyldige. Når en sigtet findes skyldig i en af internetkriminalitetsformerne fører det oftest til en ubetinget eller betinget frihedsstraf. Det gælder dog ikke for sigtede i hackingsager, de dømmes sjældent til en ubetinget straf. Til gengæld anvendes bøde og tiltalefrafald hyppigere i forbindelse med hackingsager. Ses der specifikt på skimmere, kan de regne med en ubetinget frihedsstraf, når de findes skyldige.

Crime in a digital world

English Summary

This report examines identify theft, payment card fraud and fraud related to internet trade (e-fraud). None of these types of crime is a new form of crime, but the internet has provided new opportunities and means for carrying them out. Examination of these crimes requires some understanding as to how they are committed. The current report sheds light on these types of crime by examining their extent, method, cost to victims, victim profiles, prevention, police reporting, investigation, offender profiles and punishment.

Victim survey

Data were collected from 9,582 respondents during the ten-month period October 1, 2012 to July 31, 2013 as a part of Statistics Denmark's so-called omnibus surveys. Respondents were asked whether they had experienced any form of fraud during the purchase or sale of goods and services over the internet during the previous 12 months. Those who said they had were asked to describe their victimization in terms of type of e-fraud committed, type of goods or services involved, financial loss, coverage for loss, whether the crime was reported to police, and whether police solved the case. Furthermore, all respondents were asked whether their personal information or identity documents/cards had been misused within the 12 months prior to the survey. Those reporting victimization were asked to describe the type of information misused or stolen, means of acquisition, the method or form of misuse, and how the misuse was discovered. Like those reporting e-fraud, identity theft victims were also asked about the amount of financial loss suffered, coverage for loss, whether the crime was reported to police, and whether police solved the case.

Polsas data

Offender profiles are constructed on the basis of persons charged by the police. The National Police have created two data files for this purpose. The first data file contains information about persons charged for relevant penal code violations in regard to identity theft, payment card fraud and e-fraud in the period 2010-2012. The analysis is made for unique persons, which implies that a person charged for 30 criminal incidents – often collected in one case file – only counts once in the analysis. Offender profiles include hackers, skimmers, identity thieves, payment card betrayers and e-trade betrayers. The second data file of the National Police contains information about the criminal past of the same persons listed in the first data file. Information about the criminal past is related to the period 2001-2009 and includes penal law violations.

Definition of identity theft

While identity theft is a frequent form of attack, there is still no legal definition of it in Denmark. During the last few years there has been a debate over whether identity theft should be added as a new and separate offence in the criminal code. So far, there has not been a political majority to support a separate penal provision for identity theft. Identity theft defines as acquiring and mis-using identifying information of a person. This may be bank account information, CPR-number, entry codes or identification documents, like health insurance card or driver license. In previous research (Kruize, 2009, 2013) payment card fraud has been considered as a form of identity theft. In this report payment card fraud is described as separate entity. The rationale behind this decision is the exclusion of payment card fraud as form of identity theft by the Danish authorities.

Extent

The victim survey suggests that 4 percent of the Danish population has been victim of one of these crimes (identity theft, payment card fraud or e-fraud) over the past 12 months. This corresponds with circa 166.500 Danes. The risk is highest for e-fraud.

Table S.1 Victim rates (n=9.582)

	Number of victims	Victim rate
Misuse of traditional ID-information	29	0,30 %
Misuse of banking information	35	0,37 %
Misuse of digital ID-information	30	0,31 %
Misuse of payment card information	71	0,74 %
Fraud with merchant trade	159	1,66 %
Fraud with private trade	74	0,77 %
Total*	**384**	**4,01 %**

* The categories add up to 398 victims, but 14 persons are victimized in two categories.

Table S.2 Number of victims in Danmark: estimate and 95 % confidence interval

	Estimate	95 % - interval
Identity theft	46.900	38.400 – 55.400
Payment card fraud	29.400	22.500 – 36.300
E-fraud	109.900	95.700 – 124.100
Total	**166.500**	**149.900 – 183.100**

Methods

It is obvious that e-fraud takes place online. There are, however, many ways in which a perpetrator can acquire someone's identity or payment card information. Victims cannot always reconstruct how their information might have been stolen. Acquiring of payment card information happens for one out of three cases offline, but most victims believe that they have lost their payment card in-formation as a result of internet trade. This may suggest data loses of internet businesses. Hacking

and phishing – to fish for personal information in the digital world – is the basis for approximately 50 percent of all identity thefts.

Table S.3 Acquiring/misusing methods

	ID-theft	Card fraud	E-fraud
Offline	18 %	33 %	-
Hacking/phishing	53 %	24 %	-
Internet trade	16 %	41 %	100 %
Other methods online	13 %	2 %	-

Financial losses

All three forms of internet crime lead to financial losses. Not for everyone, but for some (ID-theft), many (payment card misuse) or nearly all (e-fraud). Table S.4 shows the overall financial losses for the victim survey respondents. On the basis of the median losses an estimate is made for losses on national level. In regard to payment card losses the estimate is close to the reported loss of 96 million Danish Kroner by payment card providers.

Table S.4 Financial losses

	Victim survey (n=9.582) (kroner)	Estimate for DK (million kroner)
Identity theft	311.127	59
Payment card fraud	639.149	91
E-fraud	779.489	81
Total	**1.729.765**	**231**

Victim profiles

The victim survey contains information about gender, age, profession and level of education of the respondents. Level of education appears to be unrelated to the risk of victimization, but the three other variables do show a correlation. In general are men more often victim than women – with exception of e-fraud – and fall the risk of victimization with age. Exception in regard to age is victimization of payment card fraud. Here the curve is parabolic. Risk for victimization in regard to profession show the highest risk for students, while retirees have the lowest risk for victimization. Also here payment card fraud is the exception with a more equally distributed victimization risk.

Victim profiles are not the same. Young men (1.9 %) have a four times higher chance for victimization of identity theft than elderly women (0.5 %). Midlife men (1.1 %) have the highest risk for payment card fraud, while young women (0.4 %) have the lowest risk. The risk for victimization of e-fraud is the highest for young women (4.5 %) while elderly women (1.1 %) have the lowest risk.

Table S.5 Victim rates

	ID-theft	Card fraud	E-fraud
Men	1,2 %	0,9 %	2,4 %
Women	0,8 %	0,6 %	2,5 %
Younger than 30 years old	1,6 %	0,6 %	4,0 %
30 – 49 years old	1,1 %	0,9 %	3,1 %
50 years old or more	0,6 %	0,6 %	1,4 %
With paid labour	1,1 %	0,7 %	2,5 %
Without paid labour	1,0 %	1,1 %	3,0 %
Student	1,6 %	0,7 %	4,0 %
Retiree	0,2 %	0,6 %	0,9 %

Prevention

Prevention of identity theft over internet can be enhanced through the use of technical security measures and prudent behavior online. Security measures protect against malware, while cautious online behavior reduces the risk of being a victim of phishing. Despite this, many privately-owned computers are under-secured. Governmental authorities have now begun helping citizens to update their software. For example, people using the password program NemID to log on to the Tax Administration's website are required to update to the latest version of Java before they can complete the login process. A similar scenario applies to *virk.dk* from the Danish Agency for Digitisation.

Payment cards can be misused online when offenders have access to the card number, expiration date and security code. Visa and Mastercard have introduced the so-called 3-D Secure: In addition to the card number, expiration date and security code, users must also provide an access code which they establish themselves prior to using the card. Individual online merchants can decide for themselves whether to require the extra form of security. The vast majority of Danish online merchants do not require its use. This choice reflects a greater concern for usability than security. Now that NemID has been introduced in Denmark, it may come to provide the same level of security for Dankort as 3-D Secure provides for Visa and Mastercard.

NemID – Denmark's digital signature – was introduced in July 2010. The introduction of NemID made access to netbanking and other online services safer than ever. Each time a customer logs on, he or she is required to provide a unique six-digit code read from a list of codes prepared by NemID. Funds stolen from netbanking are generally transferred abroad. Nordea Bank has already put this knowledge to use in the security hardening of their netbank system. Nordea asks customers for an additional confirmation by text message (SMS) when requesting money for international

transfer. Further technical hurdles could be added, but the banking industry also weighs user-friendliness and security concerns when designing its online systems.

Online banking is secured not only via access control, but also through the monitoring of payments. Payment monitoring takes place at bank data centers. These data centers can spot potential bank thefts by noticing unusual transfer activity or other warning signs. Foreign transfers do not occur instantaneously, but after a so-called clearance period of a few hours. The data centers therefore have a window of time within which they can stop suspicious activities. Figures from the Danish Bankers Association indicate that approximately half of all illicit netbanking transfers are discovered and stopped during the clearance period. Nets monitors transaction using VISA/Dankort and ensures that payments are transferred from the buyer's account to the merchant's account. Monitoring consists of identifying atypical transaction patterns, where the definition of "atypical" is experience-based and frequently updated. This may, for example, be the monitoring of so-called sprint transactions where a card is used within a (very) short period in multiple locations, for example, the cardholder's own bank, another bank, and for the purchase of up to 4,000 Danish Kroner worth of goods in a store.

Consumers are encouraged to be realistic in regard to their purchases over the web. If a price seems too good to be true, one should generally be skeptical. Denmark has established a so-called e-mark (*e-mærket*) to protect consumers who shop online. As of September 20, 2013, there were a total of 1,569 e-mark certified Danish webshops. In 2012, there were 298 cases reported by consumers in which a corrupt online store was alleged to have abused the e-mark system.

Danes transacting on the online auction sites qxl.dk and lauritz.com are – like online shopping – protected by legislation (*købeloven*). This legislation, however, is not applied to private transactions. In order to increase security for private online transactions, the classified advertising website dba.dk offers central person registry (CPR) or NemID validation of the seller.

Police reporting and investigation

Police investigation in regard to internet crime is organized in three levels. The first level is the ordinary police officer. IT-coordinators of police districts are the second level. There are around 45 IT-coordinators in Denmark. As rule internet crime is reported to and investigated at the level of a police district, but it is possible to benefit from more specialists knowledge of the national IT crime section (NITES). NITES have circa 60 employees of whom 50 are police officers, post-educated in data logics or computer science (often abroad). All together the Danish Police have employed circa 100 police-officers with more specialists knowledge of internet crime investigation. This corresponds with 1 percent of the police force.

Investigation requires a criminal complaint and many identity thefts go unreported to police. Only about 20 percent of survey respondents who report having been victims of identity theft say they filed an official note with police. A police report does not automatically lead to an investigation despite the fact that there are always digital tracks to follow. Police prioritize cases for investigation on the basis of factors like extent of the loss and whether there is evidence of repeat offending by an organized criminal group. Among survey respondents who reported an identity theft to police, 17 % say police successfully solved the case.

Nets reports typically payment card fraud to the police. Therefore the victim survey does not give a clue about the reporting practice in case of payment card fraud.

In victim survey, 18 % of those who experienced an e-fraud say they reported their victimization to police. Reporting to police is significantly more likely when fraud occurs in connection with transactions between private individuals as compared to transactions with a corrupt online merchant. The police clear the case in 38 % of the cases. In eight victim survey cases, police refused to file a report. Why the police refused to file these reports is unknown.

Offender profiles

Offender profiles are based on persons charged for internet crime. Not all cases are reported to the police and the police clear only a limited number of reported crimes. Therefore it is questionable whether the offender profile presented here is applicable for all offenders. Especially the profile of hackers seems to be selective, in the sense that only in easy and non-specialist hacker cases persons are charged.

Table S.6 Characteristics of offenders

	Hackers	ID-thieves	Skimmers	Card be-trayers	E-trade betrayers
Men	96 %	81 %	98 %	76 %	74 %
Women	4 %	19 %	2 %	24 %	26 %
Younger than 15 years old	4 %	-	-	4 %	-
15-24 years old	45 %	39 %	19 %	54 %	60 %
25-34 years old	16 %	31 %	52 %	25 %	31 %
35-44 years old	21 %	24 %	25 %	11 %	24 %
45-54 years old	11 %	5 %	4 %	6 %	7 %
55-65 years old	3 %	2 %	-	1 %	-
Danish citizen	92 %	78 %	6 %	77 %	98 %
Foreign citizen	8 %	22 %	94 %	23 %	2 %
No criminal record	60 %	39 %	96 %	40 %	26 %
Less than 10 prior charges	28 %	42 %	4 %	41 %	48 %
10 or more prior charges	12 %	19 %	-	19 %	26 %

Punishment

The public prosecution service or the court decides about punishment. The prosecutor may decide to waive the charges (lack of evidence), withdraw the charges or a give a ticket fine. The court may decide about the case by demanding an unsuspended sentence, a (partly) suspended sentence, fine, another type of decision or acquittal.

Table S.7 Punishment

	Hackers	ID-thieves	Skimmers	Card be-trayers	E-trade betrayers
Under criminal age (15 years)	5 %	-	-	5 %	-
Waiving the charges	34 %	28 %	23 %	30 %	9 %
Withdraw the charges	16 %	2 %	-	6 %	11 %
(ticket)fine	17 %	2 %	-	8 %	9 %
Suspended sentence	21 %	30 %	-	24 %	31 %
Unsuspended sentence	5 %	33 %	66 %	22 %	37 %
Acquittal	2 %	5 %	11 %	5 %	3 %
Not proven guilty	36 %	33 %	34 %	35 %	12 %
Proven guilty	59 %	67 %	66 %	60 %	88 %

Litteratur

Ahmad, Shehzad, Jens Borup Pedersen og Tonny Bjørn (2012) *DK-Cert Trendrapport 2011: It-kriminalitet og sikkerhed i året der gik*. Danmarks IT-center for uddannelse og forskning (UNI-C).

Ahmad, Shehzad, Jens Borup Pedersen og Torben B. Sørensen (2013). *DK-Cert Trendrapport 2012: Status på informationssikkerhed i året der gik.* Danish e-infrastructure cooperation (DeiC).

Balvig, Flemming, Britta Kyvsgaard & Anne-Julie Boesen Pedersen (2012) *Udsathed for vold og andre former for kriminalitet.* Københavns Universitet, Justitsministeriet, Det Kriminalpræventive Råd, Rigspolitiet.

Binder, R. & M. Gill (2005). *Identity theft and fraud: learning from the USA*. Perpetuity Research and Consultancy International.

Cheney, J.S. (2005) *Do definitions still matter?*

Center for Cybersikkerhed (CFCS) (2013) *Situationsbillede af sikkerhedstilstanden på internettet*. April 2013. Forsvars Efterretningstjeneste.

Danmarks Statistik (2011). *Befolkningens brug af internet 2010.*

European Central Bank (2012). *Report on card fraud.*

Europol (2003). Computer-related crimes within the EU: Old crimes new tools, new crimes new tools.

Europol (2006). *Organised Crime Threat Assessment* (OCTA).

Europol (2011). OCTA 2011: EU Organised Crime Threat Assessment. www.europol.europe.eu

Europol (2013). SOCTA 2013: EU Serious and Organised Crime Threat Assessment. www.europol.europe.eu

FDIH (2012a). *Dansk e-handelsanalyse: Forbrugerstatistik, Årsrapport 2011*.

FDIH (2012b). *Dansk e-handelsanalyse: Forbrugerstatistik, Årsrapport 2012*.

Furnell, S. (2010). Hackers, viruses and malicious software. In: Jewkes, Y. & M. Yar (eds.) *Handbook of Internet Crime*. Devon: Willan Publishing.

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

Javelin Strategy & Research (2003-2011). *Identity Fraud Survey Report.*

Jewkes, Yvonne & Majid Yar (eds.) (2010). *Handbook of Internet Crime*. Cullompton, Devon: Willan Publishing.

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

Karstoft, Susanne (2012) Internetbetalinger. I: Trzaskowski, Jan (red.) *Internetretten* (2. udgave). København: Ex Tuto Publishing, s. 189-259.

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

Konkurrence- og Forbrugerstyrelsen (2012). *Betalingskortmarkedet.*

Kruize, Peter (2009). *Identitetstyveri*. Københavns Universitet: Det Juridiske Fakultet.

Levy, S. (1984) *Hackers: Heroes of the Computer Revolution*. New York: Anchor Press.

Lundø, Martin (2011). *Danske virksomheders brug af it 2011*. Danmarks Statistik.

Lundø, Martin (2012). *It-anvendelse i den offentlige sektor – 2011*. Danmarks Statistik.

McAfee (2006). Virtual Criminology Report: Cybercrime The Next Wave. www.mcafee.com

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; Cullompton, Devon: Willan Publishing, pp. 33-55.

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

Nederlandse Vereniging van Banken (NVB) (2012). *Jaarverslag 2011*.

OECD (2009). *Online Identity Theft*.

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

PwC (2011a). *Virksomhedskriminalitet i Danmark 2011.*

PwC (2011b). *The Global Economic Crime Survey.*

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

Rogers, M. (2006). A two-dimensional circumplex approach to the development of a hacker taxonomy. *Digital Investigation*, 3 (2006), pp. 97-102.

Ruiter, Marlies (2013). Skimming: Kat-en-muisspel voor knappe koppen. In: *Blauw*, 9:15/16, p. 8-11.

Sørensen, Carsten (2013). E-handel runder omsætning på 50 milliarder. *www.altomdata.dk*

Stol, Wouter (2012). Cyberspace and safety. In: Leukfeldt & Stol (eds.) *Cyber Safety: An introduction*. The Hague: Eleven international publishing, pp. 19-30.

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

Tambour Jørgensen, Tanja (2013). *Omfanget og karakteren af stalking: en befolkningsundersøgelse*. Justitsministeriets Forskningskontor.

Tranberg, Charlotte Bagger & Lars Bo Langsted (2012). Internet kriminalitet. I: Trzaskowski, Jan (red.) *Internetretten* (2. udgave). København: Ex Tuto Publishing, s. 675-722.

Wall, D. (2007) *Cybercrime: The transformation of crime in the information age*. Cambridge/ Malden MA: Polity.

Wijas-Jensen, Justyna (2012a). *It-anvendelse i befolkningen – 2011*. Danmarks Statistik

Wijas-Jensen, Justyna (2012b). *It-anvendelse i befolkningen – 2012*. Danmarks Statistik

Wix Wagner, Eva (2012). *Betalinger ved handel på internettet*. Nationalbanken, Kvartalsoversigt, 1. kvartal 2012, del 1, s.127-138.

Yar, M. (2006). *Cybercrime and Society*. London: Sage.

Websider

Internetkriminalitet metoder

https://www.cert.dk/

Identitetstyveri

http://www.finansraadet.dk/
http://www.idtyveri.info/
https://www.javelinstrategy.com/

E-bedrageri

http://www.fdih.dk/
http://www.dba.dk/
http://www.qxl.dk/
http://www.lauritz.com/da/

Betalingskortmisbrug

http://www.nets.eu/dk-da/Pages/default.aspx
https://www.teller.com/da/ForsideDansk/
http://www.ecb.int/home/html/index.en.html

Forebyggelse

http://www.dkr.dk/

Efterforskning

https://www.europol.europa.eu/
https://www.politi.dk/da/servicemenu/forside/

Data fra danske websider:

Netbankindbrud statistik. Under Tal & Fakta, Netbanksikkerhed på Finansrådets hjemmeside:
www.finansraadet.dk/tal--fakta/statistik-og-tal/netbankindbrud---statistik.aspx
Dankort misbrugstal. Under Om Nets, Nets i tal på Nets hjemmeside:
www.nets.eu/dk-da/Om/om-virksomheden/nets-i-tal/misbrugstal/Pages/default.aspx

Spørgeskema offerundersøgelse

Bilag 1

Spørgsmål i forbindelse med e-bedrageri	
Har du inden for de seneste 12 måneder været udsat for bedrageri ved køb eller salg af varer/ydelser over internettet?	1 Ja 2 Nej
Hvilken form for bedrageri var du sidst udsat for? (Flere svar muligt)	1 Betalt for varer/ydelser i en internetbutik, men har aldrig modtaget varerne 2 Betalt for varer/ydelser til en privatperson, men har aldrig modtager varerne 3 Solgt varer/ydelser til en virksomhed, men har aldrig modtaget betaling 4 Solgt varer/ydelser til en privat person, men har aldrig modtaget betaling
Hvad for en vare/ydelse ville du købe / sælge?	[tekst]
For hvilket beløb er du blevet bedraget?	[beløb]
Hvor stor en del af dette beløb, har du selv betalt? (Fx hvis bank eller kreditkortselskab kun har dækket noget af beløbet?)	[beløb]
Har du meldt bedrageriet til politiet?	1 Ja, men politiet afviste anmeldelsen 2 Ja, og politiet optog anmeldelsen 3 Nej
Er bedrageriet opklaret, det vil sige at én eller flere personer er sigtet i sagen?	1 Ja 2 Nej / Ved ikke

Spørgsmål i forbindelse med identitetstyveri	
Har du inden for de seneste 12 måneder været udsat for misbrug af personoplysninger eller identitetsbeviser?	1 Ja 2 Nej
Hvilke personoplysninger / identitetsbeviser blev sidst misbrugt? (Flere svar muligt)	1 Navn / CPR-nummer 2 Identitetsbeviser (pas, id-kort, sygesikring, kørekort mm) 3 Betalingskort (Dankort eller kreditkort) 4 Bankoplysninger (kontonummer, adgangskode mm) 5 Digitale profiler (e-mail, Facebook mm) 6 Andet
Til hvilken formål misbrugte gerningspersonen personoplysningerne eller identitetsbeviser? (Flere svar muligt)	1 At købe varer/ydelser på nettet 2 At købe varer/ydelser i en almindelig butik 3 At hæve penge fra min konto (hæveautomat) 4 At overføre penge fra min konto til en anden konto 5 At leje noget (fx en bil) i mit navn 6 At afslutte et abonnement (fx mobiltelefon) i mit navn 7 At oplyse mit navn til myndighederne (fx ved en trafikforseelse) 8 At publicere (fx på nettet) noget eller sende en besked i mit navn 9 Andet
Hvordan har du opdaget, at dine personoplysninger / identitetsbeviser blev misbrugt?	1 Betalingskort blev spærret af kortudbyder 2 Gennem udskrifter (på papir eller netbank) 3 Regning / opkrævning fra en virksomhed for en vare / ydelse 4 Andet

Hvordan, tror du, at gerningspersonen har fået fat i dine personoplysninger / identitetsbeviser? (Flere svar muligt)	1 Jeg har oplyst det gennem en falsk e-mail / falsk hjemmeside (phishing, pharming) 2 Min computer er blevet udsat for hacking/malware (spyware) 3 Ved at handle på nettet (internetbutik mm) 4 Jeg har selv lagt oplysningen på nettet (Facebook profil mm) 5 Jeg har selv oplyst mine ID-oplysninger i telefon 6 ID-bevis er blevet stjålet (indbrud, tricktyveri, røveri, lommetyveri mm) 7 Ved brug af betalingskort i udlandet 8 Andet
Hvor stor et beløb er der trukket fra din konto eller opkrævet pga. misbrug af personoplysninger / identitetsbeviser?	[beløb]
Hvor stor en del af dette beløb, har du selv betalt? (Fx hvis bank eller kreditkortselskab kun har dækket noget af beløbet?)	[beløb]
Har du meldt misbruget til politiet?	1 Ja, men politiet afviste anmeldelsen 2 Ja, og politiet optog anmeldelsen 3 Nej
Er misbruget opklaret, det vil sige at én eller flere personer er sigtet i sagen?	1 Ja 2 Nej / Ved ikke