DET JURIDISKE FAKULTET
KØBENHAVNS UNIVERSITET

Kriminalitet i en digitaliseret verden

Identitetstyveri og bedrageri på internettet

Peter Kruize

Maj 2013

Kriminalitet i en digitaliseret verden

Identitetstyveri og bedrageri på internettet

Peter Kruize

Maj 2013

ISBN 978-87-985490-1-7

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* omfatter to dele, hvoraf den første belyser omfanget af og omkostningerne ved identitetstyveri og bedrageri på internettet. Det sker på baggrund af eksisterende statistikker, offerundersøgelser og interviews med nøglerespondenter. Resultaterne fra projektets første del beskrives i denne rapport.

Projektets anden del har til formål at beskrive en gerningsmandsprofil ud fra politiets registre. Arbejdet hermed starter i maj 2013 og slutter efter planen sidst i september 2013. Der rapporteres separat om projektets anden del.

Projektet er økonomisk støttet af Justitsministeriets Forskningspulje og Det Kriminalpræventive Råd. Sociologistuderende Sanna Larsen har assisteret ved undersøgelsen og læst korrektur. David Sorensen har stået for oversættelse af resuméet til engelsk.

Jægerspris, 27. maj 2013
Peter Kruize

Kriminalitet i en digitaliseret verden:
Identitetstyveri og bedrageri på internettet

Resume

Denne undersøgelse retter sig mod identitetstyveri og bedrageri (e-bedrageri) 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 i denne rapport at give plads til en beskrivelse af de metoder, som internetkriminelle benytter til at begå identitetstyveri på internettet og bedrageri ved internethandel. Desuden belyses de to kriminalitetsformer i denne rapport også ud fra følgende perspektiver: Omfang, tab, offerprofil, forebyggelse og efterforskning.

Undersøgelsesmetoder
For at få indblik i omfanget af og fremgangsmåden ved identitetstyveri og e-bedrageri benyttes følgende eksisterende statistikker: malware og phishing (DK•CERT), netbankindbrud (Finansrådet), Dankortmisbrug (Nets), kriminalstatistik (Danmarks Statistik, Rigspolitiet), internetbrug og handel (Danmarks Statistik, FDIH).

Danmarks Statistik gennemfører årligt en spørgeskemaundersøgelse blandt danskere, danske virksomheder og myndigheder om deres brug af internettet. Disse spørgeskemaundersøgelser bidrager med interessante data vedrørende internetkriminalitet. Men for at få nærmere indblik i identitetstyveri og e-bedrageri er der udført en supplerende offerundersøgelse som led i Danmarks Statistiks omnibus. Data er indsamlet i perioden fra oktober 2012 til februar 2013, og i løbet af de fem måneder er 4.890 respondenter adspurgt. Respondenterne svarer blandt andet på, hvorvidt de har været udsat for bedrageri ved køb eller salg af varer/ydelser over internettet indenfor de sidste 12 måneder. Hvis dette er tilfældet, er der 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 adspurgt, om de har været udsat for misbrug af personoplysninger eller identitetsbeviser inden for de sidste 12 måneder. Respondenter, der har været udsat herfor, er stillet op følgende spørgsmål: Type oplysninger, tilegnelse, misbrug, opdagelse, beløb, hæftelse for tab, politianmeldelse og opklaring af sagen.

Desuden er der afholdt personlige interviews med repræsentanter fra Finansrådet, Nets, FDIH og Rigspolitiet.

Computere under angreb

Undersøgelser fra Danmarks Statistik viser, at en betydelig del af danske computere er udsat for malware. I 2011 svarer en tredje del af de adspurgte privatpersoner, at de har været under angreb fra malware. Det samme gælder for 7 procent af de danske virksomheder og 15 procent af de danske myndigheder. Overordnet set er trojanere den mest anvendte malware i 2012.

DK•CERT modtager anmeldelser vedrørende danske phishing-sider og sider med trojanere. Der er i 2012 1.211 anmeldelser omkring inficerede danske internetsider. I perioden fra 2005 til 2012 stiger antallet af inficerede danske internetsider støt, men samtidig lukker hostingselskaberne og internetudbyderne hurtigere phishing-sider.

Identitetstyveri (på internet)

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. Men et mindretal i retsudvalget har opfordret regeringen til at foretage initiativer, der sikrer, at myndigheder, virksomheder og privatpersoner står bedst muligt rustet over for identitetstyveri og de kriminelle følger heraf.

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 betalingskortoplysninger og adgangskoder 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, er en offerundersøgelse gennemført. Denne undersøgelse viser, at 1,8 procent af de adspurgte respondenter har været udsat for identitetstyveri indenfor de sidste 12 måneder. Antallet af ofre for identitetstyveri er steget fra ca. 48.000 i 2009 til ca. 73.000 i 2012. Stigningen er statistisk signifikant. Denne offerrisiko gælder for den *brede* definition af identitetstyveri: Betalingskortmisbrug er således inkluderet, og både online og offline identitetstyveri omfattes. Offerrisikoen for den brede definition af identitetstyveri kan opdeles i tre underkategorier:

Tabel R.1 Offerrisiko for identitetstyveri i Danmark (2012)

	Risiko	Antal danskere
Økonomiske identitetsoplysninger	1,1 %	45.000
Traditionelle personoplysninger	0,4 %	16.000
Digitale identitetsoplysninger	0,3 %	12.000
I alt	**1,8 %**	**73.000**
95 % -interval	1,4 – 2,2 %	57.000 – 89.000

Der er mange måder, hvorpå gerningspersonen kan tilegne sig andres identitetsoplysninger, og de udsatte kan ikke altid rekonstruere, hvordan det er sket. Lidt over halvdelen (54 procent) af respondenter mener dog, at deres oplysninger er blevet stjålet online, mens lidt under halvdelen (46

procent) tror, at det er sket offline. Phishing – at fiske efter personoplysninger i den digitale verden – står for ca. 25 procent af tilegnelserne.

Tab(sfordeling) som følge af identitetstyveri

I de fleste tilfælde misbruges stjålne identitetsoplysninger økonomisk. Hyppigst hæves eller overføres penge fra ofrets konto ved hjælp af betalingskort- eller kontooplysninger. Men oplysningerne anvendes også til køb af varer og ydelser. I offerundersøgelsen oplyser respondenterne størrelsen på det tab, de har lidt indenfor de seneste 12 måneder som følge af identitetstyveri. Når dette ganges op til at gælde hele den danske befolkning, udgør tabet omkring 125 mio. kr. Dette tal er i nærheden af, hvad betalingskortudbydere oplyser, at tabet som følge af identitetstyveri er i 2012. Ifølge deres beregninger udgør tabet ca. 100 mio. kr. Ifølge oplysninger fra kortselskaberne står misbrug på internettet for ca. 40 mio. kr. af det samlede tab

Offline hæfter kortindehaveren typisk for en selvrisiko på 1.100 kr., når vedkommendes betalingskortoplysninger misbruges. Når Dankort derimod anvendes ved internethandel – hvilket oftest sker - hæfter indehaveren ikke for misbrug. Da Dankort kan anvendes på internettet uden pinkode eller anden form for ekstra sikkerhed. Respondenterne i offerundersøgelse svarer samlet set, at de i snit hæfter for 3 procent af det økonomiske tab som følge af misbrug af deres identitetsoplysninger. Til sammenligning hæfter kortindehavere, der har været udsæt for misbrug af deres Dankort, i snit for 6 procent af tabet, hvis det antages, at de alle betaler en selvrisiko på 1.100 kr. ved misbrug i offline verdenen. Begge oplysninger peger i retning af, at kortindehaveren generelt set hæfter for en beskeden del af tabet.

I forbindelse med misbrug af identitetsoplysninger på internettet, er det typisk forretninger (når Dankort misbruges) eller kreditkortselskaber (når internationale betalingskort misbruges), der hæfter for tabet.

Offerprofil ved identitetstyveri

Risikoen for identitetstyveri falder med alderen. Det er således mænd under 30 år, der har større risiko for at blive udsat for identitetstyveri. Offerrisikoen er i modsætning hertil uafhængig af uddannelsesniveau, men der er en sammenhæng med erhvervsform. Studerende har således den højeste risiko, mens pensionister tegner sig for den laveste. At være i arbejde har en dæmpende effekt på risikoen for at blive udsat for identitetstyveri.

Forebyggelse af identitetstyveri

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 anvendes. 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 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.

Efterforskning af identitetstyveri

Efterforskning kræver en anmeldelse. Men langt fra alle anmelder identitetstyveri til politiet. I offerundersøgelsen svarer ca. en tredjedel af respondenterne, der har været udsat for identitetstyveri, at de har anmeldt sagen, hvis der ses bort fra tilfældene, hvor Nets har spærret betalingskortet. 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. 20 procent af respondenterne, der har været udsat for identitetstyveri og efterfølgende anmeldt sagen til politiet, svarer, at dette har ført til opklaring.

E-bedrageri

Der handles mere og mere på internettet. Internethandel står således for ca. 18 procent af detailhandlens samlede omsætning på 283 milliarder kroner i 2012. Der er dog brancher, hvor internethandlen udgør langt mere end de 18 procent. Herudover handler danskere også privat på internettet, og der eksisterer utallige sider, hvor der kan opslås en salgs- eller købsannonce. Den mest kendte almene handelsside på internettet – udover aktionssiderne qxl.dk og lauritz.com – er dba.dk. Ikke alle sider, der kan handles privat på, er dog almene. En stor del af dem retter sig mod et særligt publikum.

En privatperson kan udsættes for e-bedrageri i forbindelse med køb af en vare eller ydelse i en falsk internetbutik, eller ved snyd fra en privat sælgers side. Omvendt kan en privat sælger føres bag lyset af en upålidelig køber. I offerundersøgelsen angiver 112 ud af 4.890 respondenter (2,3 procent), at de har været udsat for e-bedrageri indenfor de sidste 12 måneder. Blandt disse svarere ca. to ud af tre, at det skete i forbindelse med handel i en (falske) internetbutik, mens en ud af tre handlede privat.

Tabel R.2 Offerrisiko for e-bedrageri i Danmark (2012)

	Butikshandel	Privathandel	I alt
Andel af udsatte for e-bedrageri	1,5 %	0,8 %	2,3 %
95 % -interval	1,2 – 1,8 %	0,6 – 1,0 %	1,9 – 2,7 %
Antal udsatte i Danmark (personer)	64.000	32.000	96.000
Antal udsatte i Danmark (husstande)	40.000	20.000	60.000

Kategorien 'tøj, sko og smykker' placerer sig øverst på listen over, hvilke varekøb danskerne snydes mest med i (falske) internetbutikker. På denne liste placerer kategorien 'kosmetik, medicin og kosttilskud' sig også højt. I forbindelse med handel privatpersoner imellem, hvor en af parterne udsættes for e-bedrageri, placerer kategorien 'tøj, sko og smykker' sig også øverst på listen over varekøb, som der snydes mest med.

Tab som følge af e-bedrageri

Respondenterne i offerundersøgelse, der har været udsat for e-bedrageri, har samlet set tabt en halv mio. kr. Det svarer til et gennemsnit på godt 4.000 kr. Dette er dog 'kunstigt' højt, da der er tale enkelte store beløb. I mere end halvdelen af e-bedragerisagerne er tabsbeløbet således på under 1.000 kr. Hvis dette beløb på 1.000 kr. tages som udgangspunkt for at beregne det samlede tab for den danske befolkning som følge af e-bedrageri i 2012, lyder tabet på mellem 60 og 90 mio. kr.

Offerprofil ved e-bedrageri

Risikoen for e-bedrageri knytter sig til alder, ældre har således en mindre sandsynlighed for at blive udsat for bedrageri på internettet end yngre. Dette hænger formentligt sammen med, at ældre ikke lige så hyppigt køber varer og ydelser på internettet. Der er ikke den store forskelle i offerrisikoen for henholdsvis mænd og kvinder. Dog har 30-39-årige kvinder størst sandsynlighed for at blive udsat for e-bedrageri, offerrisikoen er således 5,0 procent for denne gruppe. Risikoen for at blive

udsat for e-bedrageri er lidt højere for danskere med arbejde sammenlignet med danskere uden arbejde. Desuden har studerende den største risiko, mens pensionister klart har den mindste offerrisiko for e-bedrageri.

Forebyggelse af e-bedrageri
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 1.422 e-mærkede internetbutikker (pr. 20. marts 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.

Efterforskning af e-bedrageri
I offerundersøgelsen svarer 15 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 halvdelen af sagerne, hvori anmeldelse er optaget. Men i tre af tilfældene i offerundersøgelsen afviser politiet anmeldelsen. Det handler i alle tre sager om en privat sælger, der aldrig har modtaget sin betaling. Hvorfor politiet afviser anmeldelsen er ikke kendt.

Crime in a digital world:
Identity theft and e-fraud on the internet

Summary

This report examines identify theft and fraud committed over the internet (e-fraud). Neither identity theft nor fraud 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 internet identity theft and e-fraud by examining their extent, cost to victims, victim profiles, prevention and investigation.

Research Methods
The following preexisting resources were consulted in order to gauge the extent of identity theft and e-fraud, and to outline the methods used to commit them: malware og phishing (DK•CERT); theft from netbanking (The Danish Bankers Association); misuse of debit cards, especially *Dankort* (Nets); official police data (Statistics Denmark; The Danish National Police); internet use and e-commerce (Statistics Denmark; FDIH).

Statistics Denmark conducts an annual survey measuring internet use among private persons, businesses and government bodies. The standard survey collects a wide spectrum of interesting information on internet crime in general. Meanwhile, a supplementary survey of victims provides a detailed look at identity theft and e-fraud in particular. Data were collected from 4,890 respondents during the five-month period October 1, 2012 to February 28, 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.

In addition to the data described above, the current report is supplemented by personal interviews conducted with representatives from The Danish Bankers Association, Nets, FDIH, and the Danish National Police.

Computers under attack

Research from Statistics Denmark shows that a significant proportion of Danish computers are exposed to malware. One-third of private respondents indicate that their computers have suffered a malware attack. The same goes for the computers of 7% of Danish businesses and 15% of Danish government bodies. Trojans were the most common form of malware used in attacks in 2012.

In 2012, DK•CERT registered 1,211 reports of Danish websites equipped to spread Trojans and/or conduct phishing scams. During the period 2005-2012, the number of Danish websites containing these dangers increased dramatically. At the same time, however, web hosting companies and internet service providers (ISPs) got faster at identifying and closing phishing websites and thereby also reducing the risk of abuse.

Identity theft (over internet)

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 offense in the criminal code. So far, there has not been a political majority to support a separate penal provision for identity theft, though the government has encouraged a minority in the Legal Affairs Committee (*Retsudvalget*) to undertake initiatives to ensure that public authorities, businesses and consumers are optimally equipped to deal with identity theft and its criminal consequences.

A person only realizes that he or she has been subject to a criminal act when and if the misuse of identity is discovered. Furthermore, not all information stolen, e.g., intercepted debit card and/or password data, is ultimately used to commit further crimes. The actual extent of identity theft is therefore – by nature – unknown. The extent of known (discovered) cases is, however, routinely measured via victim surveys. These surveys indicate that 1.8% of Danish respondents are aware of having been victims of identity theft within the previous year. Extrapolating from survey data, one can estimate that the number of known identity theft victims has increased from circa 48,000 in 2009 to circa 73,000 in 2012. This increase is statistically significant. These numbers are based on a broad definition of identity theft. The definition includes identity thefts occurring both on- and offline, including the misuse of credit/debit cards. This broad definition of identity theft can be divided into three sub-categories. Risks of victimization for each sub-category and the estimated number of victims in 2012 are shown in Table S.1.

Table S.1 Risk of identity theft and estimated number of victims in Denmark (2012)

	Risk	Victims
Financial identity info (e.g., bank account)	1.1 %	45,000
Traditional personal info (e.g., CPR number)	0.4 %	16,000
Digital identity info (e.g., email, Facebook)	0.3 %	12,000
Total	**1.8 %**	**73,000**
95% interval	1.4 – 2.2 %	57.000 – 89.000

There are many ways in which a perpetrator can acquire someone's identity information. Victims cannot always reconstruct how their information might have been stolen. Nonetheless, just over half (54%) of respondents believe that their information was stolen online, while just under half (46%) believe it was stolen offline. Phishing – to fish for personal information in the digital world – is the basis for approximately 25% of all identity thefts.

Loss resulting from identity theft

In most cases, stolen identity information is used to commit economic thefts. These thefts typically involve the misuse of credit/debit card and/or bank information for either the withdrawal or transfer of funds from the victim's account or the purchase of goods and services over the internet. Based on extrapolation of survey respondent data, one can estimate the total loss of identity theft to Danish victims each year at approximately 125 million Danish Kroner. This figure is relatively close to the estimated loss of 100 million Danish Kroner reported by credit/debit card providers. According to information from the payment card companies, theft over internet is responsible for approximately 40 million kroner of the total loss.

Victims seeking compensation for the offline misuse of their Dankort debit card information are held responsible for a 1,100 kroner deductable. Contrary to this, when Dankort cards are misused online – which is their most frequent place of misuse – victims are free of deductables since online use requires neither pin codes nor any other form of security. Looking at on- and offline thefts collectively, survey respondents report being held responsible for an average of 3% of the losses incurred. Meanwhile, the 1,100 kroner deductable for offline thefts covers only 6% of the total losses to Dankort providers each year. Under both scenarios, it is clear that consumers are held responsible for only a minor fraction of total the loss.

When identity information is misused online, it is typically businesses (when Dankort is misused) or credit card companies (when international payment cards are misused) that cover the loss.

Victim profile for identity theft

The risk of identity theft falls with age. Men under 30 have the highest risk of victimization. While risk of identity theft appears to be unrelated to educational achievement, there is a correlation with vocation. Risk is highest for students and lowest for retirees. The risk is generally lower for those outside the labor force.

Prevention of identity theft

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.

Investigation of identity theft

Investigation requires a criminal complaint and many identity thefts go unreported to police. Only about one-third of survey respondents who report having been victims of identity theft say they filed an official note with police (excluding those cases in which Nets froze the payment card). 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, 20% say police successfully solved the case.

E-fraud

The number of financial transactions conducted over the internet is constantly increasing. In 2012, internet transactions accounted for approximately 18% of the 283 billion Danish Kroner worth of retail sales engaged in by Danish buyers and/or sellers. There are, however, certain branches where internet transactions account for far more than 18% of sales. Danes also engage in private transactions over the web. There are numerous webpages where one can post goods and services for purchase and sale. Many of these webpages target a specialized audience. Apart from the auction pages qxl.dk and lauritz.com, the best known page for ordinary personal advertisements in Denmark is dba.dk.

Private individuals can fall victim to e-fraud by buying goods or services over the internet from a corrupt online merchant or corrupt private seller. Likewise, a private seller can be deceived by an unreliable buyer. Among 4,890 respondents to a victim survey, 112 (2.3%) reported that they had experienced an e-fraud within the previous 12 months. Among those victims, approximately two-thirds say they were cheated by an online merchant, while one-third say they were cheated while conducting online transactions with a private seller.

Table S.2 Risk of e-fraud and estimated number of victims in Denmark (2012)

	Merchant trade	Private trade	In total
Proportion reporting e-fraud	1.5 %	0.8 %	2.3 %
95 % interval	1.2 – 1.8 %	0.6 – 1.0 %	1.9 – 2.7 %
Estimated persons victimized	64,000	32,000	96,000
Estimated households victimized	40,000	20,000	60,000

When asked what types of transactions they were defrauded in, e-fraud victims most often cited purchase of ‘clothes, shoes and jewelry’ from (fake) online stores. The second most-frequently cited transaction category was purchase of ‘cosmetics, medicines and food supplements’. In the context of transactions between private parties, e-fraud was also reported to be most prevalent when purchasing ‘clothes, shoes and jewelry’.

Loss resulting from e-fraud

Victim survey respondents that have experienced e-fraud report a collective loss of half a million Danish Kroner. This corresponds to an average loss of just over 4,000 kroner per respondent. This figure is, however, artificially inflated due to a small number of very big losses. More than half of all e-fraud cases involve a loss of no more than 1,000 kroner. If 1,000 kroner is taken as the average loss, then one can estimate total loss to the Danish public due to e-fraud at somewhere between 60 and 90 million Danish Kroner per year.

Victim profile for e-fraud

The risk of e-fraud is correlated with age. Older people have a lower risk of fraud over the internet. This is presumably due to the fact that older people use the internet less frequently than their younger counterparts for the purchase of goods and services. While there is no significant difference in risk for men and women, it is women ages 30-39 who suffer the highest prevalence of victimization (5.0%). The risk of e-fraud is higher for Danes in school and those attached to the labor market than it is for the unemployed and the retired. Students have the highest risk of e-fraud victimization while retirees have by far the lowest.

Prevention of e-fraud

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 March 20, 2013, there were a total of 1,422 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.

Investigation of e-fraud

In victim surveys, 15% 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. In three victim survey cases, police refused to file a report. All three cases concerned a private seller who allegedly never received payment for goods or services rendered. Why the police refused to file these reports is unknown. On average, suspects were identified in half of all e-fraud cases reported to police.

Indholdsfortegnelse

Kapitel 1

Indledning

1.1 Internettet: en ny verden

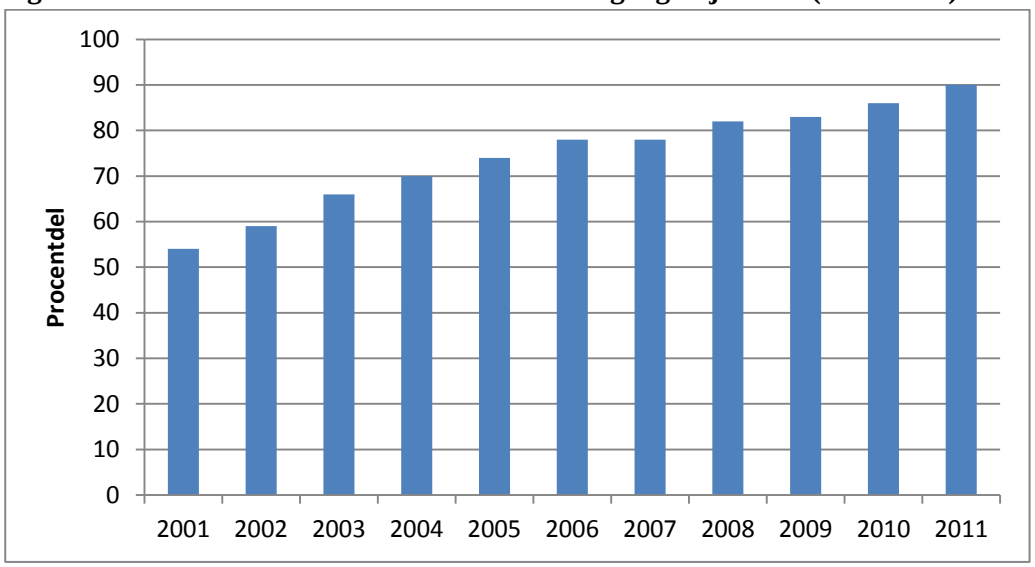
Efter et kapløb med en britisk ekspedition ledet af Robert Scott når den norske polarforsker Roald Amundsen Sydpolen d. 14. december 1911. Hans ekspedition er således den første på Sydpolen, og hermed er jorden kortlagt. Der er ingen nye horisonter, der kan opdages, i hvert fald ikke på jorden. Nye verdener 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*, der 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 2011 er der en computer tilgængelig i 90 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 (7 %) bruger det aldrig, mens godt tre ud af fire danskere (78 %) er dagligt på internettet. Desuden har tre ud af fire danskere (75 %) netbank, og de fleste danskere (70 %) køber varer eller ydelser over internettet. Det er billetter til biograf, teater mm, der topper listen, efterfulgt af tøj og sportsudstyr. Mænd køber lidt oftere over internettet end kvinder, og ældre danskere (pensionister) benytter sig mindre hyppigt af internetkøb end de yngre generationer (Wijas-Jensen, 2012).

Figur 1.1 Procentdel af danskere med internetadgang i hjemmet (2001-2011)



Kilde: Danmarks Statistik (Wijas-Jensen, 2012)

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, der 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 (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 beskrive forskellige former for internetkriminalitet, men derimod at se nærmere på to former for berigelseskriminalitet: Identitetstyveri på internettet og bedrageri ved internethandel (e-bedrageri). Når disse *computerassisterede* kriminalitetsformer undersøges nærmere, kan det ikke undgås at belyse metoderne, som internetkriminelle anvender til at begå henholdsvis identitetstyveri og e-bedrageri.

I den første del af dette forskningsprojekt er formålet at få et bedre indblik i identitetstyveri og e-bedrageri. I forbindelse hermed er det basale spørgsmål som omfang, udvikling, fremgangsmåde, tab og offerprofil, der søges svar på. Den anden del af forskningsprojektet har til formål at belyse henholdsvis borgernes, virksomhedernes og myndighedernes indsats overfor at undgå og bekæmpe disse former for internetkriminalitet. 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 og e-bedrageri?
- Hvad er størrelsesbeløbet på de direkte og indirekte økonomiske tab som følge af identitetstyveri og e-bedrageri, og hvem betaler regningen?
- Hvordan ser en offerprofil(er) ud for dem, der udsættes for identitetstyveri og e-bedrageri?
- Hvilke muligheder er der for at undgå at blive udsat for identitetstyveri og e-bedrageri?
- Hvilke muligheder er der, når det gælder efterforskning og strafforfølgelse af identitetstyveri og e-bedrageri?

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 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 og e-bedrageri.

Eksisterende statistikker og anden viden

Ved identitetstyveri og e-bedrageri er det ikke altid i virksomhedens interesse at informere politiet eller andre myndigheder. 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. Samtidigt 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 og e-bedrageri inddrages 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)

Offerundersøgelser blandt danskere

Danmarks Statistik gennemfører årligt en spørgeskemaundersøgelse blandt danskere om deres IT-vaner og internetadfærd. I undersøgelserne fra 2010 og 2011 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, 2012, s. 34).

Danmarks Statistiks spørgeskemaundersøgelse om danskernes IT-vaner og internetadfærd giver interessante data i forbindelse med internetkriminalitet. Men for at få nærmere indblik i identitetstyveri og e-bedrageri 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 omnibus i perioden oktober 2012 til og med februar 2013. I omnibussen adspørges ca. 1.000 personer pr.

måned[1]. I løbet af de fem måneder er 4.890 respondenter således adspurgt, enten telefonisk eller via et internetspørgeskema. Tabel 1.1 viser fordelingen.

Tabel 1.1 Respondenterne offerundersøgelse 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
I alt	**2.929**	**1.961**	**4.890**

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 der 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 eller identitetsbeviser 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.

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 myndighedernes anvendelse af informationsteknologi. Besvarelserne er indsamlet i august 2011 i en spørgeskemabaseret undersøgelse omfattende stat, regioner og kommuner. Alle landets kommuner og regioner modtager

[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).

spørgeskemaet. Inden for den statslige sektor indgår alle departementer, styrelser og direktorater samt de største uddannelsesinstitutioner (længerevarende og videregående). 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.

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 alle 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 varer typisk 1½ time og optages.

1.5 Rapportens struktur

Undersøgelsens resultater præsenteres i seks kapitler. I kapitel 2 beskrives metoder til at begå internetkriminalitet: Malware, phishing og DDoS-angreb. Efterfølgende redegøres for, hvor ofte henholdsvis privatpersoner, virksomheder og myndigheder oplever, at deres computer(systemer) angribes. Kapitel 3 har identitetstyveri som overskrift. I dette kapitel forklares begrebet identitetstyveri, og resultater fra offerundersøgelsen blandt 4.890 danskere præsenteres. Der skelnes i forbindelse hermed mellem tre typer af identitetsoplysninger, nemlig finansielle, traditionelle og digitale oplysninger. Desuden differentieres der mellem online og offline identitetstyveri. I kapitel 3 rettes blikket mod en specifik form for identitetstyveri: Netbankindbrud. Kapitel 4 handler i modsætning hertil om e-bedrageri, altså bedrageri i forbindelse med internethandel i internetbutikker og blandt private. I dette kapitel præsenteres også resultater fra offerundersøgelsen. Misbrug af betalingskort knytter sig både til identitetstyveri og e-bedrageri, hvorfor kortsvindel beskrives i et kapitel for sig selv, nemlig i kapitel 5. Her belyses omfanget af misbrug samt tabsfordelingen ved betalingskortmisbrug. Forebyggelse, sikring og overvågning af internetkriminalitet kastes der lys over i kapitel 6, mens kapitel 7 fokuserer på den repressive reaktion på diverse former for internetkriminalitet (anmeldelse og efterforskning). Rapporten slutter af med enkelte bemærkninger i kapitel 8.

Kapitel 2

Internetkriminelles værkstøjskasse

2.1 Malware

Når en enhed (computer, smartphone, tablet) tilsluttes internet, 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:

- *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 2.1 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 sine 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.

2.2 Phishing

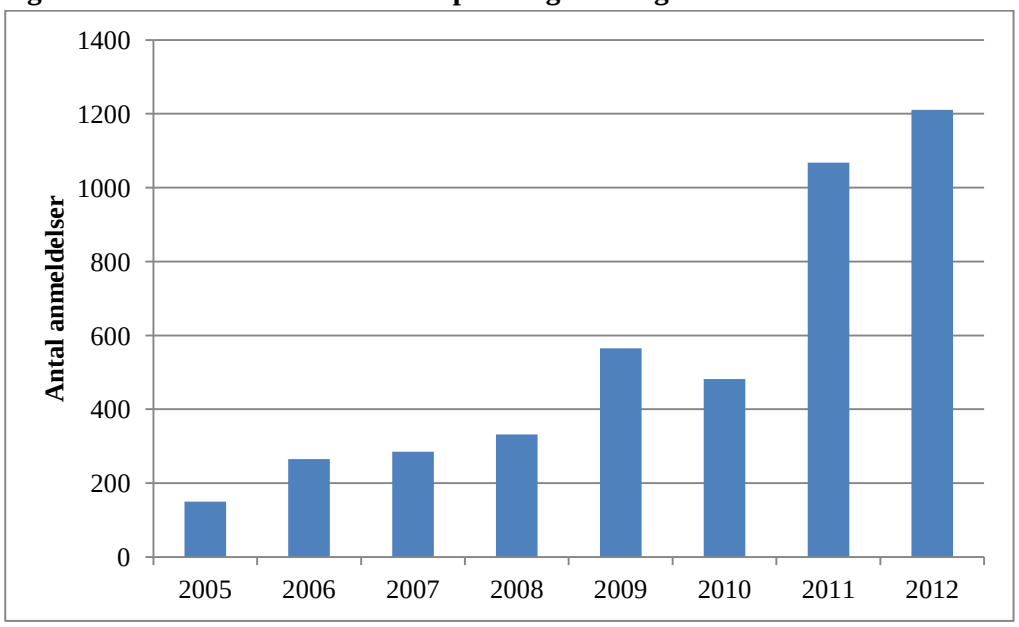
Formålet med phishing er at franarre offeret fortrolige oplysninger, typisk identitets- og finansielle oplysninger. Phishing sker hyppigst ved at en mail sendes til rigtigt mange adresser. For et par

hundrede dollars en mail sendes til en million e-mail-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 2.1 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 2.1 Danske internetsider med phishing-sider og malware



Kilde: DK•CERTs Trendrappport, adskillige årgange

2.3 DDoS-angreb

En form for angreb, som er specifikt rettet mod virksomheder og myndigheder, er DDoS-angreb. DDoS står for Distributed Denial of Service og er betegnelsen for et angreb, der bevidst overbelaster en internetserver i en sådan grad, at reelle forespørgsler til serveren ikke kan besvares i tide. Der sker ingen skade på hardware, og målet er ikke at bryde ind, men at genere offeret. Mest kendt i denne sammenhæng er Anonymous-bevægelsen med DDoS-angreb på FBI, CIA og andre

myndigheders internetsider. Danskerne stiftede for alvor bekendtskab med bevægelsen i forbindelse med fagforeningens konflikt med Restaurant Vejlegården. DK•CERTs skriver følgende om dette angreb (Ahmed et al, 2013, s. 26):

> Den 19. juli 2012 blev 3F's hjemmeside udsat for et Denial of Service-angreb, der gjorde den utilgængelig i flere dage. Angiveligt deltog folk fra blandt andet USA, Mexico, Brasilien, Spanien, Tyskland, Portugal og Australien i angrebet, som i første omgang blev proklameret af Twitter-brugeren Elan0r. Angrebene ramte siden både LO og HK's hjemmesider og berørte cirka 30.000 dagpengemodtageres mulighed for indberetning af ledighed med forsinket udbetaling af dagpenge til følge.

Der skelnes mellem DoS-angreb og DDoS-angreb. Forskellen er, at et DoS-angreb udføres fra en enkelt computer, mens mange computere indgår i et DDoS-angreb. For at udføre et DDoS-angreb benyttes ofte et botnet. Et botnet er en større samling af computere, der fungerer autonomt, men som kontrolleres af en bagmand, der typisk har kontrol med computerne via malware. Botnettet kan bruges til at sende spam, men også til at bombardere en virksomhed med så mange mails eller forespørgsler, at virksomhedens system bryder sammen (DDoS-angreb).

2.4 Omfanget af angreb på danskernes computere

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, 2012, s. 34).

I Danmarks Statistiks undersøgelser spørges der 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 tab af 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 2.2 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.

Tabel 2.2 Danskere der har været udsat for malware (seneste 12 måneder)

	2010	2011
Omfang stikprøve	4.588	4.988
Andel af udsatte internetbrugere i stikprøven	31 %	33 %
Antal udsatte husstande i Danmark[2]	675.000	765.000

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

Det er ikke overraskende, at malware er et meget udbredt fænomen. Men at så mange danskere taber informationer eller tid på grund af malware er bekymrende. At malware skader i sådan et omfang skyldes ikke, at danskere undlader at benytte sikkerhedssoftware. Langt hovedparten har installeret et antivirusprogram og har en firewall. Dog viser tabel 2.3 overraskende, at brugen af sikkerhedssoftware er faldet en anelse fra 2010 til 2011. Muligvis skyldes det den stigende popularitet af Apple-produkter (iMac, iPad), der traditionelt udsættes mindre for malware end computere, som benytter Windows styresystemer.

Tabel 2.3 Andel af internetbrugere der benytter sikkerhedssoftware/værktøj

	2010	2011
Antivirus software eller antispyware	83 %	77 %
Hardware eller software firewall	70 %	61 %
E-mail filter for at undgå spam	63 %	59 %
I alt	**89 %**	**86 %**

Kilde: Danmarks Statistik (2011, 2012).

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 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 2.4 viser oversigten:

[2] 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.

Tabel 2.4 Andel af internetbrugere som holdt sig fra aktiviteter på internet

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

Kilde: Danmarks Statistik (2011, 2012)

2.5 Omfanget af angreb på danske virksomhedernes IT-systemer

I 2011 gennemfører 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 medtages – 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 (se afsnit 2.5.2), 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 2.5 viser oversigten:

Tabel 2.5 Virksomhedernes bekymring[3] omkring cybercrime (2011)

	Danmark	Global
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 gerningsmænd. Mens den anden halvdel er splittet mellem at mene, at truslen kommer fra interne gerningsmænd (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.

2.6 Omfanget af angreb på danske myndighedernes IT-systemer

Danmarks Statistiks undersøgelse af myndighedernes IT-vaner er spørgeskemabaseret. Skemaet er sendt ud til alle landets kommuner, regioner, departementer, styrelser og statslige uddannelses-institutioner. Det svarer i alt til 202 skemaer, og 151 af dem er besvaret. Undersøgelsen viser, at 15 procent af myndighederne har været udsat for et virusangreb med tab af data eller arbejdstid til følge. Det lyder umiddelbart som et højt procenttal, det er derfor vigtigt at være opmærksom på, at

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

et 'ja' står fx for en kommune, det vil sige alle kommunale afdelinger og institutioner. Tabel 2.6 viser oversigten:

Tabel 2.6 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.

Kapitel 3

Identitetstyveri

3.1 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 definerer identitetstyveri som følgende:

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

Ifølge denne definition er der to led i forbindelse med identitetstyveri: (1) at tilegne sig en andens personoplysninger, og (2) at udgive sig for at være denne person. Rådet for IT-sikkerhed 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

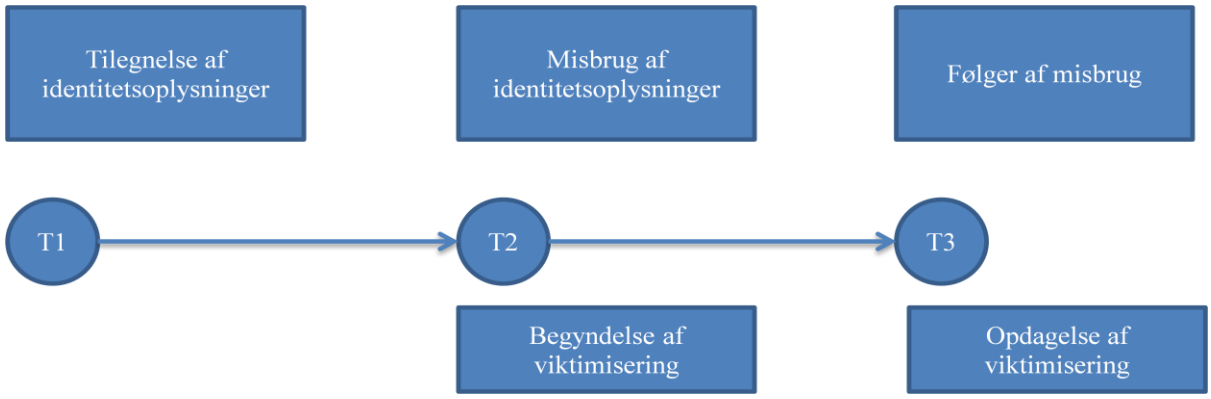
Assessment (OCTA) betragtes identitetssvig både som misbrug af rigtige personoplysninger og misbrug ved hjælp af fiktive oplysninger, mens identitetstyveri kun knytter sig til misbrug af rigtige personoplysninger.[4]

Det diskuteres også, 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, og The Federal Identity Theft and Assumption Deterrence Act fra 1998 inkluderer kortsvindel i begrebet identitetstyveri.[5]

I denne rapport anvendes Rådet for IT-sikkerheds definition af identitetstyveri, hvilket betyder, at brugen af en *fiktiv* identitet ikke regnes under begrebet identitetstyveri. Anvendelse af en anden persons identitet begrænses ikke til den digitale, virtuelle verden. Misbrug i offline verdenen knytter sig således også til begrebet identitetstyveri.

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 tager det også tid, førend forurettede opdager, at vedkommendes identitetsoplysninger er blevet misbrugt. Nedenstående skema viser processen.

Skema 3.1 Tre faser af identitetstyveri i tidsperspektiv



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

[4] "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).

[5] 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."

3.2 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 er identitetstyveri (ID Theft) defineret 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.

3.3 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 betalingskortoplysninger og adgangskoder 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 spørges der 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 spørges til, om respondenten har været udsat for dette misbrug inden for de sidste 12 måneder. Men kan respondenten huske, om det var 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 der gennemført en offerundersøgelse 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 4.890 respondenter i perioden oktober 2012 til og med februar 2013. Af disse 4.890 respondenter angiver 87 personer, eller 1,8 procent, at de har været udsat for identitetstyveri indenfor de sidste 12 måneder. Men 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.[6] (se tabel 3.1). Sammenlignet med en måling fra 2009 (Kruize, 2009) er der tale om en stigning i offerrisikoen. I 2009 svarer 1,1 procent af respondenterne, at de har været udsat for identitetstyveri indenfor de sidste 12 måneder. Stigningen er statistisk signifikant. Når procentdelen af respondenter, der har været udsat for identitetstyveri, i stikprøverne ganges op til at gælde hele den danske befolkning, er antallet af ofre steget fra ca. 48.000 i 2009 til ca. 73.000 i 2012. Det skal understreges, at denne offerrisiko gælder for den brede definition af identitetstyveri. Betalingskortmisbrug er således inkluderet, og det er desuden både online og offline identitetstyveri, der omfattes.

Tabel 3.1 Offerrisiko for identitetstyveri i Danmark

	2009	2012
Omfang stikprøve	1.853	4.890
Andel af udsatte for ID-tyveri	1,1 %	1, 8 %
95 % -interval	0,6 – 1,6 %	1,4 – 2,2 %
Antal ofre i Danmark (estimat)	47.850	73.420

Den brede definition af identitetstyveri kan opdeles i tre underkategorier:

1. Personer der har mistet økonomiske identitetsoplysninger/beviser, typisk betalingskort- og bankoplysninger.
2. Personer der har mistet traditionelle personoplysninger og/eller -beviser, typisk cpr-nummer, kørekort, pas og sygesikringskort.
3. Personer der har mistet digitale identitetsoplysninger, typisk adgangskoder til mail og sociale medier.

Tabel 3.2 viser resultatet ved denne opdeling. Som ventet udgør misbrug af økonomiske personoplysninger og/eller -beviser den største gruppe.

Tabel 3.2 Offerrisiko efter type af misbrugte identitetsoplysninger (2012 undersøgelse)

	Antal ofre	Procentdel	Offerrisiko
Økonomiske ID-oplysninger/beviser	50	62 %	1,1 %
Traditionelle ID-oplysninger/beviser	19	23 %	0,4 %
Digitale ID-oplysninger	12	15 %	0,3 %
I alt	**81**	**100 %**	**1,8 %**

Note: Risikoen er beregnet ved at relatere antallet af personer, som har været udsat for misbrug, til antallet af respondenter (4.890) i stikprøven. Ved 6 af ofrene mangler oplysninger, hvorfor de ikke kan inddeles i en de tre kategorier. Offerrisikoen er spejlet til alle 87 udsatte.

[6] 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 person-oplysninger. Når disse vægte anvendes stiger offerrisikoen for identitetstyveri fra 1,8 procent til 1,9 procent. På grund af denne marginale forskel er analysen gennemført uden vægterne.

Stikprøven fra undersøgelsen i 2009 er for begrænset til at opdele ofrene for identitetstyveri yderligere ud fra forskellige faktorer. Men stikprøveomfanget i 2012 tillader denne øvelse, der viser, at risikoen for at blive udsat for identitetstyveri falder med alderen. Når denne observation kombineres med de udsattes køn, så viser det sig, at unge mænd (under 30 år) har større risiko for at blive udsat for identitetstyveri. Denne offerprofil kan formentlig forklares med unge mænds adfærd på internettet. Hypotesen er dog ikke testet i undersøgelsen.

Tabel 3.3 Offerrisiko for identitetstyveri efter køn og alder (2012 undersøgelse)

	Mand	Kvinde	I alt
Under 30 år	3,1 %	2,0 %	2,6 %
30 – 49 år	1,7 %	1,9 %	1,8 %
50 år og ældre	1,5 %	1,3 %	1,4 %
I alt	**1,9 %**	**1,6 %**	**1,8 %**

Note: Antal ofre er 87, mens stikprøven omfatter 4.890 respondenter.

Offerrisikoen er uafhængig af uddannelsesniveau. Der er imidlertid en sammenhæng mellem erhverv og offerrisiko, hvilket tabel 3.4 viser. To af gruppernes – de studerendes og pensionisternes – offerrisici knytter sig formentlige til aldersvariablen. Men tabel 3.4 viser, at arbejde har en dæmpende effekt på risikoen for at blive udsat for identitetstyveri. Hvordan dette resultat skal tolkes er mere udfordrende, og jeg har ikke umiddelbart et bud herpå.

Tabel 3.4 Offerrisiko for identitetstyveri efter erhverv (2012 undersøgelse)

	Antal ofre	Antal respondenten	Offerrisiko
Med arbejde	48	2794	1,7 %
Uden arbejde	12	455	2,6 %
Studerende	18	662	2,7 %
Pensionister	9	972	0,9 %
I alt	**87**	**4.883**	**1,8 %**

Note: 7 respondenter har nægtet at oplyse deres erhverv. Uden erhverv omfatter også førtidspensionister. Efterlønsmodtagere hører til kategorien pensionister.

3.3.1 Tilegnelse af identitetsoplysninger

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 identitets-

tyveri indebærer, at der er tale om en handling i den fysiske verden. Denne kan dog være af teknisk art, fx skimming.

I offerundersøgelsen spørges respondenterne, om de har en idé om, hvordan gerningspersonen har fået fat i deres identitetsoplysninger. Blandt de 87 respondenter, der har været udsat for identitets-tyveri, svarer 59 (68 procent), at de har en formodning om, hvordan de har tabt deres oplysninger. Lidt over halvdelen (54 procent) mener, at deres oplysninger er blevet stjålet online, mens lidt under halvdelen (46 procent) tror, at det er sket offline. Tabel 3.5 viser en oversigt over de metoder, der efter respondenternes egen vurdering er blevet anvendt til tilegnelse af deres identitetsoplysninger.

Tabel 3.5 Anvendte metoder ved tilegnelse af identitetsoplysninger

	Antal	Procentdel subkategori	Procentdel i alt
Online identitetstyveri			
Malware (spyware)	9	28 %	15 %
Internethandel	9	28 %	15 %
Lagt selv/fundet på internettet	8	25 %	14 %
Falsk e-mail/internetside	6	19 %	10 %
I alt online	***32***	***100 %***	***54 %***
Offline identitetstyveri			
Tabt/stålet identitetsbeviser	10	37 %	17 %
Tabt/stjålet kort/bankoplysninger	9	33 %	15 %
Brug af betalingskort i udlandet	6	22 %	10 %
Selv oplyst i telefon	2	7 %	3 %
I alt offline	***27***	***100 %***	***46 %***
I alt	**59**		**100 %**

Note: 28 respondenter har ingen anelse om, hvordan deres identitetsoplysninger er blevet stjålet.

Oversigten viser, at ca. et ud af fire tilfælde kan tilskrives phishing: At fiske efter personoplysninger i den digitale verden (kategorierne malware og falsk e-mail/internetside i tabel 3.5). Svarkategorien 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.

3.3.2 Misbrug af identitetsoplysninger

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 sådan en situation 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 en andens digitale profil eller til at sende beskeder ud i udsattes navn.

Offerundersøgelsen viser, at hensigten med identitetstyveri i 81 procent af tilfældene er at opnå økonomisk gevinst. Hyppigst hæves eller overføres penge fra ofrets konto ved hjælp af betalingskort- eller kontooplysninger. Men oplysningerne anvendes også til blandt andet køb af varer og ydelser. Tabel 3.6 viser, at oplysninger, der tilegnes offline, ikke nødvendigvis anvendes offline.

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 eller kreditkort. 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 en anden vis. Offerundersøgelsen giver ikke mulighed for at skelne klart mellem disse to former for misbrug, men alt peger i retning af, at *account take over* er den mest anvendte metode.

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. 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

[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).

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 én respondent, at vedkommendes identitetsoplysninger er misbrugt i forbindelse med at vildlede myndighederne.

Tabel 3.6 Hensigt med misbrug af identitetsoplysninger efter tilegnelsesmetode

	Online	Offline	Ukendt	I alt	Procent
Økonomisk misbrug					
Købe på internettet	7	6	3	16	22 %
Købe i en butik	-	1	1	2	3 %
Leje noget/afslutte abonnement	-	1	1	2	3 %
Hæve penge	4	10	2	16	22 %
Overføre penge	9	4	2	15	21 %
Uspecificeret økonomiske misbrug	1	-	7	8	11 %
I alt økonomisk misbrug	***21***	***22***	***16***	***59***	***81 %***
Kriminelt misbrug	-	1	-	1	1 %
Socialt misbrug	11	-	2	13	18 %
I alt (oplyst formål)	***32***	***23***	***18***	***73***	***100 %***
Uoplyst formål	-	4	10	14	
I alt	**32**	**27**	**28**	**87**	

Omfanget af socialt misbrug er mindre end økonomisk misbrug, men fænomenet er formentlig i vækst. 18 procent af respondenterne rapporterer, at deres identitetsoplysninger er blevet misbrugt til at publicere noget på internettet eller sende e-mails ud. 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 logge ind på en jævnaldrende piges Facebook konto og ændre hendes profil. Hendes profilbillede ændres (i hendes ansigt samt en penis) og private beskeder gøres tilgængelige for alle, som hun er venner med på Facebook. 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. Chef-redaktøren 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

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

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).

3.3.3 Opdagelse af økonomisk misbrug

Når identitetsoplysninger misbruges med henblik på økonomisk gevinst, er det enten finansielle institutioner (bank eller kortindløser) eller ofret selv, der opdager misbruget. I kapitel 6 beskrives, hvordan banker og Nets overvåger kundernes pengeforbrug for at spotte misbrug. I tilfælde hvor (muligt) misbrug opdages, spærres betalingskortet eller bankoverførslen standses. Når ofret selv opdager misbrug, skyldes det typisk fratrukkede betalinger, som ikke kan genkendes, eller regning for noget, ofret ikke selv har købt.

Offerundersøgelsen viser, at det i fire ud af ti misbrugstilfælde er kortindløseren (Nets), der opdager misbruget og herefter spærrer betalingskortet. Blandt de tilfælde, hvor kortindløser (Nets) spotter misbruget, er der en ligelig fordeling af ofre, der har mistet deres oplysninger online og offline.

Tabel 3.7 Opdagelse af økonomisk misbrug af identitetsoplysninger

	Online	Offline	Ukendt	I alt	Procent
Betalingskort spærret	8	7	7	22	37 %
Fratrukket betaling (netbank eller udskrift)	6	8	4	18	31 %
Regning/opkrævning fra en virksomhed	5	3	4	12	20 %
Uoplyst	2	4	1	7	12 %
I alt	**21**	**22**	**16**	**59**	**100 %**

3.3.4 Tab på grund af misbrug

Ved økonomisk misbrug af identitetsoplysninger kan der opstå et tab. Men det sker ikke nødvendigvis: Banken eller kortindløseren stopper i visse tilfælde betalingen eller spærre kortet præventivt, og så er der intet økonomisk tab (se også afsnit 3.4 og kapitel 5). I offerundersøgelsen angiver 40 ud af de 59 respondenter, som har været udsat for økonomisk misbrug, at der var tale om et tab. 10 svarer ikke på spørgsmålet, hvorfor det antages, at der ikke var tale om økonomisk tab ved 9 ud af de 59 respondenter. Tabel 3.8 viser oversigten.

Det gennemsnitlige tab (blandt de 40 respondenter, der rapporterer om tab) er 10.884 kr. Gennemsnittet trækkes op på grund af to større beløber (70.000 og 100.000). Derfor ligger medianen på et lavere beløb, nemlig 3.800 kr. I alt er der samlet set tale om et tab på 435.360 kr. for de 40 respondenter.

Tabel 3.8 Tabets omfang på grund af økonomisk misbrug ved hjælp af identitetsoplysninger

	Antal	Procent
Intet tab	9	15 %
<= 1.000 kr.	10	17 %
1.001 – 5.000 kr.	13	22 %
5.001 – 10.000 kr.	9	15 %
>= 10.001 kr.	8	14 %
Uoplyst	10	17 %
I alt	**59**	**100 %**

I de fleste tilfælde hæfter ofrene ikke for tab, der knytter sig til økonomisk misbrug som følge af identitetstyveri. Der er dog en selvrisiko, som beskrives i betalingstjenesteloven § 62, stk. 2 (Karstoft, 2012). Denne paragraf bestemmer, at ofret skal betale højst 1.100 kr., når vedkommende mister sin pinkode. Dette er uanset, om det kan bebrejdes indehaveren af kortet – ved vold eller trussel om anvendelse af vold sker der undtagelse (se også afsnit 5.4). Offerundersøgelsen viser, at 11 ud af de 40 respondenter, der rapporterer om tab, (delvist) selv har hæftet herfor: 5 hæfter for de 1.100 kr., mens 5 hæfter for et mindre beløb, fordi tabet er mindre end 1.100 kr. 1 respondent hæfter for det fulde beløb (3.600 kr.).[9]

Tabel 3.9 Tabsfordeling mellem bank/forretning og kunden

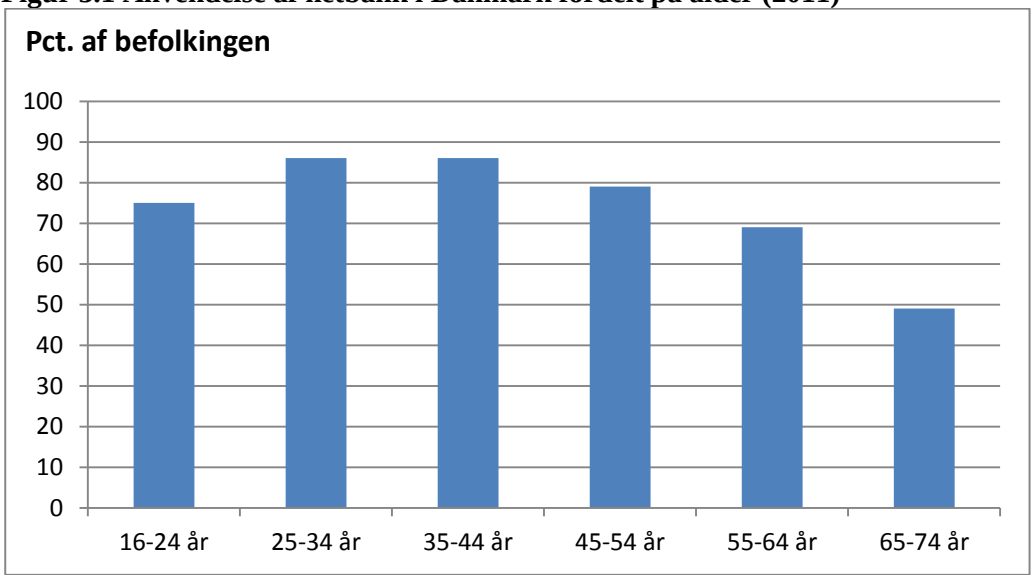
	Antal ofre	Beløb selvrisiko	Tab for bank/forretning	Tabet (i alt)
Ingen selvrisiko	29	-	368.060	368.060
Maks. Selvrisiko	5	5.500	55.100	60.600
Fulde beløb	6	6.700	-	6.700
I alt	**40**	**12.200**	**423.160**	**435.360**

3.4 Netbank

Tre ud af fire danskere i alderen 16-74 år anvender netbank i 2011. Det er markant flere end gennemsnittet i de 27 EU-lande, der ligger på knap fire ud af ti indbyggere. Norge fører an på listen over andelen af netbankbrugere. 85 procent af den norske befolkning benytter således netbank, mens udbredelsen er over 70 procent i henholdsvis Holland, Finland og Sverige (Danmarks Statistik, 2012). Set i et historisk perspektiv er anvendelsen af netbank i EU-landene næsten fordoblet i perioden fra 2005 til 2011. Ses der specifikt på Danmark er andelen steget fra knap 50 procent i 2005 til 75 procent i 2011. I Danmark er anvendelsen af netbank en anelse mere udbredt blandt mænd (77 procent) end kvinder (73 procent). Desuden aftager brugen af netbank med alderen, hvilket er forventeligt. Dog benytter knap halvdelen af aldersgruppen 65-74 år netbank. Figur 3.1 viser aldersfordelingen.

[9] Ifølge betalingsloven kan man hæfte for 8.000 kr., hvis det er undladt at underrette udbyder af kortet snarest muligt; hvis indehaveren overgiver pinkode, mens denne kunne/burde indse, at der var risiko for misbrug; hvis der er tale om groft uforsvarlig adfærd ved opbevaring af pinkoden.

Figur 3.1 Anvendelse af netbank i Danmark fordelt på alder (2011)



Kilde: Danmarks Statistik, 2012, Figur 22, s. 18

I Danmarks Statistiks undersøgelse af danskernes it-anvendelse i 2011 fremgår det, at risikoen for netbankindbrud afholder 14 procent af internetbrugerne fra at benytte denne internetaktivitet. Blandt danskerne har 90 procent internetadgang og 75 procent anvender netbank. Der er således 15 procent af de danske internetbrugere, der ikke har netbankadgang. Dette tal er stort set lig med de 14 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.

3.4.1 Netbankindbrud i Danmark

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 gerningsmanden skaffer sig adgang til en kundes netbank, men det lykkes ikke at overføre penge. Forsøg, hvor 'døren står åben' og gerningsmand ikke er til stede til at gennemføre *real time phishing*, er ikke talt 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 gerningsmanden at slippe af sted med penge.
- *Tabets omfang:* Beløbet som gerningsmanden slipper af sted med. Dette korrigeres, såfremt nogle af pengene kommer retur. Banken dækker tabet for privatkunder, mens

erhvervskunder selv hæfter for tabet.[10] Erhvervskunder kan tegne en forsikring for netbankindbrud – separat eller som en del af en kriminalitetsforsikring – ved deres forsikringsselskab.

Tabel 3.10 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 6). 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 gerningsmanden at opnå et udbytte.[11]

Tabel 3.10 Netbankindbrud i Danmark (2006-2012)

	Antal netbank-indbrud	Antal netbank-indbrud med tab	Procentdel af indbrud med 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

3.4.2 Netbankindbrud internationalt set

Antallet af netbankindbrud i Danmark ligger på et beskedent niveau ifølge interviewrespondenten fra Finansrådet. Dette skyldes ikke, at de danske banker er bedre sikret end udenlandske banker. Forklaringen må i stedet findes i det faktum, at Danmark er et lille land med et lille sprogområde, og bankerne er ikke så store. Et netbankindbrud er skræddersyet til en specifik bank, og dermed er store banker mere interessant for internetkriminelle. Chancen for at ramme en af kunderne i en stor bank er trods alt betydeligt større. Til sammenligning kan der ses på Holland, der er et land med tre gange så mange indbyggere som Danmark. Her taber bankerne 35 mio. euro (260 mio. kr.) på grund af netbankindbrud i 2011 (NVB, 2012, s. 33). I Danmark er tabet i dette år historisk lavt (0,2 mio. kr.), men også i andre år er tabet i Danmark betydeligt mindre end i Holland.

[10] 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.

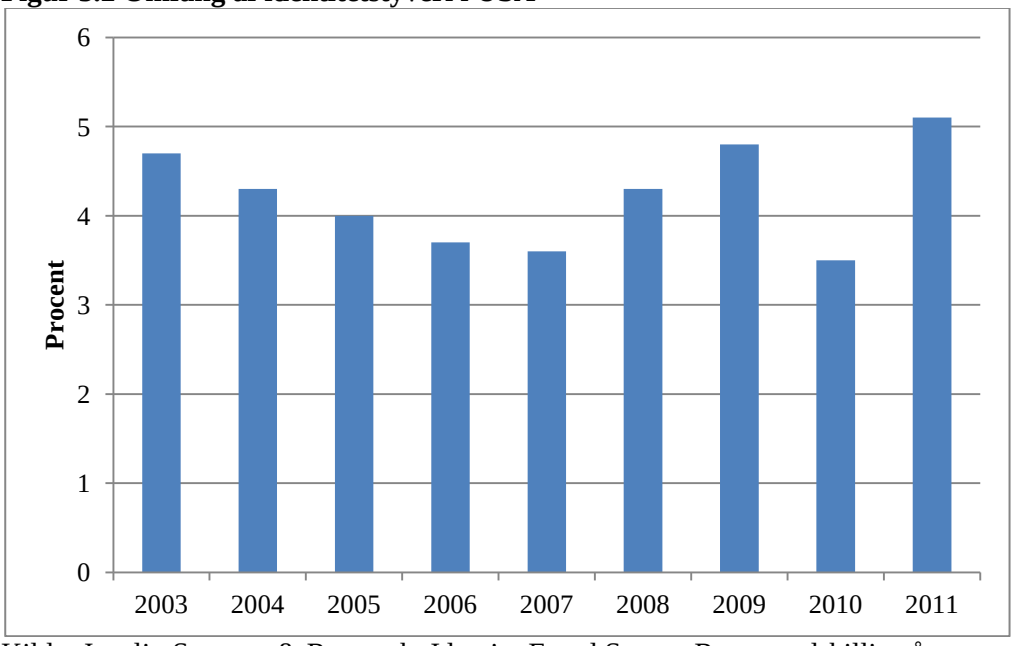
[11] Det gennemsnitlige udbytte kan påvirkes kraftigt af indbrud med store tab. Bankerne oplyser imidlertid ikke tabet pr. indbrud, så det er ikke muligt at beregne medianen eller at korrigere for ekstreme beløb.

3.5 Identitetstyveri i internationalt perspektiv

I de sidste par år er der kommet mere fokus på identitetstyveri i flere europæiske lande. Et af de første spørgsmål, som stilles, er: Hvor stort er omfanget? Dette spørgsmål er ikke nemt at besvare. Identitetstyveri er sjældent et juridisk begreb, hvorfor der ikke eksisterer offentlige statistikker, som afspejler fænomenet. Dette betyder, at man i stedet skal forsøge at se på delområder for at få et overblik over omfanget. I Norge forsøger de således at se på antallet af forsvundne pas, som sendes med posten. I 2010 ligger tallet på 537. Desuden har de i Norge også en statistik over hvor mange, der opretter et mobilabonnement med et falsk ID. Disse tiltag kan give en idé om omfanget, men ikke et samlet billede.

I Norge er der også gennemført offerundersøgelser. Men i modsætning til de danske undersøgelser er der spurgt til, om respondenterne har været udsat for, at nogen har misbrugt deres identitet indenfor de seneste *to* år. Der er gennemført undersøgelser de sidste tre år, og offerrisikoen ligger omkring 3 procent: 3,1 procent i 2010; 2,3 procent i 2011; 2,9 procent i 2012 (idtyveri.info). Da der er spurgt til en to års periode, er offerrisikoen ca. 1,5 procent på årsbasis. Et risikotal, der ligger i nærheden af, hvad der er målt i Danmark. Tallene fra Norge peger imidlertid ikke på en stigende tendens. I modsætning hertil tegner der sig i Danmark et billede af en stigning mellem de to målinger (2009 og 2012), der er dog for lidt data til at kunne fastslå tendensen.

Figur 3.2 Omfang af identitetstyveri i USA



Kilde: Javelin Strategy & Research: Identity Fraud Survey Report; adskillige årgange

For at få indblik i udviklingen af identitetstyveri må vi hellere vende blikket mod USA. Siden 2003 har Javelin Strategy & Research (JSR) undersøgt omfanget af identitetstyveri i en national repræsentativ stikprøve på næsten 4.800 voksne. Figur 3.2 viser, at der er tale om en faldende tendens fra 2003 til og med 2007. Fra 2008 sker der derimod en stigning, dog med et fald i 2010. Ifølge James Van Dyke, Javelins direktør, knytter denne stigning sig til den økonomiske krise: ”The

only thing we can logically attribute to that is the economy. If people need to make money, and decide to do so illicitly, identity fraud is the logical opportunity." (www.identitytheftassistance.org)

Kapitel 4

E-bedrageri

4.1 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 mest hyppigt 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 1.422 e-mærkede internetbutikker (pr. 20. marts 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. Men det er ikke kun forbrugere, der snydes af enten falske internetbutikker eller private sælgere, som ikke leverer de betalte vare. Butikker bedrages også af forbrugere, der ikke betaler for varerne eller anvender stjålne kortoplysninger i forbindelse med køb.

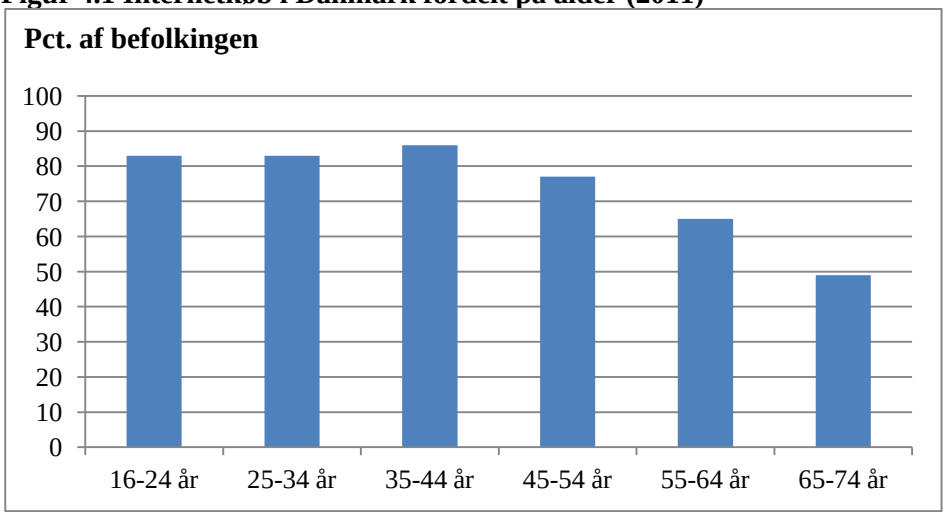
4.2 Internetbutikker

Den danske internethandel udgør i 2012 54,7 mia. kr., hvoraf 12,5 mia. ligger i udenlandske internetbutikker (FDIH, 2012b). Internethandel 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 4.1 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).

4.3 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.

Den Blå Avis

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.

QXL

I marts 2013 køber Lauritz.com QXL Danmark og QXL Norge. ”Lauritz.com’s strategi med købet af QXL er at udvide sit virkefelt, så der også kan tilbydes en auktionsplatform for varer under 800 kr. Lauritz.com’s eksperter takker dagligt nej til mange billigere varer; disse varer kan fremover med succes sælges via QXL”, lyder det i pressemeddelelsen.

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. Der kan købes og sælges både via auktionsprincippet og via fastpris-princippet. Ved oprettelse af en annonce betales normalt et oprettelsesgebyr (et mindre beløb). Desuden betales der når varen er solgt på auktion typisk 8 procent af salgsprisen, mens gebyret ligger på 6 procent, når varen er solgt for en fastpris.

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).

Lauritz.com

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. Lauritz.com har 20 auktionshuse fordelt i 4 lande: Danmark, Sverige, Belgien og Tyskland. På lauritz.com oplyses, at der er tre kvart mio. besøgende hver uge, og i 2011 er der lidt under 300 tusinde hammerslag og en omsætning på 724 mio. kroner. Ligesom ved køb på qxl.dk har købere på lauritz.com 14 dages fortrydelsesret. Det koster 12 procent i sælgersalær, dog minimum 250 kr., for at handle på lauritz.com.

4.4 Virksomheder og e-bedrageri

Respondenten fra FDIH påpeger, at dem der snyder netbutikker kan deles op i to grupper. Den første gruppe består af ikke-professionelle kriminelle, som misbruger forbrugerens beskyttelsesregler ved nethandel. Svindleren påstår, at varen (fx koncertbilletter) aldrig er modtaget, og at en anden person har indtastet svindlerens betalingskortoplysninger. Den anden gruppe består af mere professionelle kriminelle, der ofte bestiller varer eller ydelser med stjålne betalingskort-oplysninger.

FDIH har ingen statistik over hvor stort et beløb, internetbutikker snydes for. Men de har to gange gennemført mindre undersøgelser blandt deres medlemmer. Disse viser, at tab på grund af e-bedrageri ikke overstiger 1 procent af omsætningen, hvilket er lidt under, hvad der tabes i fysiske butikker: Her er tab på grund af butikstyveri i visse tilfælde 5 procent af omsætningen. De forskellige internetbutikker har ikke lige stor risiko for at blive udsat for bedrageri. Ifølge FDIH-respondenten er elektronik – specielt Apple-udstyr – i høj kurs. Det samme gælder for bestemte tøjmærker, såsom Canada Goose og Nike.

4.5 Privatpersoner og e-bedrageri

Ikke kun virksomheder udsættes for e-bedrageri, også privatpersoner oplever snyd på internettet. Det kan blandt andet ske i forbindelse med køb af varer eller ydelser i en falsk internetbutik, eller ved at private sælgere snyder. Omvendt kan en privat sælger føres bag lyset af en upålidelig køber.

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 e-bedrageri (se

bilag 1) til 4.890 respondenter i perioden oktober 2012 til og med februar 2013. Af disse 4.890 respondenter angiver 112 personer eller 2,3 procent, at de har været udsat for e-bedrageri indenfor de sidste 12 måneder. Da opgørelsen baserer sig på en stikprøve, medfører dette en vis statistisk usikkerhed.[12]

Offerundersøgelsen viser altså, at risikoen for e-bedrageri er 2,3 procent. Når dette procenttal skal ganges op til hvor mange danskere, der udsættes for e-bedrageri, 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 e-bedrageri, 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 e-bedrageri. I tabel 4.1 sættes de 2,3 procent derfor både i relation til personer og til husstande. I forbindelses med personer svarer procenttallet således til 96.000, mens det drejer sig om 60.000 husstande. Formentligt placerer det virkelige tal sig mellem disse to resultater, og dermed er et godt bud, at ca. 75.000 udsættes for e-bedrageri.

Tabel 4.1 Offerrisiko for e-bedrageri i Danmark (2012)

	Butikshandel	Privathandel	I alt
Omfang stikprøve	4.890	4.890	4.890
Antal udsatte	75	37	112
Andel af udsatte for e-bedrageri	1,5 %	0,8 %	2,3 %
95 % -interval	1,2 – 1,8 %	0,6 – 1,0 %	1,9 – 2,7 %
Antal udsatte i Danmark (personer)	64.000	32.000	96.000
Antal udsatte i Danmark (husstande)	40.000	20.000	60.000

Tabel 4.1 viser desuden, at ca. to ud af tre personer, der har oplevet e-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 handel er også knyttet til dette forhold, men denne kategori inkluderer desuden, at sælgeren ikke modtager sin betaling. Ved de 37 private handler, der er registreret i undersøgelse i forbindelse med e-bedrageri, modtog 28 personer ikke varen eller ydelsen, mens 9 personer oplyser, at de ikke modtog betaling fra køberen.

[12] 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 e-bedrageri fra 2,3 procent til 2,4 procent. På grund af denne marginale forskel gennemføres analysen uden vægte.

4.5.1 Offerprofil ved e-bedrageri

Udsathed for e-bedrageri hænger sammen med borgernes alder. Ældre danskere har således en mindre risiko for at blive udsat for bedrageri på internettet. Dette hænger formentligt sammen med, at ældre ikke lige så hyppigt køber varer og ydelser på internettet. Der er ingen store forskelle i offerrisikoen for mænd og kvinder. Tabel 4.2 viser, at kvinder mellem 30 og 49 år har den største offerrisiko for e-bedrageri. Når denne gruppe opdeles yderligere i kvinder i henholdsvis alderen 30-39 år og 40-49 år, viser det sig, at de 30-39-årige kvinder har en offerrisiko på 5,0 procent.

Tabel 4.2 Offerrisiko for e-bedrageri efter køn og alder

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

Note: Antal ofre er 112, mens stikprøven omfatter 4.890 respondenter.

Risikoen for at blive udsat for e-bedrageri er lidt højere for danskere med arbejde sammenlignet med danskere uden arbejde. Studerende har den største risiko, mens pensionister klart har den mindste offerrisiko for e-bedrageri.

Tabel 4.3 Offerrisiko for e-bedrageri efter erhverv

	Antal ofre	Antal respondenten	Offerrisiko
Med arbejde	74	2.794	2,6 %
Uden arbejde	10	455	2,2 %
Studerende	21	662	3,2 %
Pensionister	7	972	0,7 %
I alt	**112**	**4.883**	**2,3 %**

Note: 7 respondenter har nægtet at oplyse deres erhverv. Kategorien 'uden arbejde' omfatter også førtidspensionister, mens efterlønsmodtagere hører til kategorien pensionister.

4.5.2 Butikshandel og e-bedrageri

Varekategorien 'tøj, sko og smykker' placerer sig øverst på listen over produkter, som der snydes mest med i forbindelse med køb via (falske) internetbutikker (ifølge købernes egne oplevelser). Der er således 38 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 23 procent af bedragerierne med vare i en (falsk) internetbutik, mens dens andel af nethandelomsætningen kun udgør omkring 5 procent. Tabel 4.4 viser hele oversigten.

Tabel 4.4 Butikshandel og e-bedrageri: varekategorier

	Antal	Procentdel	Nethandel*
Tøj, sko og smykker	24	38 %	16 %
Kosmetik, medicin og kosttilskud	15	23 %	5 %
Elektronik og hvidevarer	7	11 %	9 %
IT, tele og foto	5	8 %	13 %
Bolig, have og blomster	5	8 %	6 %
Auto-, både- og cykeludstyr	3	5 %	3 %
Sports- og fritidsudstyr	2	3 %	4 %
Film, musik, bøger, spil og legetøj	2	3 %	17 %
Rejser og kulturoplevelser	1	2 %	17 %
I alt	**64**	**100 %**	

* FDIH handelsanalyse 2012 (FDIH 2012b, s. 17)

I alt har 75 personer oplevet bedrageri i forbindelse med køb i en internetbutik. I tabel 4.4 optræder 64 af disse. De 11 resterende har bl.a. oplevet snyd i forbindelse med køb af et abonnement (2 personer), en billet, en massagetime og levering af blomster.

4.5.3 Privat handel og e-bedrageri

I forbindelse med handel privatpersoner imellem, hvor en af parterne udsættes for e-bedrageri, placerer varekategorien 'tøj, sko og smykker' sig også øverst på listen over produkter, som der snydes mest med. På listen efterfølges denne varekategori af 'IT, tele og foto'. Tabel 4.5 viser oversigten.

Tabel 4.5 Butikshandel og e-bedrageri: varekategorier

	Antal	Procentdel
Tøj, sko og smykker	10	27 %
IT, tele og foto	7	19 %
Bolig, have og blomster	6	16 %
Elektronik og hvidevarer	4	11 %
Rejser og kulturoplevelser	4	11 %
Auto-, både- og cykeludstyr	3	8 %
Sports- og fritidsudstyr	2	5 %
Film, musik, bøger, spil og legetøj	1	3 %
I alt	**37**	**100 %**

4.5.4 Tab på grund af e-bedrageri

Blandt respondenterne har i alt 9 personer privat solgt noget på nettet uden at modtage betalingen. I 8 af tilfældene er der tale om mindre beløb fra 200 kroner op til 1.500 kroner. Mens en respondent beretter om et tab på 95.000 kr. i forbindelse med et bilsalg.

De øvrige 103 respondenter, der har været udsat for e-bedrageri, har købt noget på nettet: 75 af dem i en (falsk) internetbutik og 28 hos en privat sælger. Respondenterne, der har købt hos en privat

sælger, taber i 25 ud af de 28 tilfælde deres penge. To af de tre respondenter, der har fået dækket deres tab, har handlet for forholdsvis store beløb (7.000 og 10.000 kr.). 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 4.6 Tabsfordeling ved e-bedrageri

	Antal ofre	Tabet (i alt)
Butikshandel		
Betaler selv	55	96.658
Tab dækket	20	152.911
Butikshandel i alt	***75***	***249.569***
Privat handel		
Købt på nettet	28	75.326
Solgt på nettet	9	101.420
Privat handel i alt	***37***	***176.746***
I alt	**112**	**426.315**

Tabel 4.6 viser, at det samlede tab ligger på 426.315 kr. Det svarer til et gennemsnit på næsten 4.000 kr. Dette er dog 'kunstigt' højt på grund af enkelte store beløb. I mere end halvdelen af e-bedrageri sagerne er tabsbeløbet under 1.000 kr. Tabel 4.7 viser oversigten.

Tabel 4.7 Tabsbeløb ved e-bedrageri

	Butikshandel	Privat handel	I alt
Under 1.000 kr.	44	15	59
1.000 – 4.999 kr.	24	16	40
5.000 – 9.999 kr.	3	3	6
10.000 kr. eller mere	4	3	7
I alt	**75**	**37**	**112**

Kapitel 5

Misbrug af betalingskort

Betalingskort spiller en central rolle i forbindelse med internethandel, og stjålne oplysninger kan derfor anvendes til køb af enten varer eller ydelser. I sådanne tilfælde hører kortmisbrug til under begrebet *identitetstyveri*. I kapitel 3 er denne form for identitetstyveri knyttet til misbrug af økonomiske identiteter eller beviser. Forbrugere kan imidlertid også snydes, i forbindelse med at de selv anvender deres betalingskort på nettet: De køber en vare eller en ydelse i en (falsk) netbutik, og pengene trækkes fra kortet. Men varen leveres ikke. I sådanne tilfælde hører kortmisbrug til under begrebet *e-bedrageri*. Kortmisbrug kan således både knytte sig til identitetstyveri og e-bedrageri, hvorfor oplysninger omkring betalingskortsmarked her får et kapitel for sig.

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. [13] 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):

[13] 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).

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 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.

I*nternationale 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 Kortmisbrug

Der findes forskellige metoder, hvorved 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.[14]

En tredje måde, hvorpå betalingskort kan misbruges, forgår på internettet. Kortoplysninger franarres enten ved hjælp af phishing (se også afsnit 2.3), aflures med spyware (se også afsnit 2.2) 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.

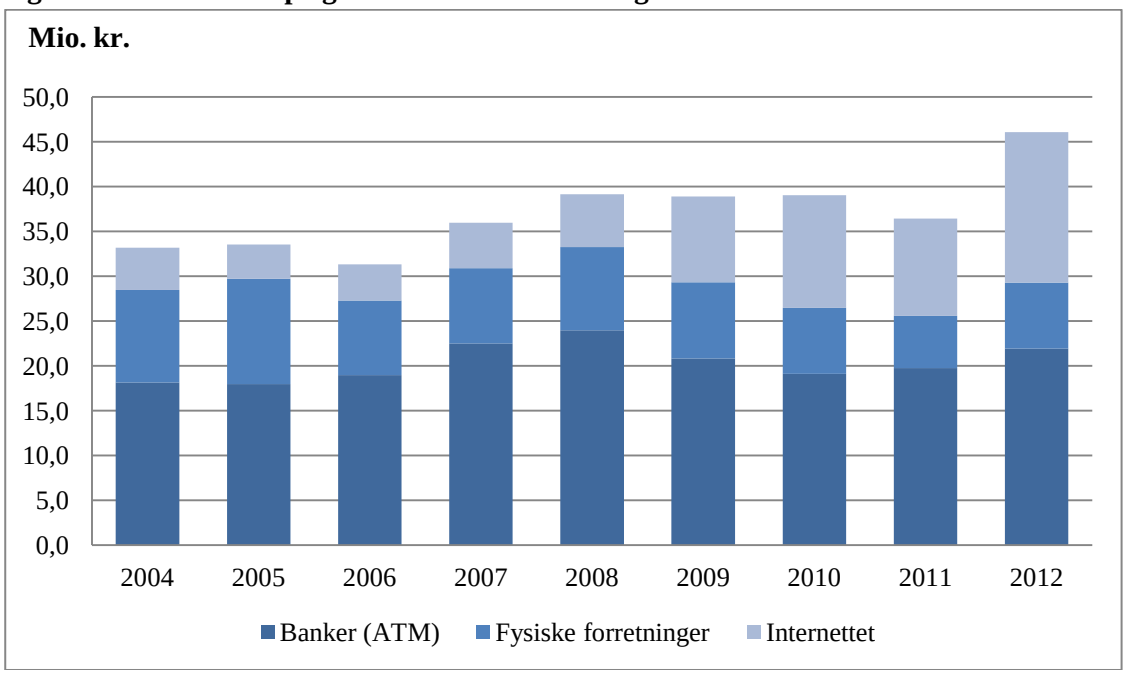
[14] Denne praksis har medført, at fx Rabobank (en hollandsk bank) ikke tillader brug af betalingskort uden for EU, medmindre kunden søger dispensation herfra.

5.3 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 om 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[15]: Indtastning af kortnummer, kontrolcifre og udløbsdato

Figur 5.1 Samlede tab på grund af Dankortmisbrug



Kilde: Nets (egne beregninger)

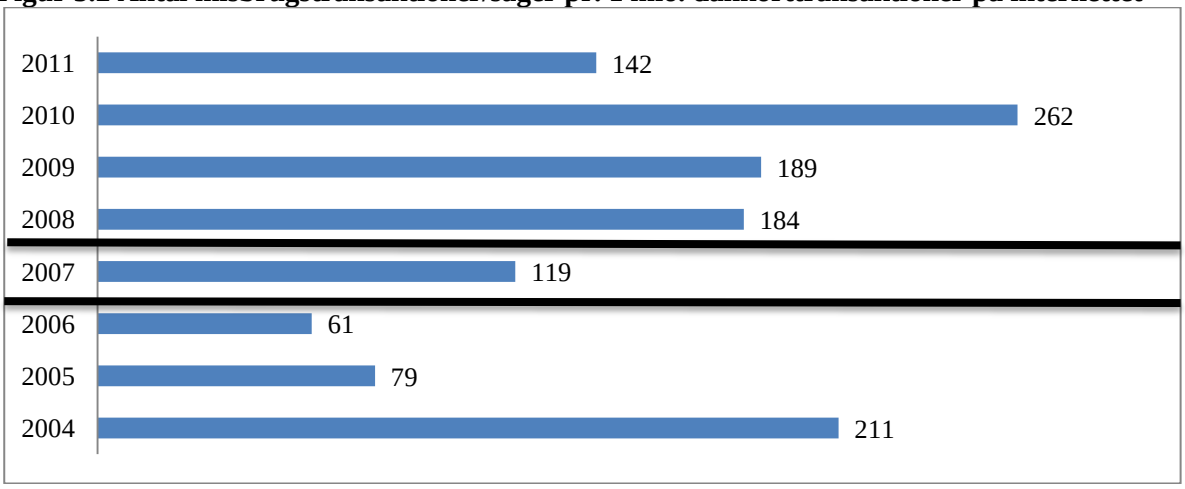
Figur 5.1 viser tabet i perioden 2004 til 2012. Det samlede tab stiger i denne periode fra 33,2 mio. kr. i 2004 til 46,1 mio. kr. i 2012. Det svarer til en stigning på 39 procent. Figuren viser desuden, at internettet benyttes oftere og oftere ved misbrug af Dankort i perioden fra 2004 til 2012. I 2004 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.

[15] 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 Dankorttransaktioner 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

5.4 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 findes 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 først 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.

5.5 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 er beskrevet i betalingstjenesteloven § 62, stk. 2. Der skelnes mellem tre størrelser knyttet til selvrisikobeløbet (Karstoft, 2012):

- 1.100 kr. 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.

Regler 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 betyder, 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 nettet – kontrolleres kortoplysningerne af Nets. Hvis kortet ikke er spærret, eller kortbrugen ikke virker mistænksom (fx brug af kortet inden for meget kort tid), så gennemføres betalingen uden at tjekke ved kortudstederen (banken), om der er dækning på kortet. Der er i princippet ikke et maksimum beløb, der 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 for 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 5.1 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 5.1 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.

5.6 Kortmisbrug i Danmark internationalt set

Den Europæiske Central Bank (ECB) publicerer tal om kortmisbrug i eurolandene.[16] I denne opgørelse anvendes samme opdeling, som Nets benytter i forbindelse med Dankortmisbrug statistik: banker (ATM), fysiske forretninger (POS) og internet (CNP). Det viser sig, at kortmisbrug forgår i mindre grad på internettet i Danmark sammenlignet med eurolande. 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 5.2 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

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

[16] SEPA: Single Euro Payments Areas

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.

Kapitel 6

Forebyggelse, sikring og overvågning

Ved forebyggelse af internetkriminalitet har både privatpersoner, virksomheder og myndigheder en rolle. Privatpersonerne er forbrugerne, og de repræsenteres bl.a. af Forbrugerrådet. Deres primære interesse er at minimere den (økonomiske) risiko, de jager dog oftest samtidig det billige og nemme alternative. Virksomhedernes fokus er profit, hvilket betyder, at de sælger deres produkter således, at de tjener mest på dem. I hvilken grad myndighederne blander sig i denne dans mellem forbrugerne og virksomhederne afhænger af den pågældende samfundsmodel og politiske overbevisning. I den danske velfærdsstat er myndighedernes rolle traditionelt set stor.

Til at starte med omhandler dette kapitel, hvordan computere[17] er sikret i dagens Danmark. Efterfølgende ses der nærmere på sikring mod betalingskortmisbrug og sikring mod netbankindbrud. Kortmisbrug og netbankindbrud forebygges ikke kun med teknisk sikring, men også ved overvågning.

6.1 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.

[17] Siden man kan komme på nettet med langt flere apparater end traditionelle computere – tablets, smartphones, printere, fjernsyn og så videre – skal computeren tolkes i bred forstand.

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, og dermed blandt andet kan anvendes i et botnet. Botnet er en forkortelse for robot netværk, hvilket betyder et netværk af computere, der kan fjernstyres. DDoS angreb udføres typisk med hjælp fra et botnet.

Nedlæggelse af myndigheders og virksomheders internetsider er næsten daglig kost i første halvår af 2013. I Danmark udsættes NemID for DDoS-angreb, og politikerne er derfor på dupperne i forhold til bedre sikring heraf. Ifølge anonyme kilder i hackermiljøet er det uhyre simpelt at nedlægge NemID med hjælp fra en såkaldt *booter*, som kan købes for 10 dollars på nettet. DanishLutzTeam tager ansvaret for angrebene på NemID (Politiken, 12. april 2013). I Holland er adskillige storbanker – ING, Rabobank, ABN-AMRO, SNS – blevet ramt af DDoS-angreb, og betalingssystemerne (netbank, mobilbank) er som følge heraf ude af drift i op til flere dage. Det nyoprettede Center for Cybersikkerhed ved Forsvarets Efterretningstjeneste bemærker, at ”DDoS er relativt lette at iværksætte, og imødegåelse af DDoS kræver forberedelse hos virksomheder og myndigheder. (…) For at kunne forsvare netværket i dag har virksomhederne behov for at implementere DDoS-sikkerhed i flere lag, fra netværksperimeteren til ISP’ens backbone.” (CFCS, 2013, s. 5)

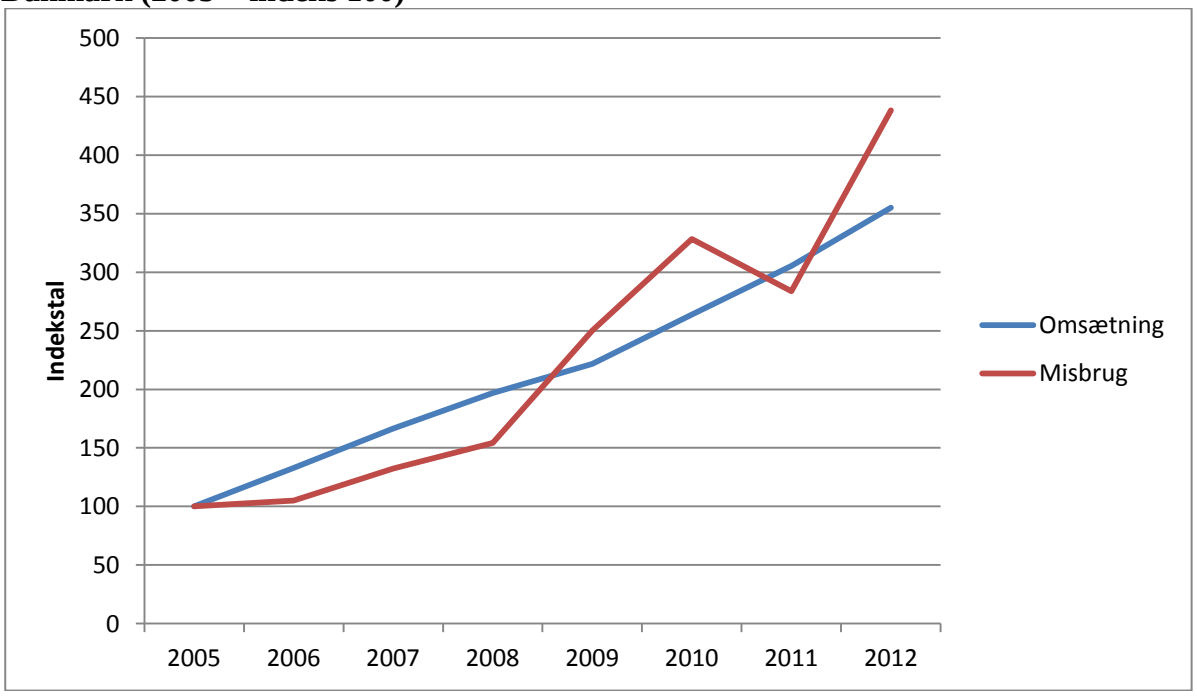
6.2 Betalingskortsikring

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.[18] 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, der 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 6.1).

Figur 6.1 Indekseret udvikling af omsætning og misbrug af Visa/Dankort ved internethandel i Danmark (2005 = indeks 100)



Kilde: Nets (egne beregninger)

[18] 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.

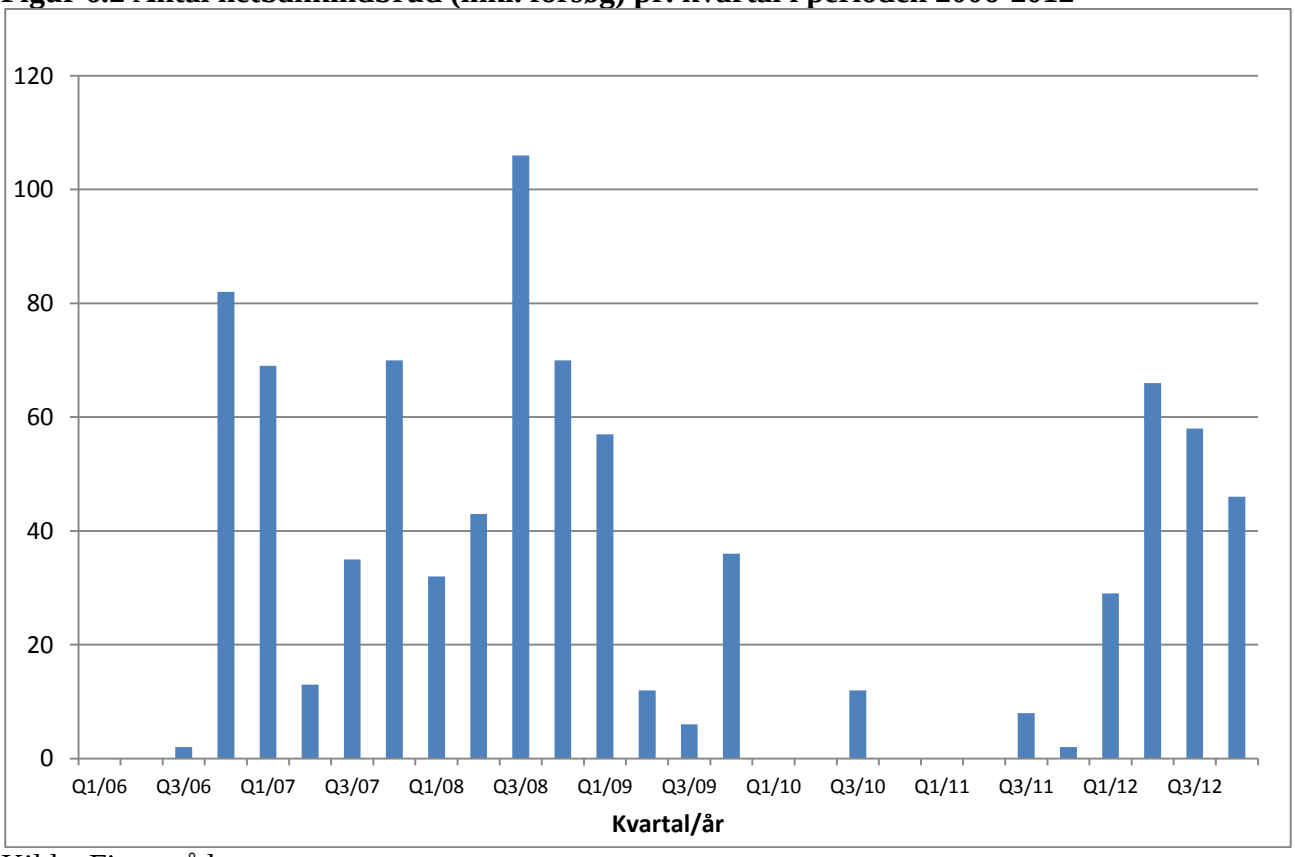
6.3 NemID som to-trins sikring

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[19] 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 6.2 Antal netbankindbrud (inkl. forsøg) pr. kvartal i perioden 2006-2012



Kilde: Finansrådet

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

Figur 6.2 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.

6.4 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 netbankindbruddene.

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 erfaringsbaserede 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.

6.5 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.

DDoS-angreb

Den enkelte virksomhed bør i relation til DDoS-angreb - og andre cybertrusler – foretage en risikovurdering. I forbindelse hermed er det væsentligt at overveje konsekvenserne ved manglende adgang til virksomhedens internetside og/eller andre dele af IT-infrastrukturen. Der er ISP'er i Danmark, der tilbyder DDoS-værn. Internetsider eller tjenester som understøtter kritiske systemer, eller som af andre årsager har brug for forstærket robusthed, bør overveje DDoS-værn (CFCS, 2013, s. 5).

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.

Kapitel 7

Anmeldelse og efterforskning

7.1 Politiets anmeldelsesstatistik

Politiets sagsstyringssystem – Polsas – bruger gerningskoder, som er inspireret af straffeloven. Det kan derfor være svært at genkende nye kriminalitetsfænomener. Dette gælder eksempelvis for identitetstyveri (se også afsnit 3.2). 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.

DDoS-angreb

Bagger Tranberg og Langsted (2012) redegør for hvilke straffelovsparagraffer, der kan anvendes i forbindelse med angreb på computere. Hvis angrebet retter sig mod særligt vigtige computere og informationssystemer, fx Skats eller en storbanks, kan der være tale om overtrædelse af straffelovens § 193, stk.1. Det er sjældent, at denne paragraf anvendes i praksis. Den mest oplagte straffelovsparagraf i forbindelse med angreb på computere og informationssystemer er § 293, stk. 2. Lovteksten lyder: "Den, der uberettiget hindrer en anden i helt eller delvist at råde over ting, straffes med bøde eller fængsel indtil 1 år". Denne paragraf ændres i 2004 med henblik på at kunne omfatte blandt andet DDoS-angreb (Bagger Tranberg og Langsted, 2012, s. 699). Straffelovens § 293 kendes under betegnelse 'brugstyveri'. I politiets anmeldelsesstatistik er der en stribe Polsas-koder for brugstyveri, de fleste knytter sig til brugstyveri af transportmidler. Der findes desuden en kode med navnet 'hindring af andres ret', som henviser til § 293, stk. 2. Denne gerningskode anvendes imidlertid sjældent.

Hacking

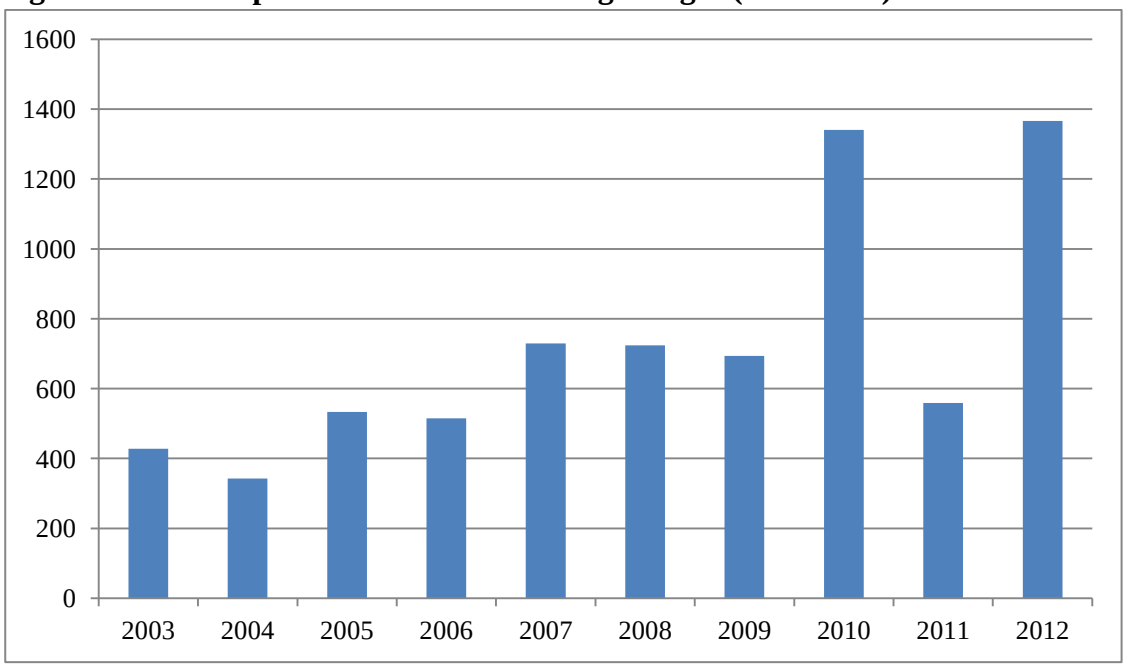
Uberettiget adgang til computere og informationssystemer er kendt under begrebet hacking og er kriminaliseret i straffelovens § 263, stk. 2: "Den, som uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem, straffes med

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. Borgerne 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 og misbrug af betalingskort på nettet er forbrydelser, som typisk hører hjemme under databedrageri. Figur 7.1 viser udviklingen i disse anmeldelser. Som det ses er antallet af anmeldelser stigende 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 7.1 Antal af politianmeldte databedragerisager (2003-2012)



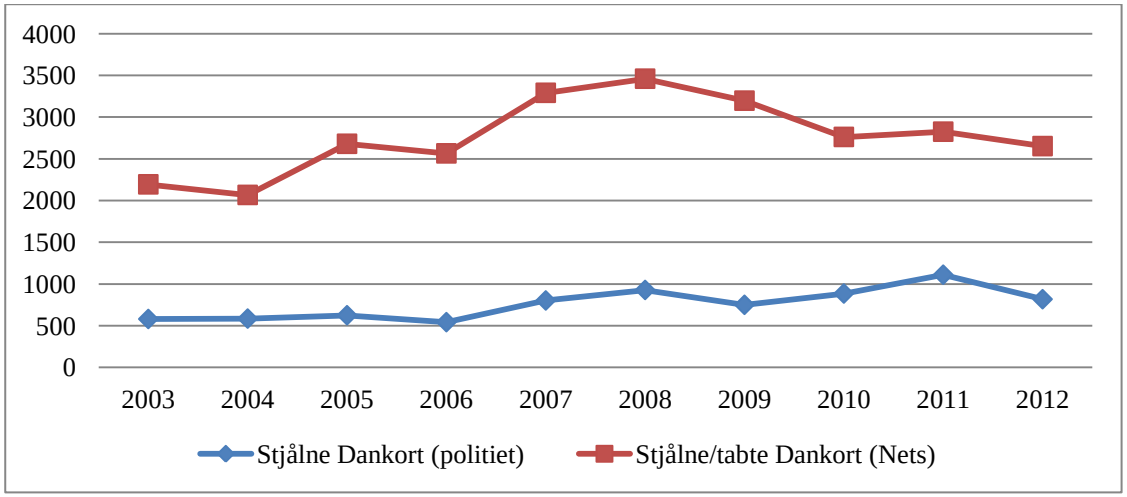
Kilde: Danmarks Statistik/ Rigspolitiet

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 7.2 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 7.2 Antal af anmeldte bedragerisager med stjålne Dankort (politiet vs. Nets)

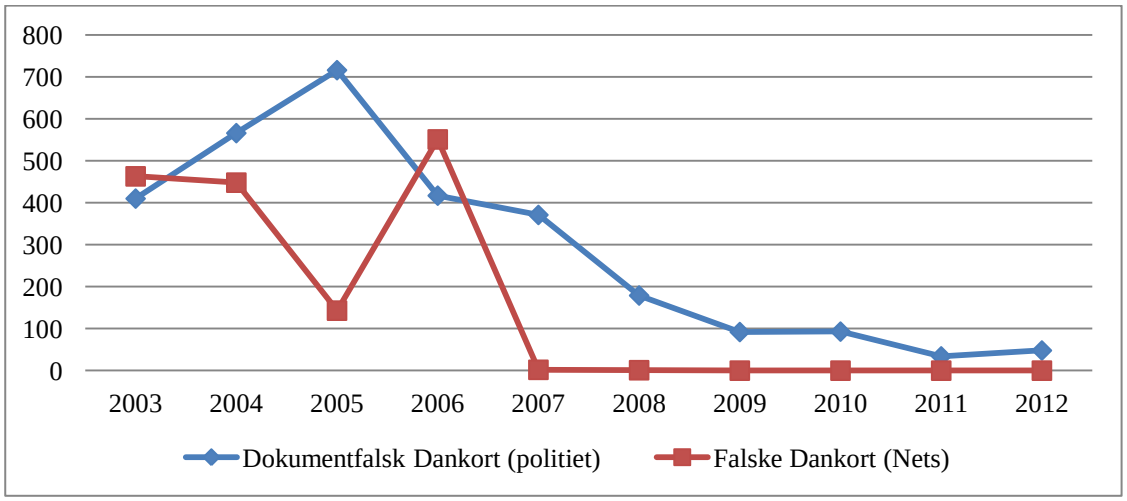


Kilde: Danmarks Statistik/Rigspolitiet og Nets

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 7.3 Antal af anmeldte dokumentfalsksager Dankort (politiet vs. Nets)



Kilde: Danmarks Statistik/Rigspolitiet og Nets

Netbankindbrud
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.

7.2 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 gerningsmanden (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.

7.3 Politianmeldelse og opklaring af identitetstyveri og e-bedrageri

I offerundersøgelsen af identitetstyveri og e-bedrageri (resultaterne omtales i kapitel 3 og 4) spørges der til, hvorvidt de respondenter, der har været udsat for internetkriminalitet, har meldt sagen til politiet, og i så tilfælde om sagen er opklaret.

Tabel 7.1 viser resultaterne for de, der har været udsat for identitetstyveri. Det skal bemærkes, at en person, der udsættes for betalingskortmisbrug, ikke nødvendigvis selv skal anmelde sagen til politiet (se også afsnit 7.1). Når kortindløseren (Nets) spærrer kortet, er det ofte dem eller banken, der anmelder sagen. Dette spørges der ikke til i offerundersøgelsen, hvorfor det antages i tabel 7.1, at der altid sker anmeldes ved kortspærring. Hvis denne antagelse holder, er omkring halvdelen af

identitetstyverierne anmeldt til politiet. Tabel 7.1 viser, at anmeldelsestilbøjelighed ikke er ens for de tre typer af identitetsoplysninger, der misbruges.

Tabel 7.1 Anmeldelsestilbøjelighed ved identitetstyveri

	Antal ofre	*Anmeldelse*	*Spærret*	*Anmeldelses-procent*
Økonomiske ID-oplysninger/beviser	50	13	22	70 %
Traditionelle ID-oplysninger/beviser	19	4	-	21 %
Digitale ID-oplysninger	12	1	-	8 %
I alt	**81**	**18**	**22**	**49 %**

Ved seks ofre mangler oplysninger til at inddele dem i en de tre kategorier, to af dem har anmeldt sagen til politiet.

I alt svarer 20 respondenter i offerundersøgelsen, at de har anmeldt identitetstyveriet til politiet. Politiet optager i alle disse sager anmeldelse. 4 ud de 20 respondenter (20 procent) svarer, at politiet har opklaret sagen: 2 af sagerne knytter sig til betalingskort og de 2 øvrige til stjålne ID-beviser/cpr-numre. Om politiet har opklaret andre af de 16 sager, ved vi ikke, men respondenterne har i hvert fald ikke kendskab til det.

Tabel 7.2 viser, hvor ofte udsatte for e-bedrageri melder sagen til politiet. I alt svarer 15 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 tre af tilfældene afviser politiet anmeldelsen. Det handler i alle tre sager om et privat køb: Der er således solgt en vare (henholdsvis bog, mobiltelefon og Louis Vuitton taske) over nettet, men betalingen er aldrig modtaget. Hvorfor politiet afviser anmeldelsen er ikke kendt.

Tabel 7.2 Anmeldelsestilbøjelighed ved e-bedrageri i Danmark

	Antal ofre	*Anmeldelse*	*Anmeldelses-procent*
Butikshandel	75	4	9 %
Privathandel	37	13	35 %
I alt	**112**	**17**	**15 %**

Politiet opklarer halvdelen (7) af de 14 e-bedragerisager, hvori anmeldelse er optaget. 1 af de 4 anmeldte butikshandel bedragerisager er opklaret, mens 6 ud af de 10 anmeldte privathandel bedragerisager er opklaret.

Kapitel 8

Afsluttende bemærkninger

I rapportens indledende kapitel bemærkes, at en voksende del af kriminaliteten foregår på nettet. I denne undersøgelse har to former for berigelseskriminalitet været i fokus, henholdsvis identitetstyveri og bedrageri i forbindelse med internethandel. Det viser sig, at disse former for kriminalitet kan betragtes som *high volume* kriminalitet. Offerundersøgelsen viser, at 1,8 procent af danskerne har været udsat for identitetstyveri i 2012, og der er hovedsageligt tale om misbrug af økonomisk identitet. Desuden har 2,3 procent af danskerne ifølge offerundersøgelsen været udsat for e-bedrageri i 2012. Til sammenligning ligger offerrisikoen for cykeltyveri ligeledes på ca. 2 procent.[20]

Udsathed for identitetstyveri på internettet kan (til dels) forebygges ved at overholde visse færdselsregler, blandt andet skal den enkelte internetbruger være opmærksom på, at følsomme identitetsoplysninger ikke oplyses til ukendte, og at software, antivirusprogrammer og firewalls opdateres jævnligt. Men realiteten viser, at ikke alle internetbrugere er varsomme og ved, hvordan de skal opføre sig på nettet. I forlængelse heraf kan det diskuteres, hvorvidt og i hvilken grad brugere skal være ansvarlige for deres egen sikkerhed på nettet. Ovenfor anvender jeg ordet færdselsregler, hvilket fører mine tanker hen på en sammenligning mellem computeren og bilen: Sikker bilkørsel kræver, at chaufføren opfører sig fornuftig i trafikken. Men bilejeren er ikke ansvarlig for, at airbags og ekstra udstyr er installeret forsvarligt i bilen. Desuden afleverer de fleste bilejere deres bil til service, hvor olie, bremser og så videre tjekkes. Derimod står computerejeren selv med ansvaret for mange sammenlignelige opgaver.

I Danmark blander staten sig i høj grad i vedligeholdelsen af borgernes private ejendomme, blandt andet kræves et årligt eftersyn af oliefyr og varmepumper. I kommunen, hvor jeg bor, er husejerne tvunget med i en ordning vedrørende årlig tømning af bundfaldstanke. Staten kræver desuden en del i forbindelse med sikkerhed, blandt andet skal børn køre med cykelhjelm. Men på nettet kan danskere færdes ude sikkerhed. Det kan diskuteres i hvor høj grad, den danske stat skal blande sig i borgernes private adfærd. Dog er det tankevækkende, at der ingen krav er på så omfangsrigt og vigtigt område som internettet.

---

[20] Ca. 12 procent af danskere udsættes for en form for tyveri i 2011, og 18 procent af disse tyverier omfatter cykler. Dermed er offerrisikoen for cykeltyveri (12*18/100=) 2,2 procent (Balvig, Kyvsgaard & Boesen Pedersen, 2012)

Hvad med producenterne? Kan det være rigtigt, at et produkt som udgør en fare for brugerens netsikkerhed havner på marked? Når der anlægges en nye vej, eller bygges en ny bro, så kræves beregninger vedrørende, hvad det nye indgreb i infrastrukturen betyder for miljøet. Før en ny medicin havner på marked, skal den testes intensivt for at dokumentere dens effekter og eventuelle bivirkninger. Men når Danske Bank introducerer *MobilePay*, kræves der så en redegørelse af sikkerhedseffekter?[21]

Internetsikkerhed opnås uden tvivl bedre gennem sikring og forebyggelse end gennem efterforskning. Dermed ikke sagt, at politiet ingen forpligtelse har til at efterforske internetkriminalitet. Politiet står dog i forbindelse hermed over for flere udfordringer: For det første anmelder mange virksomheder ikke hackerangreb. For det andet er det en forholdsvis beskeden del af politistyrken, der kan anvendes i kampen mod internetkriminalitet – omfanget er beskedent grundet prioritering og kvalifikationer indenfor politiets rækker. For det tredje er der altid efterforskningsspor, men de fører ofte til udlandet. Internationalt politisamarbejde ser derfor ud til at være vejen frem, men denne vej er ikke enkel, og den er ressourcekrævende. For det fjerde må vi konstatere, at politiet har en begrænset værktøjskasse, hvad angår internetkriminalitet. Agentvirksomhed på hackerfora er ikke mulig på grund af IT-kriminalitetens strafferamme.[22] Desuden er det ikke tilladt at 'hacke tilbage'. Alt i alt er det således svært at nå frem til gerningspersonen. I andre vesteuropæiske lande – fx Holland – debatteres det, hvorvidt politiets beføjelser skal opgraderes i denne sammenhæng.

I forbindelse med internettet opstår en ny verden. Hvordan vi færdes sikrest her vil fremtiden vise. Ligesom i den kendte fysiske verden vil der altid være folk, som overskrider vores fælles grænser. Forleden så jeg en dokumentar omkring, hvilke projekter virksomheder arbejder på i *Silicon Valley*. Et af disse var Google Glass, og dette stiller os allerede overfor en række spørgsmål vedrørende regulering af internettet. Fremtiden ser spændende ud.

---

[21] MobilePay er en app, hvorfra brugeren kan overføre penge til andre brugere via modtagerens mobilnummer. Omkring sikkerhed skriver Danske Bank på deres internetside: "MobilePay giver dig samme forbrugerbeskyttelse, som du har ved brug af dine betalingskort. App'en er beskyttet med en firecifret personlig kode. Dine oplysninger opbevares sikkert – på samme måde som i mobilbank. Og når du sender penge, får både du og modtageren straks en kvittering, der bekræfter overførslen." Dette betyder en forringelse af sikkerheden ved pengeoverførsel via MobilePay sammenlignet med mobilbank. Da mobilbank kræver en unik NemID-kode ved hver betaling.

[22] Straffelovens § 754 a. Politiet må ikke som led i efterforskningen af en lovovertrædelse foranledige, at der tilbydes bistand til eller træffes foranstaltninger med henblik på at tilskynde nogen til at udføre eller fortsætte lovovertrædelsen, medmindre:
1) der foreligger en begrundet mistanke om, at lovovertrædelsen er ved at blive begået eller forsøgt,
2) efterforskningsskridtet må antages at være af afgørende betydning for efterforskningen og
3) efterforskningen angår en lovovertrædelse, *som efter loven kan straffes med fængsel i 6 år eller derover*.

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 Kriminal-præventive 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 (2006). *Organised Crime Threat Assessment* (OCTA).

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

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

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.

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

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

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 identiteits-roof. 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.

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 befolknings-undersøgelse*. 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 (2012). *It-anvendelse i befolkningen – 2011*. Danmarks Statistik

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

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

Bilag 1

Spørgeskema offerundersøgelse

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 (konto-nummer, adgangskode mm) 5 Digitale profiler (e-mail, Facebook mm) 6 Andet
Til hvilken formål misbrugte gerningspersonen person-oplysningerne 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 hjemme-side (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