Peter Kruize, Det Juridiske Fakultet, Københavns Universitet

INTERNET-KRIMINALITET 2014

OFFERUNDERSØGELSE OM IDENTITETSTYVERI, BEDRAGERI, AFPRESNING OG CHIKANE I CYBERSPACE

DKR
DET KRIMINAL PRÆVENTIVE RÅD

KØBENHAVNS UNIVERSITET

Det Kriminalpræventive Råd
Polititorvet 14,
1780 København V
45 15 36 50
dkr@dkr.dk
www.dkr.dk

Forfatter: Lektor og Ph.d Peter Kruize,
Københavns Universitet, Det Juridiske Fakultet

Det projekt, der beskrives i denne rapport, er finansieret af 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 Det Kriminalpræventive Råd.

Denne publikation er kun udgivet digitalt som pdf på dkr.dk

Ansvarshavende redaktør: Anna Karina Nickelsen, DKR

April 2015

DKR.nr: 15-230-0222
ISBN 978-87-92966-27-8

Forord

Det er nu tredje gang, at jeg skriver en rapport om internetrelateret kriminalitet i Danmark. Den første rapport udkom i 2009 og handlede om identitetstyveri. Den anden fik titlen "Kriminalitet i en digitaliseret verden" og så dagens lys i 2013. Det betyder, at der så småt er ved at blive opbygget historiske data om internetrelateret kriminalitet og dermed skabt større indsigt i udviklingen af denne.

Timingen af denne rapports publicering er ikke tilfældig. Den Kriminalpræventive Dag (DKD) 2015 afholdes den 23. april 2015 i Aalborg med fokus på cyberkriminalitet. Det Kriminalpræventive Råd og TrygFonden står bag DKD 2015, og resultaterne af min undersøgelse vil blive præsenteret under dette arrangement.

Under udviklingen af spørgeskemaet til offerundersøgelsen samt indhentningen af feedback på rapportens udkast er der blevet inddraget repræsentanter fra Det Kriminalpræventive Råd, Justitsministeriets Forskningskontor og politiet. Følgende personer har bidraget til undersøgelsen med nyttige kommentarer og tilføjelser: Anders Young Rasmussen (DKR), Anne Lerche (DKR), Anna Vibe Onsberg Hansen (DKR), Anne-Julie Boesen Pedersen (JM Forskningskontor) samt Johnny Lundberg og Christina Dela Widenmann (Politiet, NC3). Det endelige ansvar for undersøgelsen er alene forfatterens.

Projektet er finansieret af Det Kriminalpræventive Råd.

Jægerspris, den 20. april 2015
Peter Kruize

Oversigt og resumé

Hovedkonklusionerne i forhold til identitetsmisbrug, betalingskortmisbrug, chikane, handelsbedrageri, forskudsbedrageri og afpresning i cyberspace.

1. Undersøgelsen viser, at ca. 3,6 procent af danskere i alderen 16-74 år har været udsat for disse former for internetkriminalitet inden for de sidste 12 måneder. Det svarer til ca. 150.000 danskere. Ca. halvdelen af disse sager omhandler misbrug af betalingskortoplysninger.
2. Berigelseskriminalitet i den virtuelle verden sker (stadig) betydeligt mindre hyppigt end i den fysiske verden. Til sammenligning: 11 procent af danskere i alderen 16-74 år har været udsat for tyveri i 2013; det svarer til ca. 450.000 danskere (Boesen Pedersen, Kyvsgaard & Balvig, 2014).
3. Målingen i 2014 viser et fald i offerrisikoen for internetkriminalitet i forhold til målingen i 2013 (3,6 procent versus 4,0 procent). Denne forskel er dog ikke statistisk signifikant. Faldet skyldes en markant nedgang i antallet af internethandelsbedragerisager i 2014 i forhold til 2013.
4. Undersøgelsen peger i retning af, at risikoen for tab af identitetsoplysninger (inklusiv betalingskortoplysninger) ofte sker i forbindelse med nethandel (databrud). Det er muligvis en større risikofaktor end phishing og hacking.
5. Det samlede økonomiske tab er beregnet til 271 mio. kr. Til sammenligning: tabet ved tyveri er beregnet til 4.900 mio. kr. (Boesen Pedersen, Kyvsgaard & Balvig, 2014).
6. Forskudsbedrageri er de former for bedrageri, hvor offeret bliver lokket til at betale et forskud for at opnå et eller andet, fx Nigeria-breve eller datingbedrageri. Offerundersøgelsen viser, at forskudsbedrageri ikke er et udbredt fænomen i Danmark.
7. Udsathed for ransomware (malware, der spærrer en computer) er fundet i meget begrænset omfang i modsætning til en anden undersøgelse (Digitaliseringsstyrelsen og DKCERT, 2015). Formentligt har fænomenet ransomware toppet, og der findes ikke ret mange nye ofre anno 2014.
8. Sexafpresning blev slet ikke konstateret i offerundersøgelsen, hvilket er et klart tegn på, at fænomenet ikke er ret udbredt i Danmark.
9. Offerrisikoen er større for dem, der bor i en bykommune, end for dem, der bor uden for en bykommune. Ligeledes har højtuddannede større risiko for at blive udsat for internetkriminalitet end lavtuddannede. Offerrisikoen er to gange større for de respondenter, der opfylder begge risikokriterier, end for de respondenter, der bor uden for en bykommune og er lavtuddannede. Vi må antage, at livsstil og (risiko)adfærd er de bagliggende variabler, der har en indflydelse på risikoen for internetkriminalitet.
10. Lidt under en tredjedel af sagerne vedrørende internetrelateret kriminalitet bliver ifølge offerundersøgelsen politianmeldt.

Denne rapport behandler identitetsmisbrug, betalingskortmisbrug, chikane, handelsbedrageri, forskudsbedrageri og afpresning i cyberspace. Ingen af disse kriminalitetsformer er nye, men med internettets opblomstring er der skabt nye, alternative muligheder for forbrydelser. Det er derfor formålstjenligt at give en beskrivelse af de metoder, internetkriminelle benytter. De nævnte kriminalitetsformer belyses her ud fra følgende perspektiver: omfang, fremgangsmåde, tab, offerprofil og politianmeldelse.

Datagrundlag

For at få indblik i omfanget, tabet, offerprofilerne og anmeldelsesraten benyttes en offerundersøgelse. De forskellige data er blevet indsamlet som led i Danmarks Statistiks omnibus-undersøgelse i perioden august 2014 til og med januar 2015. Godt 1.000 personer blev udspurgt hver måned, og man har dermed i alt haft kontakt med 6.130 respondenter, enten telefonisk eller via et internetspørgeskema. Respondenterne er blevet spurgt om, hvorvidt de inden for de seneste 12 måneder som privatpersoner har været udsat for identitetstyveri eller en anden form for internetkriminalitet. I spørgeskemaet forklaredes disse begreber således:

> Ved identitetstyveri forstås, at en anden person har anvendt dine personoplysninger (fx navn, CPR-nr., mailkonto) eller identitetsbeviser (fx kørekort, sygesikringsbevis) uden din tilladelse for at opnå en økonomisk gevinst. Identitetstyveri kan både ske på internettet og i den 'reelle' verden.
>
> Ved internetkriminalitet forstås, at dine betalingskortoplysninger er blevet misbrugt til at købe varer/ydelser på nettet, at du er blevet udsat for chikane på internettet (fx at nogen har misbrugt din mailadresse eller din profil på Facebook), at du har været udsat for bedrageri ved køb eller salg af varer/ydelser på internettet, at du over internettet er blevet lokket til at sende penge til en person, som viste sig at være en bedrager (fx via et datingsite eller Facebook), eller at du er blevet afpresset over internettet (fx med trusler om, at dine computerdata vil blive slettet, eller at personfølsomme oplysninger vil blive offentliggjort).

Respondenter, der har været udsat herfor, har fået yderligere spørgsmål, bl.a. om typen af oplysninger, tilegnelse, misbrug, opdagelse, beløb, hæftelse for tab og politianmeldelse af sagen.

Hermed er den måde, hvorpå respondenterne er blevet udspurgt, noget anderledes end i undersøgelsen fra 2013, men resultaterne kan anses for at være sammenlignelige (se også bilag 1 for en metodisk redegørelse).

Som supplement til offerundersøgelsen er oplysninger fra eksisterende kilder blevet inddraget i analysen. Det drejer sig om tal om netbankindbrud (Finansrådet), misbrug af Dankort (Nets), misbrug af andre betalingskort (Konkurrence- og Forbrugerstyrelsen) og falske internetbutikker (e-mærket).

Danmarks Statistik gennemfører årligt en spørgeskemaundersøgelse om danskernes it-vaner og internetadfærd. Siden 2010 er desuden medtaget spørgsmål om sikkerhed og sikkerheds-problemer. Disse spørgsmål drejer sig om beskyttelse (sikkerhedssoftware), udsathed for kriminalitet og tryghed ved internetbrug. Også disse statistikker er blevet inddraget i rapporten. Den sidste vigtige kilde i forbindelse med internetkriminalitet er trendrapporterne fra DKCERT. I disse trendrapporter beskrives internetrelaterede sikkerhedsproblemer i det forgangne år. Trendrapporten 2014 indeholder også et afsnit om borgernes it-sikkerhed.

Identitetstyveri

Identitetstyveri er et ofte anvendt begreb, der i Danmark ikke har en juridisk definition, men som kan afgrænses til tilegnelse og misbrug af identitetsoplysninger. Ifølge Digitaliseringsstyrelsen kan identitetstyveri både omfatte, at nogle ulovligt tilegner sig andres oplysninger, og at nogle misbruger sådanne oplysninger til fx at optage lån, købe ting eller udføre chikane. De personlige oplysninger kan fx være cpr-nummer, adgangskoder, sundhedsoplysninger eller andre følsomme persondata. At opsnappe andres kreditkortoplysninger og misbruge dem betegnes derimod ikke som identitetstyveri.

I denne rapport fastslås det, at vi ikke kender – og ikke kommer til at kende – omfanget af ulovlig tilegnelse af identitetsoplysninger. Først når identitetsoplysninger bliver misbrugt, er der et offer, som kan rapportere det. Ergo er det mere korrekt at tale om omfanget af identitets*misbrug*. I rapporten skelnes mellem tre former for identitetsmisbrug: 1) misbrug af identitetsoplysninger med henblik på økonomisk gevinst, 2) misbrug af betalingskortoplysninger og 3) misbrug af person-oplysninger med henblik på chikane af offeret.

En gerningsperson kan overordnet tilegne sig en andens identitetsoplysninger på tre forskellige måder: Oplysningerne kan enten blive fremlagt af offeret selv, de kan blive franarret, eller de kan blive stjålet. Tilegnelse kan ske online, men også offline. I denne rapport beskrives internet-kriminalitet, men der kan også være tale om, at kriminelle tilegner sig identitets- eller betalingsoplysninger offline, fx ved tyveri af pung eller tegnebog indeholdende kørekort og Dankort, men at misbruget finder sted online, fx ved bestilling af en vare eller ydelse. Derfor er offline-tilegnelse inkluderet i undersøgelsen.

Datasikkerhed er et vigtigt emne for danske internetbrugere. Disse brugere udlægger ikke kun tekniske hindringer for at holde hackere og malware væk, men deres internetadfærd påvirkes også 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.

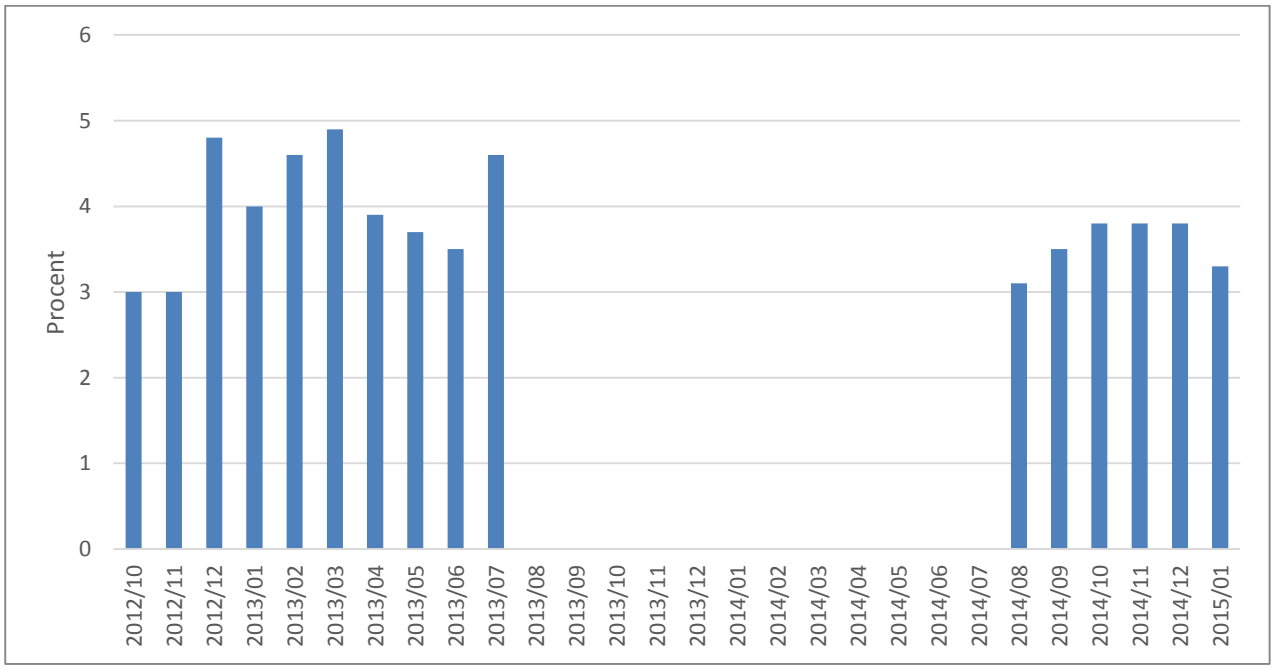
En stor del af de respondenter, der har fået misbrugt deres person- eller betalingsoplysninger, har svært ved at pege på, hvordan de har mistet deres oplysninger. Af det mindretal, der har en

fornemmelse af, hvordan gerningspersonen har fået fat i oplysningerne, peger en betydelig del på handel på internettet. Det ser ud til, at dette er en større risikofaktor end phishing og hacking. Hvis det holder stik, er det et interessant resultat i forhold til de forebyggende indsatser.

Omgang med og udvikling af misbrug og bedrageri på internettet

I undersøgelsen fra 2013 er der indsamlet data over en periode på 10 måneder, fra oktober 2012 til og med juli 2013. Undersøgelsen fra 2014 omfattede de seks måneder fra august 2014 til og med januar 2015. Den samlede offerrisiko lå i 2013 på 4,0 procent, hvilket svarer til, at 166.500 danskere havde været udsat for disse former for internetkriminalitet inden for de sidste 12 måneder. Den risiko var i 2014 faldet til 3,6 procent, hvilket svarer til 150.220 danskere. Dette fald er imidlertid ikke statistisk signifikant. Figur O.1 viser, at offerrisikoen i perioden oktober 2012-juli 2013 lå mellem 3 og 5 procent, mens den svingede mellem 3 og 4 procent i perioden august 2014-januar 2015. Den gennemsnitlige offerprocent og de månedlige udsving indikerer, at den samlede offerrisiko var lidt lavere i 2014-undersøgelsen end i 2013-undersøgelsen.

Figur O.1: Offerrisiko for internetkriminalitet i perioden oktober 2012 – januar 2015



Spørgsmålet er, hvordan udviklingen har været inden for de mange forskellige former for misbrug og bedrageri. Misbrug af identitetsoplysninger, kortoplysninger og digitale profiler (chikane) var genstand for offerundersøgelserne i 2009, 2013 og 2014. Derimod var handelsbedrageri kun medtaget i 2013 og 2014. Tabel O.1 viser, at misbrug af ID-oplysninger steg fra 2009 til 2013 (men stigningen er ikke statistisk signifikant), og at 2014 viste det samme niveau som 2013. Det samme gjaldt misbrug af digitale profiler (chikane). Misbrug af betalingskortoplysninger blev derimod mere end fordoblet i 2014 i forhold til 2013, mens handelsbedrageri udviste et markant fald i offerrisikoen.

Både stigningen ved misbrug af betalingskortoplysninger, og faldet ved handelsbedrageri er statistisk signifikant.

Tabel O.1 Offerrisiko for forskellige former af internetkriminalitet

	2009 (n=1.853)	2013 (n=9.582)	2014 (n=6.130)
Misbrug af ID-oplysninger	0,46 %	0,75 %	0,82 %
Antal ofre i Danmark (estimat)	18.653	31.249	34.471
95 %-sikkerhedsinterval (estimat)	12.165 – 36.495	24.924 – 37.386	25.181 – 46.166
Misbrug af betalingskortoplysninger	0,80 %	0,74 %	1,78 %
Antal ofre i Danmark (estimat)	32.796	29.408	74.463
95 %-sikkerhedsinterval (estimat)	16.398 – 49.194	23.526 – 35.290	62.052 – 86.873
Misbrug af digitale profiler (chikane)	0,05 %	0,29 %	0,38 %
Antal ofre i Danmark (estimat)	2.802	14.027	15.955
95 %-sikkerhedsinterval (estimat)	0 – 16.812	9.351 – 18.703	9.117 – 22.793
Handelsbedrageri		2,40 %	0,54 %
Antal ofre i Danmark (estimat)		109.940	22.783
95 %-sikkerhedsinterval (estimat)		96.197 – 123.682	16.876 – 28.690

Kan det nu være rigtigt, at der sker sådanne markante ændringer i kriminalitetsbilledet inden for blot halvandet år? Den mest oplagte forklaring er, at der må være tale om registreringseffekter, eftersom formuleringen af spørgsmålene ikke er helt identisk i henholdsvis 2013- og 2014-undersøgelserne. Men et nærmere blik på data giver ikke belæg for idéen om, at respondenter er blevet byttet rundt fra handelsbedrageri til betalingskortbedrageri, selvom betalingskort ofte anvendes ved internethandel (se også bilag 1 for en metodisk redegørelse).

Et nøjere kig på de eksisterende kilder giver indtryk af, at stigningen i omfanget af betalingskort-misbrug i 2014 er reel. En opgørelse fra Konkurrence- og Forbrugerstyrelsen viser, at tabet ved kortmisbrug ved fjernsalg (som altovervejende finder sted ved internethandel) steg fra ca. 120 mio. kr. i 2012 til 190 mio. kr. i 2013. Når respondenterne i offerundersøgelsen er blevet spurgt om, hvorvidt de har været udsat for betalingskortmisbrug, drejer spørgsmålet sig kun om de seneste 12 måneder. Det vil sige, at 2014-målingen tilnærmelsesvist omfatter udsathed i 2013, mens 2013-målingen refererede til udsathed i 2012.

Den stigning, som Konkurrence- og Forbrugerstyrelsens beregninger viser, er på ca. 60 procent, mens offerundersøgelsen peger på en stigning på hele 140 procent i udsatheden for betalingskortmisbrug. Konkurrence- og Forbrugerstyrelsens opgørelse er imidlertid i tabte kroner, mens offerundersøgel-

sen taler om udsatte respondenter. Offerundersøgelsen viser samtidig, at det gennemsnitlige tab i 2014 var mindre end i 2013. Ergo er gabet fra 2013 til 2014 i offerundersøgelserne mindre i kroner og øre end i antallet af udsatte personer. Af tabets omfang fremgår, at opgørelsen fra Konkurrence- og Forbrugerstyrelsen og offerundersøgelsen nærmer sig hinanden meget godt.

Der findes ingen eksisterende kilder, der kan verificere det meget markante fald i handelsbedrageri på nettet. Navnlig set i lyset af, at handelen på nettet vokser år for år, skulle man forvente en stigning i stedet for et fald. Den oplagte forklaring er, at danskerne er blevet klogere. Jo mere man handler på nettet, jo skarpere bliver man til at gennemskue snyd. Undersøgelser fra Danmarks Statistik og Foreningen for Dansk Internet Handel (FDIH) viser også, at danskerne foretrækker at handle i danske netbutikker. Måske er en del af forklaringen også, at udvalget af danske netbutikker vokser, og at folk dermed får nemmere ved at finde, hvad de søger i danske butikker. Under alle omstændigheder er det en glædelig nyhed, at markant færre danskere blev udsat for handelsbedrageri på nettet ifølge den sidste måling.

I 2014-undersøgelsen blev der tilføjet to nye emner i forhold til 2013-undersøgelsen: forskudsbedrageri og afpresning. Forskudsbedrageri er de former for bedrageri, hvor offeret bliver lokket til at betale et forskud for at opnå et eller andet. Indtil videre findes der to kendte varianter af forskudsbedrageri på nettet, nemlig Nigeria-breve og datingbedrageri. Offerundersøgelsen viser dog, at forskudsbedrageri ikke er et udbredt fænomen i Danmark. Åbenbart kan langt de fleste potentielle ofre på forhånd gennemskue fidusen.

Afpresning på internettet kan rette sig mod virksomheder såvel som privatpersoner. Denne rapport vedrører dog alene afpresning af privatpersoner med fokus på to former for internetafpresning: ransomware og sexafpresning. Ransomware er en type malware, der er i stand til at spærre en computer. Computerbrugeren får besked om at indbetale en løsesum for atter at få adgang til programmer og/eller data. Ved sexafpresning anvendes erotiske eller intime billeder og videoer af ofrene til at afpresse disse for fx flere billeder eller penge.

En undersøgelse foretaget af Digitaliseringsstyrelsen og DKCERT rapporterer om en offerrisiko for ransomware på hele 8 procent, mens denne offerundersøgelse peger på 0,1 procent inden for de sidste 12 måneder. De 8 procent er (formentlig) en livstids prævalens, men der er stadig langt ned til de 0,1 procent i offerundersøgelsen. Igen kan det skyldes selve registreringen; spørgsmålene er simpelthen formuleret forskelligt. Det er imidlertid svært at tro, at dette skulle udmønte sig i en så stor forskel. En anden forklaring kan være, at fænomenet ransomware har toppet, og at der i 2014 ikke fandtes ret mange nye ofre. Sexafpresning blev slet ikke konstateret i offerundersøgelsen, hvilket er et klart tegn på, at fænomenet ikke er ret udbredt i Danmark.

Økonomisk tab

De fleste af de undersøgte former for internetkriminalitet kan føre til økonomiske tab, dog med chikane som en undtagelse. Forskudsbedrageri og afpresning forekommer i meget beskedent omfang, og det giver ikke mening at regne sig frem til et tabstal. Det betyder, at vi her udelukkende ser nærmere på økonomiske tab grundet identitetsmisbrug, betalingskortmisbrug og handelsbedrageri.

Langt de fleste, der udsættes for bedrageri i forbindelse med internethandel, lider et økonomisk tab. Det samme gælder for lidt færre af dem, der udsættes for misbrug af betalingskort online og for endnu færre af dem, der rammes af identitetstyveri online (se tabel O.2).

Tabel O.2 Procentdel af ofre, der melder om tab (uanset om de selv hæfter for det)

	2013	2014
Identitetstyveri	56 %	54 %
Misbrug af betalingskortoplysninger	71 %	86 %
Bedrageri ved internethandel	100 %	87 %

Tabel O.3 viser de samlede tab for respondenterne i offerundersøgelsen. På baggrund af det mediane tab er der udregnet et estimat for, hvad disse kriminalitetsformer koster på landsplan. Fra Nets og andre kortselskaber kender vi dog det officielle økonomiske tab for dem, der udsættes for betalingskortmisbrug. I 2013 var det samlede tab ifølge den officielle opgørelse 190 mio. kroner, hvilket er meget tæt på det estimat, der foretages på baggrund af offerundersøgelsen, og som lyder på 200 mio. kroner.[1]

Tabel O.3 Samlede økonomiske tab (x mio. kr.)

	2013	2014
Identitetstyveri	59	60
Misbrug af betalingskortoplysninger	91	200
Bedrageri ved internethandel	81	11
I alt	**231**	**271**

Offerprofil

I offerundersøgelsen er der oplysninger om respondenternes køn, alder, herkomst, kommunetype, husholdning, uddannelse og erhverv. Disse baggrundsvariabler er blevet anvendt til at tegne en offerprofil i forbindelse med internetkriminalitet. Det er gjort ved hjælp af en logistisk regressionsanalyse. Derved er der blevet taget højde for, at baggrundsvariablerne påvirker hinanden indbyrdes.

[1] De officielle tal for året 2013 svarer til offerundersøgelsens data fra 2014. Respondenterne blev spurgt om, hvorvidt de havde været udsat for denne type kriminalitet i løbet af de seneste 12 måneder.

Analysen viser, at to variabler har en signifikant indflydelse på offerrisikoen: kommunetype og uddannelse. Disse to variabler giver i alt fire profiler, nemlig respondenter der enten bor i en bykommune eller i en ikke-bykommune, og som er enten højt- eller lavtuddannede.

Tabel O.4 Offerrisiko pr. profil

	ID-misbrug	Betalings-kortmisbrug	Handels-bedrageri	I alt
Højtuddannet, i bykommune (n=1.221)	1,1 %	2,6 %	0,5 %	4,9 %
Højtuddannet, *ikke* i bykommune (n=742)	0,8 %	1,6 %	1,1 %	3,8 %
Lavtuddannet, i bykommune (n=1.803)	1,1 %	2,1 %	0,7 %	3,8 %
Lavtuddannet, *ikke* i bykommune (n=2.364)	0,5 %	1,2 %	0,3 %	2,5 %

Det samlede resultat viser, at offerrisikoen er større for dem, der bor i en bykommune, end for dem, der bor uden for en bykommune. Ligeledes har højtuddannede større risiko for at blive udsat for internetkriminalitet end lavtuddannede. Offerrisikoen er to gange større for de respondenter, der opfylder begge risikokriterier, end for de respondenter, der bor uden for en bykommune og er lavtuddannede. Vi må antage, at livsstil og (risiko)adfærd har en indflydelse på risikoen for internetkriminalitet. Hvordan en persons bopælsadresse og uddannelsesniveau hænger sammen med livsstil og adfærd, kan ikke fastslås med denne undersøgelse.

Politianmeldelse

Lidt under en tredjedel af sagerne vedrørende internetrelateret kriminalitet bliver ifølge offerundersøgelsen politianmeldt. Det er ikke nødvendigvis respondenten, der anmelder sagen, men ved misbrug af betalingskort ofte banken eller kortselskabet.

Tabel O.5 Politianmeldelse

	Antal udsatte	Politianmeldt (procentdel)
Identitetstyveri	51	25 %
Misbrug af betalingskortoplysninger	109	39 %
Chikane	22	10 %
Bedrageri ved internethandel	34	22 %
Forskudsbedrageri	3	-
Afpresning	7	14 %
I alt	**226**	**29 %**

I otte af de 65 politianmeldte sager[2] (12 procent) har politiet ifølge respondenten afvist anmeldelsen. I undersøgelsen er der ikke blevet spurgt om begrundelsen, men vi må antage, at politiet har

[2] 29 procent af 226 udsatte (tabel O.5) svarer til 65 sager, der er meldt til politiet.

vurderet, at den konkrete sag ikke indebar en strafbar handling, eller at det ikke var respondenten – men fx banken – der burde anmelde sagen.

Indholdsfortegnelse

1 Indledning

1.1 Opdeling og afgrænsning af internetkriminalitet

Internettet indtager en vigtig plads i vores dagligdag, og dermed er det ikke overraskende, at en stadig større del af kriminaliteten foregår på nettet. 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 (malware) bruges til at skaffe adgang til en computer. Dette er en metode til fx at stjæle for-urettedes personoplysninger. Det er dog langtfra altid nødvendigt at hacke en computer i forbindelse med internetkriminalitet: at uploade eller downloade børnepornografi eller ophavsretligt beskyttet musik kræver ikke adgang til en anden persons computer. Desuden kan køb af varer med aflurede kortoplysninger klares med 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 fremkomst, eller om vi kan beskrive og forklare internetkriminalitet med eksisterende begreber og teorier. Wall (2007) skelner mellem tre former for internetkriminalitet:

1. *Computerintegritetsforbrydelser* (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 ved hjælp af internetteknologi. I forbindelse hermed er det især penge, varer og information, som er i fokus. Der er således en mindre grad af nyskabelse ved disse forbrydelser end ved forbrydelser, som retter sig mod computerens integritet. Men set med kriminologiske øjne er der også nye

aspekter ved computerassisterede forbrydelser, fx spiller afstand og geografiske grænser ingen rolle i cyberspace.

3. *Computerindholdsforbrydelser* (computer content crimes): Disse forbrydelser knytter sig til ulovligheder i forbindelse med indholdet af filer, beskeder eller andre informationer, der sendes ud på internettet. Ulovligt indhold kan fx være børnepornografisk, racistisk eller voldeligt (fx terrorisme). I forbindelse hermed handler det igen om forbrydelser, som vi kender til i forvejen, men som internettet tilfører en ny dimension.

1.2 Undersøgelsens fokus og formål

I denne rapport ses nærmere på de enkelte former for internetkriminalitet, der kan betragtes som computerassisterede forbrydelser: misbrug af ID-oplysninger, misbrug af betalingskortoplysninger, chikane, handelsbedrageri, Nigeria-breve og afpresning. I dette forskningsprojekt er formålet at få et bedre indblik i disse former for internetkriminalitet. I afdækningen heraf er det basale spørgsmål som omfang, udvikling, fremgangsmåde, tab og offerprofil, der søges svar på.

1.3 Eksisterende kilder

Kriminalitet kan anmeldes til politiet. Bortset fra, at kun en (mindre) del af kriminaliteten anmeldes til politiet, registreres anmeldelser som regel efter straffelovsparagraffer. Traditionelle former for kriminalitet – fx indbrud i private hjem – kan identificeres i politiets anmeldelsesstatistik, selvom de hører under den brede lovparagraf 276 (tyveri). Det gælder – indtil videre – ikke for mange internetrelaterede forbrydelser.[3] De forskellige former for bedrageri registreres under straffelovens paragraf 279, og dermed er det uklart, hvor stor en del der er internetbaserede. Politiets statistikker er dermed mindre brugbare til at skaffe indblik i disse former for internetkriminalitet.

Det er ikke altid i en virksomheds interesse at informere politiet eller andre myndigheder, hvis den har været udsat for internetkriminalitet. Informationer herom kan nemlig tænkes at være skadelige for virksomhedens troværdighed. Eksempelvis kan det være fordelagtigt at holde et indbrud i computersystemets kundeoplysninger skjult for offentligheden. Samtidig har politiet ikke nok ressourcer til at efterforske hver enkelt forbrydelse. Det er (formentlig) almen praksis, at virksom-

[3] Fra 1. april 2015 er der lagt en søgenøgle vedrørende internetkriminalitet i politiets registreringssystem POLSAS, som gør det muligt at identificere internetrelateret kriminalitet. Det forudsætter imidlertid, at denne søgenøgle også anvendes ved registrering af sagen, eller – sagt med andre ord – at politiets medarbejdere har gjort brugen af denne nøgle til rutine. Erfaringen viser, at det kan tage sin tid.

heden 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 branche-organisationer antageligt har bedre indblik i internetkriminalitetens omfang end politiet. Finansrådet oplyser således tal for netbankindbrud, Nets tal for misbrug af Visa/Dankort, og e-mærket registrerer antallet af identificerede falske internetbutikker på det danske marked. Disse statistikker inddrages i rapporten.

Danmarks Statistik gennemfører årligt en spørgeskemaundersøgelse om danskernes it-vaner og internetadfærd. Siden 2010 er desuden medtaget spørgsmål om sikkerhed og sikkerheds-problemer. Disse spørgsmål drejer sig om beskyttelse (sikkerhedssoftware), udsathed for kriminalitet og tryghed ved internetbrug. Også disse statistikker inddrages i rapporten.

Den sidste vigtige kilde i forbindelse med internetkriminalitet er trendrapporterne fra DKCERT.[4] I disse trendrapporter beskrives internetrelaterede sikkerhedsproblemer i det forgangne år. Trend-rapporten fra 2014 indeholder et afsnit om borgernes it-sikkerhed. Den er baseret på en stikprøveundersøgelse blandt 981 danskere og belyser, om "borgerne har oplevet sikkerheds-hændelser, hvilke konsekvenser det fik for borgernes videre kontakt med det offentlige (…) hvad borgerne generelt ved om informationssikkerhed." (DKCERT Trendrapport 2014, s. 33).

1.4 Offerundersøgelse

Mørketalsproblemet og manglen på officielle statistikker kan til dels afhjælpes af en offerunder-søgelse. Siden 2005 er der løbende gennemført landsdækkende, repræsentative offerundersøgelser. Disse undersøgelser finansieres af Det Kriminalpræventive Råd, Justitsministeriet og Rigspolitiet og er gennemført i et samarbejde med Københavns Universitet.

Offerundersøgelserne er endvidere et led i Danmarks Statistiks omnibusundersøgelser – interview-undersøgelser, hvori man samler flere emner i ét interview. De personer, der indgår i omnibus-undersøgelsen, udvælges tilfældigt gennem Danmarks Statistiks cpr-register, således at de udgør et repræsentativt udsnit af den del af befolkningen, der er 16-74 år. De månedlige brutto-stikprøver omfatter omkring 1.700 personer, mens nettostikprøverne omfatter ca. 1.500. Omtrent to tredjedele

[4] DKCERT, det danske Computer Emergency Response Team, hører under DeIC, Danish e-Infrastructure Cooperation. DeIC har til formål at understøtte Danmark som e-science-nation gennem levering af e-infrastruktur (computing, datalagring og netværk) til forskning og forskningsbaseret undervisning. DeIC er etableret under Ministeriet for Forskning, Innovation og Videregående Uddannelser og hører organisatorisk under Styrelsen for Forskning og Innovation.

af de udvalgte personer deltager i undersøgelserne, og dermed udspørges ca. 1.000 respondenter hver måned (Boesen Pedersen, Kyvsgaard & Balvig, 2014).

Forfatterne af den landsdækkende offerundersøgelse peger på en række metodiske ulemper ved denne type undersøgelse. De nævner bl.a., at "disse problemer betyder, at oplysningerne bliver forbundet med en vis usikkerhed og en række begrænsninger, som bør tages i betragtning, når tallene fortolkes og forklares" (Boesen Pedersen, Kyvsgaard & Balvig, 2014, s. 12). I bilag 1 refereres til de vigtigste problemer forbundet med offerundersøgelser.

I marts og juni 2009 blev der i omnibusundersøgelser stillet spørgsmål om identitetstyveri (Kruize, 2009), mens der fra oktober 2012 til og med juli 2013 blev spurgt om både identitetstyveri og handelsbedrageri på nettet (Kruize, 2013). Endelig er der i perioden august 2014 til og med januar 2015 blevet spurgt om misbrug af ID-oplysninger, misbrug af betalingskortoplysninger, chikane, e-handelsbedrageri, privathandelsbedrageri, Nigeria-breve og afpresning. De oprindelige spørgsmål (2009 og 2013) om identitetstyveri omfattede det, der senere er blevet kaldt misbrug af ID-oplysninger, misbrug af betalingskortoplysninger og chikane. Handelsbedrageri (2013) omfatter e-handelsbedrageri og privathandelsbedrageri. Datagrundlaget for offerundersøgelserne ser således ud:

Tabel 1.1 Oversigt over offerundersøgelser i forbindelse med internetkriminalitet

	2009 Marts-juni 2009 N = 1.853	2013 Okt. 2012-juli 2013 N = 9.582	2014 Aug. 2014-jan. 2015 N = 6.130
Misbrug af ID-oplysninger	X	X	X
Misbrug af kortoplysninger	X	X	X
Chikane	X	X	X
E-handelsbedrageri		X	X
Privathandelsbedrageri		X	X
Nigeria-breve			X
Afpresning			X

Offerprofil

Til datasættet er knyttet følgende baggrundsvariabler: køn, alder, herkomst, kommunetype, husholdning, uddannelse og erhverv.

Disse baggrundsvariabler benyttes til at tegne en offerprofil ved de forskellige former for internetkriminalitet. Man kan fx se ofrenes aldersfordeling i forhold til dem, der ikke har været udsat for disse typer af kriminalitet. Det samme kan lade sig gøre med hensyn til køn osv. Det er imidlertid uklart, hvordan baggrundsvariablerne påvirker hinanden indbyrdes. For at klarlægge dette kræves en

logistisk regressionsanalyse, hvori alle variabler indsættes i én model. På baggrund af denne analyse kan man sammensætte profiler og udregne deres offerrisiko.

Antallet af ofre er relativt lille, og det er derfor ikke muligt i større omfang at differentiere ved baggrundsvariablerne. Baggrundsvariablerne er dikotome, dvs. opdelt i to kategorier, der ideelt set skal være af nogenlunde samme størrelse. Tabel 1.2 viser opdelingen af baggrundsvariablerne og procentfordelingen i stikprøverne (n=6.130).

Tabel 1.2 Oversigt over baggrundsvariablernes opdeling for logistisk regressionsanalyse (n=6.130)

Variabler	Opdeling	Fordeling
Køn	Mand	50 %
	Kvinde	50 %
Alder	45 år eller yngre	45 %
	46 år eller ældre	55 %
Herkomst	Dansker	92 %
	Indvandrer/efterkommer	8 %
Kommunetype	Bykommune	49 %
	Andet	51 %
Husholdning	Par med børn	51 %
	Andet	49 %
Uddannelse	Mellem/langvarig	32 %
	Andet	68 %
Erhverv	I arbejde	59 %
	Ikke i arbejde	41 %

Eftersom antallet af respondenter, der er blevet ramt af internetkriminalitet, er meget begrænset i forhold til antallet af respondenter, der ikke er blevet ramt, er det svært at opnå statistisk signifikans. I første omgang er der blevet udført en logistisk regressionsanalyse af alle de førnævnte baggrundsvariabler. Analysen viser, at to variabler er signifikante (se kolonnen "Sig" i tabel 1.3; når tallet er 0,05 eller mindre, har variablen en signifikant indflydelse på offerrisikoen). Den første signifikante variabel er kommunetype: Respondenter, der bor i en bykommune, har en større risiko for at blive udsat for internetkriminalitet end respondenter, der ikke bor i en bykommune. Analysen påviser en statistisk sammenhæng, men siger ikke noget om kausaliteten. Den anden signifikante variabel er uddannelse. Respondenter med en mellemlang eller lang uddannelse – de "veluddannede" – har en større risiko for at blive udsat for internetkriminalitet end respondenter, der er mindre godt uddannede.

Tabel 1.3 Logistisk regressionsanalyse for offerrisikoen ved internetkriminalitet

Variabler	B	S.E.	Wald	Sig	Exp(B)
Køn	-0,059	0,140	0,179	0,672	0,943
Alder	0,033	0,142	0,055	0,814	1,034
Herkomst	-0,070	0,243	0,083	0,774	0,932
Kommunetype	0,379	0,146	6,767	0,009	1,460
Husholdning	0,152	0,144	1,118	0,290	1,164
Uddannelse	0,335	0,148	5,113	0,024	1,398
Erhverv	0,052	0,150	0,119	0,730	1,053

De tre talmæssigt mest omfangsrige former for internetkriminalitet – identitetsmisbrug, betalingskortmisbrug og handelsbedrageri – afviger ikke fra det samlede billede. På baggrund af denne analyse tegnes offerprofilen inden for kommunetype[5] og uddannelsesniveau. Der skelnes mellem fire profiler:

- Højtuddannet; bor i en bykommune (n=1.221; 20 procent)
- Højtuddannet; bor ikke i en bykommune (n=742; 12 procent)
- Lavtuddannet; bor i en bykommune (n=1.803; 29 procent)
- Lavtuddannet; bor ikke i en bykommune (n=2.364; 39 procent)

Vi må antage, at livsstil og (risiko)adfærd har en indflydelse på offerrisikoen. Hvorledes en persons bopælsadresse og uddannelsesniveau hænger sammen med livsstil og adfærd, kan ikke fastslås med denne undersøgelse (men kunne være interessant at få nærmere belyst).

[5] Kommuner inddeles i yder-, land-, mellem- og bykommuner. Kommunetypen fastsættes på baggrund af 14 indikatorer. De belyser graden af urbanisering, landbrugets betydning, demografisk struktur, erhvervs- og befolkningsudvikling, uddannelsesniveau, kommunens økonomiske grundlag og kommunens placering (center/periferi). Se også: http://barbaradiklev.dk/udkant.dk/IndikatorerForLanddistrikt.pdf.

2 Identitetstyveri

2.1 Hvad er identitetstyveri

Begrebet identitetstyveri har efterhånden vundet fodfæste i det danske sprog, og i langt de fleste tilfælde benyttes det i forbindelse med internetbrug og internethandel. Internettet spiller således i dag en central rolle for misbrug af identitetsoplysninger. Men at sløre sin egen identitet har altid været en del af den kriminelle verden. Rådet for it-sikkerhed nedlagdes i 2006, men arbejdede inden da ud fra følgende definition af identitetstyveri:

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

It-sikkerhed og identitetstyveri hører nu under Digitaliseringsstyrelsen. I 2013 åbnede styrelsen en informationsportal om identitetstyveri. Portalen er tilgængelig på borger.dk, og her defineres identitetstyveri på følgende vis:

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

Forskellen mellem disse to definitioner er, at Digitaliseringsstyrelsen udelukker misbrug af betalingskortoplysninger fra begrebet identitetstyveri. Dette er nyt, og Danmark adskiller sig således fra de fleste europæiske lande. Jeg har i hvert fald ikke kendskab til andre, som udelukker misbrug af betalingskortoplysninger. Det diskuteres imidlertid internationalt, hvorvidt kortsvindel hører under begrebet identitetstyveri. Særligt repræsentanter fra finansverdenen mener, at dette ikke burde være

tilfældet (se fx Cheney, 2005, p. 2). Denne diskussion er specielt aktuel i USA, men The Federal Identity Theft and Assumption Deterrence Act fra 1998 inkluderer kortsvindel i begrebet identitetstyveri.[6] Også Europol (2012) regner misbrug af financielle data, som betalingskortdata, for identitetstyveri (Identity Theft).

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

> ID theft occurs when a party acquires, transfers, possesses, or uses personal information of a natural or legal person in an unauthorized manner, with the intent to commit, or in connection with, fraud or other crimes (OECD, 2009, s. 16).

Ifølge McNally & Newman bruges begreberne identitetstyveri (identity theft) og identitetssvig (identity fraud) ofte som synonymer. Binder & Gill (2005) definerer identitetstyveri (identity theft) som det at overtage og misbruge en anden persons identitet, mens de definerer identitetssvig (identity fraud) som det at antage en fiktiv identitet. Binder & Gill påpeger, at "unfortunately, when you review the legislation, many times the term identity theft appears to be used interchangeably with the term identify fraud" (Binder & Gill, 2005, p. 8). I Europols Organised Crime Threat Assessment (OCTA) betragtes identitetssvig både som misbrug af rigtige personoplysninger og misbrug ved hjælp af fiktive oplysninger, mens identitetstyveri kun knytter sig til misbrug af rigtige oplysninger.[7]

De forskellige varianter af identitetstyveri har det tilfælles, at specifikke identitetsoplysninger fremskaffes af gerningspersonen, og at disse oplysninger på et senere tidspunkt misbruges. Det betyder, at der er en tidsforskel mellem tilegnelse og misbrug. Desuden kan det også tage tid, førend

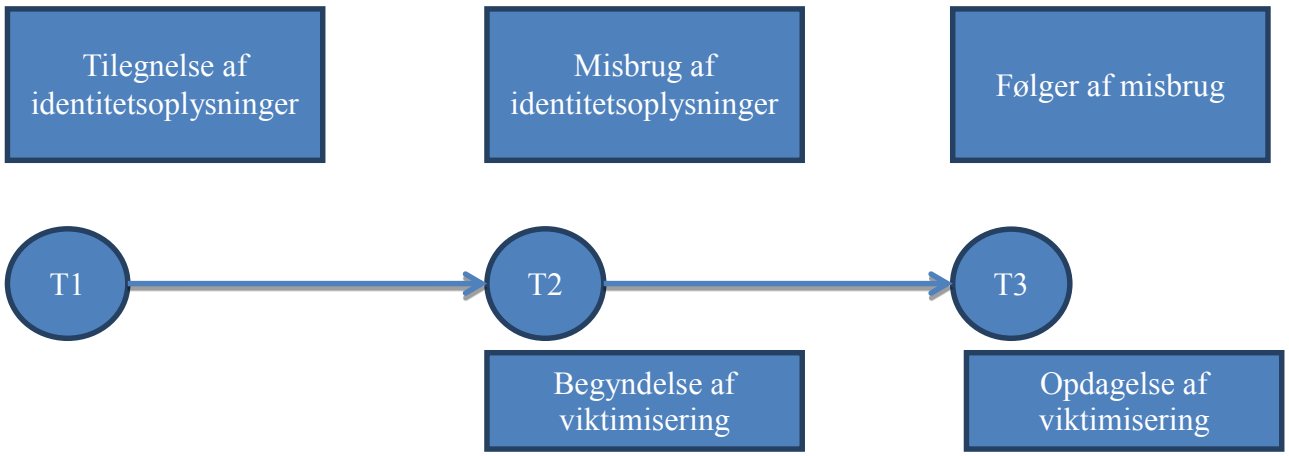
---

[6] 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."

[7] "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).

forurettede opdager, at vedkommendes identitetsoplysninger er blevet misbrugt. Nedenstående skema viser processen.

Skema 2.1 Tre faser af identitetstyveri i tidsperspektiv



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

2.2 Identitetstyveri og straffeloven

Identitetstyveri er et ofte anvendt begreb, som dog i Danmark ikke har en juridisk definition. 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). Adspurgt har rigsadvokaten svaret retsudvalget, at en falsk profil på internettet, hvor nogle udgiver sig for at være en anden eksisterende person, som udgangspunkt ikke i sig selv kan betragtes som strafbar. Rigsadvokaten tilføjer, at der imidlertid kan være tale om strafbare forhold i forbindelse med en sådan 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 strafbar-heden, 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 kun få lande specifik lovgivning vedrørende identitetstyveri. USA må betragtes som foregangsland på dette område, idet identitetstyveri her er en selvstændig forbrydelse. I USA defineres identitetstyveri (ID Theft) på følgende vis:

> Knowingly transfers, possesses, uses, without lawful authority, a means of identification of another person with the intent to commit, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law (OECD, 2009, p. 47).

I Frankrig blev et lovforslag vedrørende identitetstyveri i 2005 ikke til noget, eftersom den franske justitsminister i 2006 trak forslaget tilbage med den begrundelse, at identitetstyveri på tilstrækkelig vis kan straffes efter den eksisterende lovgivning (OECD, 2009, p. 50). Ifølge OECD har der i EU-medlemsstaterne ikke været andre initiativer 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 Politi-departementet, 2009). I den norske pressemeddelelse påpeges det, at mange handlinger, der omfattes af den nye bestemmelse, allerede er strafbare under den gamle straffelov. Det gælder bl.a. bedrageribestemmelser. Hvis der skal kunne være tale om en straffesag, er det dog her en forudsætning, at en stjålen identitet bruges til at udføre en strafbar handling. Den nye straffebestemmelse gør det enklere at strafforfølge identitetstyveri, idet det nu er lettere at bevise identitetskrænkelse end et forsøg på fuldbyrdet bedrageri.[8]

[8] De sidste meldinger fra Norge er, at der er tale om et signifikant fald i antallet af ID-tyverier siden 2013. I offerundersøgelser i Norge er der spurgt om respondenterne har været udsat for identitetsmisbrug (inklusiv kortoplysninger) inden for de sidste to år. Målingen fra 2013 gav en offerprocent på 5,9 procent, mens 2014-måling viste en offerprocent på 3,2 procent (Meyer, 2015). Hvorvidt denne udvikling har en sammenhæng med det norske lovinitiativ kan ikke siges.

I Danmark har der været debat om, hvorvidt identitetstyveri skal være et selvstændigt begreb i straffeloven. Dansk Folkeparti fremsatte den 26. oktober 2011 et forslag til folketingsbeslutning om en særskilt straf for identitetstyveri og identitetssvindel (2011/1 BF 3). Forslaget førstebehandledes i Folketinget den 17. januar 2012 og blev henvist til behandling i retsudvalget, som afholdt en høring den 8. maj 2012. Det viste sig, at der ikke var politisk flertal for en særskilt straffebestemmelse for identitetstyveri. Et mindretal i retsudvalget opfordrede efterfølgende regeringen til at iværksætte initiativer, der sikrer, at myndigheder, virksomheder og privatpersoner står bedst muligt rustet over for identitetstyveri og de kriminelle følger heraf. Desuden opfordrede 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 det løbende overvejes, om en indførelse af en sådan særskilt straffelovsparagraf vil tjene et formål i dansk sammenhæng.

2.3 Tilegnelse af identitetsoplysninger

Der er flere måder, hvorpå en gerningsperson kan tilegne sig andres (identitets)oplysninger. Offentligt tilgængelige registre, fx telefon- og navneregistre, indeholder oplysninger som navn, adresse og telefonnummer. Internetsiden krak.dk er et eksempel herpå. Desuden lægger privatpersoner ofte frivilligt personoplysninger ud på egne internetsider eller på sociale netværkssider som Facebook og LinkedIn. Oplysninger kan også blive franarret, fx ved phishing, eller stjålet. En persons (identitets)oplysninger kan dermed falde i forkerte hænder på tre måder:

- Ved frivillig upload på internettet
- Ved bondefangeri
- Ved tyveri.

Der kan skelnes mellem online og offline tilegnelse af (identitets)oplysninger (fx OECD, 2009). Online tilegnelse knytter sig til internettet og det faktum, at når en enhed (computer, smartphone, tablet) tilsluttes nettet, er det muligt at trænge ind i den og/eller kommunikere med brugeren. Offline tilegnelse betyder, at der er tale om en handling i den fysiske verden. Det kan dreje sig om lomme- eller tasketyveri, men kan dog også være af teknisk art, fx skimming.

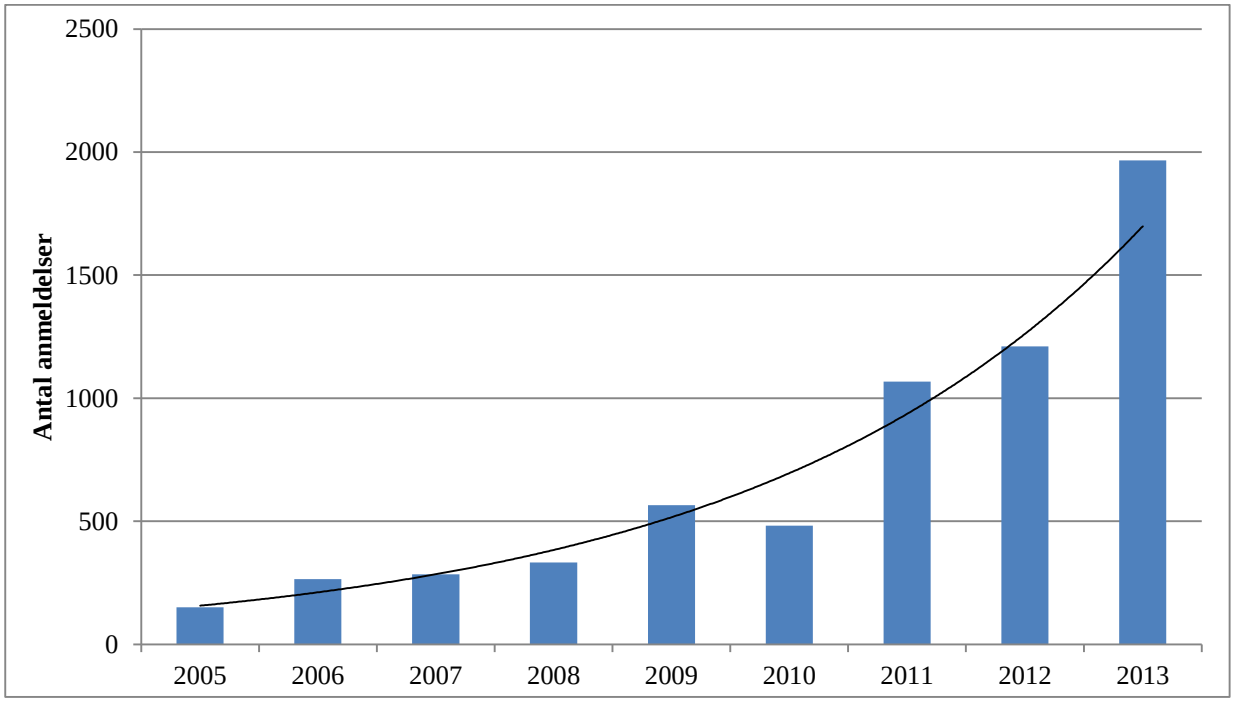
I denne rapport beskrives internetkriminalitet, altså kriminalitet, der finder sted på internettet eller ved brug af dette. Der kan imidlertid også være tale om, at selve den kriminelle tilegnelse af identitets- eller betalingsoplysninger finder sted offline, fx ved tyveri af en tegnebog eller pung, som indeholder et kørekort og et Dankort, men at misbruget sker online, fx ved bestilling af en vare eller ydelse. Disse tilfælde af offline tilegnelse er derfor inkluderet i dette kapitel. Først ses imidlertid nærmere på metoder til at franarre (phishing/pharming) og stjæle oplysninger online.

2.3.1 Phishing/pharming

Formålet med phishing er at franarre offeret fortrolige oplysninger, typisk identitetsinformation og finansielle oplysninger. Phishing sker hyppigst ved, at en e-mail sendes til et stort antal adresser. For et par tusinde kroner kan en e-mail således afsendes til en million adresser. Modtagerne opfordres enten til at indtaste de ønskede oplysninger og sende e-mailen retur eller til at klikke videre til en phishing-side (pharming; det betyder, at brugeren videresendes til hjemmesider, som ser ægte ud, men i virkeligheden er falske).

DKCERT modtager anmeldelser angående danske internetsider med phishing. I 2013 indløb således 1.966 anmeldelser om inficerede danske sider. Figur 2.1 viser, at antallet af disse er steget eksponentielt i perioden fra 2005 til 2013. Samtidig er hostingselskaberne og internetudbyderne dog blevet hurtigere til at lukke phishingsider. I DKCERT Trendrapport 2008 oplystes det, at danske hostingudbydere var langsomme til at reagere og lukke phishingsider på deres servere. Den mediane levetid for en phishingside var således i 2008 hele 16 dage. Af trendrapporten for 2011 fremgik det, at levetiden for phishingsider nu var 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 DKCERT (DKCERT Trendrapport 2011, s. 12).

Figur 2.1 Danske internetsider med phishing-sider (pharming)



Kilde: DKCERT Trendrapport, adskillige årgange.

2.3.2 Malware

Når en enhed (computer, smartphone, tablet) tilsluttes internettet, kan den kommunikere med omverdenen. Bagsiden er, at enheden kan angribes af andre brugere. Den mest kendte form for angreb er computervira. En computervirus er et lille program, der forsøger at inficere andre programmer. Oftest synes 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 hjemme under betegnelsen *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.

Typer af malware

I DKCERT Trendrapport 2014 oplystes fordelingen af malware, som antivirusproducenten F-Secure havde identificeret på danskernes computere. Trojanske heste[9], der typisk spredes via inficerede websteder og e-mails, var i 2013 stadig klart den største malware-trussel. Trojanske heste stod således for to tredjedele af alle konstaterede trusler; en mindre andel end i 2012, hvor de tegnede sig for tre fjerdedele. Til gengæld er mængden af exploits stigende. Et exploit er et angrebsprogram, der udnytter en bestemt sårbarhed. Exploits stod for 32 procent af truslerne i 2013 mod 19 procent i 2012. Det drejede sig især om exploits, der udnyttede de sårbarheder i Java, som blev spredt i 2013 (DKCERT Trendrapport 2014, s. 7).

I forbindelse med afluring af (identitets)oplysninger er en keylogger bemærkelsesværdig. En keylogger er et program, der registrerer, hvad der skrives på tastaturet. Det bruges til at spionere, 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-mailadresse. En keylogger kan i øvrigt også installeres bevidst af computerens ejer. Visse programmer til forældrekontrol indeholder reelt også en keylogger, hvormed børnenes adfærd, fx på sociale medier, kan overvåges.

[9] En trojansk hest er malware forklædt som noget harmløst. Trojaneren er ofte et serverprogram, der gør det muligt at fjernstyre den smittede enhed. Det kaldes derfor også at installere en bagdør. Adgangen kan fx misbruges til at foretage DDoS-angreb mod andre systemer på internettet. Fjernstyringsprogrammet Back Orifice er et af de mest kendte programmer til trojanske heste, selvom programmet egentlig er udviklet til legale formål.

Risiko for malware

I Danmarks Statistiks årlige undersøgelse af danskernes it-vaner og internetadfærd har man først fra 2010 spurgt om sikkerhed og sikkerhedsproblemer. Der er blevet spurgt til, om respondenten i de seneste 12 måneder har været udsat for computervirus eller andre skadelige programtyper som fx orme, trojanske heste, bagdøre, adware og spyware, der medfører tab af informationer eller (arbejds)tid. Spørgsmålet dækker dermed begrebet *malware*.

Ca. 30 procent af alle danskere med internetadgang i husstanden har i det seneste år været udsat for malware, der har medført tab af informationer eller tid. Dette procenttal er rimeligt konstant med undtagelse af 2012, hvor tallet lå væsentligt lavere. En undersøgelse i regi af DKCERT udført i januar 2014 viser, at 31 procent af alle danskere med internetadgang i husstanden har haft virus eller andre former for skadelige programmer på deres computer. I sidstnævnte undersøgelse har man også spurgt om, hvorvidt dette sikkerhedsproblem har ført til handling. 95 procent af respondenterne svarede ja. De fleste har som konsekvens installeret sikkerhedssoftware (81 procent), men er også blev mere forsigtige med at dele informationer på fx Facebook (60 procent) og har undladt at besøge bestemte websteder (58 procent)[10] (DKCERT Trendrapport 2014, s. 33-34).

2.3.3 Risikoadfærd

Datasikkerhed er et vigtigt emne for danske internetbrugere. De installerer ikke kun tekniske forhindringer for at holde hackere og malware væk, også deres internetadfærd påvirkes af bekymringer i forhold til sikkerhed.

Tabel 2.1 Andelen af internetbrugere, der har afholdt sig fra bestemte aktiviteter på internettet

	2010	2011	2012	2014
Afgivelse af personoplysninger til sociale/professionelle tjenester	33 %	34 %	31 %	38 %
Download af software, musik, videofiler, spil eller andre datafiler	23 %	26 %	20 %	27 %
Bestilling eller køb af produkter eller tjenester til private formål	21 %	26 %	21 %	24 %
Brug af netbank	13 %	14 %	10 %	16 %
Kommunikation med den offentlige sektor	7 %	7 %	6 %	9 %

Kilde: Danmarks Statistik.

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 korrekte personoplysninger i forbindelse med oprettelsen. Desuden er en betydelig del af internetbrugerne påpasselige med at downloade

[10] Derudover har 11 procent undladt at bruge offentlig digital selvbetjening, og 9 procent har anmeldt sagen til politiet.

software, musik, videoer eller spil fra internettet. Dette gælder også indkøb af varer eller ydelser på internettet (hvilket kræver afgivelse af betalingskortoplysninger). Hvad angår brug af netbank-tjenester (med risiko for netbanksindbrud), er internetbrugerne dog ikke blevet væsentligt mere forsigtige. Tabel 2.1 viser oversigten.

2.3.4 Offerundersøgelse

I offerundersøgelsen, der ligger til grund for denne rapport, er de 160 respondenter, som har været udsat for misbrug af identitets- eller betalingskortoplysninger, blevet spurgt om, hvorvidt de ved, hvordan gerningspersonen har fået fat i deres oplysninger. 62 af de 160 respondenter (39 procent) havde en idé om dette. Af disse 62 mente mere end 80 procent, at det var sket online. Tabel 2.2 viser en oversigt over de metoder, der efter respondenternes egen vurdering er blevet anvendt til tilegnelse af deres identitetsoplysninger.

Tabel 2.2 Identitetsoplysninger er stjålet ved:

	Antal	Procentdel
Handel på nettet	24	39 %
Indbrud/tyveri	9	15 %
Hacking af computer	7	11 %
Falsk e-mail (phishing)	6	10 %
Falsk hjemmeside (pharming)	6	10 %
Skimming af kort	5	8 %
Betaling i udlandet	3	5 %
Misbrug begået af bekendte/kolleger	2	3 %
I alt	**62**	**100 %**

Note: 98 respondenter havde ingen anelse om, hvordan deres identitetsoplysninger var blevet stjålet.

Oversigten viser, at der i 39 procent af tilfældene har været tale om internethandel. Det knytter sig til, at betalingskortsoplysninger eller andre informationer er blevet stjålet fra en database eller et register. I disse tilfælde bryder hackere ind i et computersystem, hvor disse data er gemt, fx en internetbutiks kundekartotek. Det skal dog bemærkes, at det er svært at tolke tabel 2.2, når 61 procent af respondenterne ikke er i stand til at besvare dette spørgsmål. Det kan sagtens være, at fx hacking i realiteten spiller en større rolle i forbindelse med tilegnelsen af identitetsoplysninger, men at det forbliver uopdaget af respondenten.

2.4 Omfanget af identitetstyveri i Danmark

Først når selve misbruget af identitetsoplysninger opdages, bliver offeret klar over, at han eller hun har været udsat for en forbrydelse. Det antages fx, at det ikke er alle opsnappede cpr-numre, der benyttes efter et dataindbrud. Omfanget af dette mørketal er – ifølge sagens natur – ukendt.

Dermed kan vi i realiteten ikke måle omfanget af identitetstyveri, bortset fra når der er tale om viktimisering (fase 2 i skema 2.1). Først når identitetsoplysninger misbruges, er der et offer, som kan rapportere om det. Det er derfor mere korrekt at tale om omfanget af identitets*misbrug*.

I denne rapport skelnes mellem tre former for identitetsmisbrug:

- Misbrug af identitetsoplysninger med henblik på økonomisk gevinst
- Misbrug af betalingskortoplysninger
- Misbrug af personoplysninger med henblik på chikane mod offeret.

Disse tre former for misbrug bliver omtalt i kapitel 3 (identitetsoplysninger), kapitel 4 (betalingskort-oplysninger) og kapitel 5 (chikane).

3 Misbrug af ID-oplysninger

3.1 Omfanget af misbrug

Som beskrevet i kapitel 1 er offerundersøgelsen gennemført som led i Danmarks Statistiks omnibus-undersøgelser. Offerundersøgelsen baserer sig på stikprøver blandt tilfældigt udvalgte danskere i alderen 16-74 år. 6.130 respondenter har i perioden fra august 2014 til og med januar 2015 fået stillet spørgsmål om identitetsmisbrug (se bilag 2). Af disse 6.130 respondenter angiver 51, eller 0,8 procent, at de har været udsat for identitetsmisbrug i løbet af de sidste 12 måneder. Det er vigtigt at understrege, at ikke alle, der har svaret "ja" til at være blevet udsat for identitetsmisbrug, også har lidt et tab. Det er imidlertid både i politiets anmeldelsesstatistik og i offerundersøgelser normal praksis at inkludere både forsøg på og fuldbyrdede kriminelle handlinger i statistikken.

Tabel 3.1 Offerrisiko for identitetsmisbrug i Danmark

	2009	2013	2014
Omfang af stikprøver	1.853	9.582	6.130
Andel af ofre for identitetsmisbrug (vægtet)	0,46 %	0,75 %	0,82 %
95 %-sikkerhedsinterval	0,3 – 0,9 %	0,6 – 0,9 %	0,6 – 1,1 %
Antal ofre i Danmark (estimat)	18.653	31.249[11]	34.471
95 %-sikkerhedsinterval (estimat)	12.165 – 36.495	24.924 – 37.386	25.181 – 46.166

Stikprøverne er repræsentative for befolkningen som helhed. Der kan dog være en skævhed i bortfaldet. For at teste, om der findes en sådan skævhed, udarbejder Danmarks Statistik vægte baseret på personoplysninger. Når disse vægte anvendes, er offerrisikoen stadig 0,8 procent, hvilket svarer til, at ca. 35.000 danskere har været udsat for identitetsmisbrug inden for de sidste 12 måneder. Da opgørelsen er baseret på stikprøver, er der en vis statistisk usikkerhed. Hvis en stikprøve – som antaget – er a-selektiv, kan et 95 %-sikkerhedsinterval[12] beregnes. Intervallet ligger mellem

[11] I 2013-rapporten nævnes antallet 46.900 (Kruize, 2013, s. 5), men dette tal er inklusiv chikane (socialt misbrug).

[12] Sikkerhedsintervallet bruges ved generalisering, når stikprøvens resultater skal overføres på en population. Statisk set, kan vi være 95 procent sikre på, at populationens mål vil falde inden for stikprøvens beregnede interval.

0,6 og 1,1 procent, eller, når det omregnes til at gælde hele den danske befolkning, mellem 25.181 og 46.166 danskere.

Offerundersøgelsen er behæftet med en række metodiske problemer (se bilag 1), og derfor bør estimatet tolkes med forbehold. Det er mere interessant at se på udviklingen i andelen af ofre. De tre målinger viser, at offerrisikoen tiltog i perioden fra 2009 til 2013. Målingen fra 2014 viste derimod ikke yderligere vækst i forhold til målingen fra 2013. Muligvis er (en af) forklaring(erne) en stigende risikobevidsthed blandt danskerne grundet den store medieopmærksomhed og de mange gode råd til at undgå identitetstyveri.

I offerundersøgelsen spørges der om, hvilke typer identitetsoplysninger der er blevet stjålet. Der sondres mellem tre typer: (bruger)navn/cpr-nummer, identitetsbeviser (pas, id-kort, sygesikringskort, kørekort) og bankoplysninger (kontonummer, adgangskode). Desuden findes en restkategori, der bl.a. inkluderer personer, som har mistet fx både kørekort og bankoplysninger. I dette tilfælde er der nemlig tale om en kombination. Tabel 3.2 viser oversigten.

Tabel 3.2 Offerrisiko efter type af misbrugte identitetsoplysninger

	2013 (n=64)	2014 (n=51)*
(Bruger)navn/cpr-nummer	28 %	42 %
Identitetsbeviser	5 %	23 %
Bankoplysninger	44 %	35 %
Kombination	14 %	-
Andet	9 %	-
I alt	**100 %**	**100 %**

* Kun 26 af de 51 respondenter har besvaret dette spørgsmål.

Af ukendte årsager har kun halvdelen af de udsatte respondenter i 2014-målingen besvaret spørgsmålet om, hvilke identitetsoplysninger der er blevet misbrugt. Dermed bliver det også svært at tolke tabel 3.2, og det er uklart, om misbruget af identitetsbeviser i virkeligheden var større i 2014 end i 2013.

3.2 Hensigten med misbrug

Identitetsoplysninger kan misbruges på mange forskellige måder. Meulen (2006) skelner mellem økonomisk og kriminelt misbrug. Meulen nævner desuden en tredje form for misbrug, nemlig identitetskloning. I et sådant tilfælde overtager gerningspersonen helt og aldeles en andens identitet. Selvom det ikke kan udelukkes, at identitetskloning finder sted, må det betragtes som et yderst

sjældent fænomen.[13] Der findes imidlertid eksempler på identitetsmisbrug, som ikke sigter mod økonomisk gevinst eller kriminelt misbrug, men snarere må rubriceres som chikane: Identitetsoplysninger misbruges med henblik på at opnå adgang til offerets digitale profil eller til at udsende beskeder i hans eller hendes navn. Chikane behandles ikke i dette kapitel, men i kapitel 5. Her ligger fokus på misbrug af identitetsoplysninger med et økonomisk sigte (bortset fra betalingskortoplysninger, der behandles i kapitel 4).

I forbindelse med økonomisk misbrug af identitetsoplysninger er det relevant at spørge, hvordan gerningspersonen tilegner sig penge, varer og/eller ydelser i en andens navn uden at blive sporet øjeblikkeligt. Til dette formål benyttes gerne et såkaldt muldyr: En person, der bevidst eller ubevidst hjælper den kriminelle med at transportere penge og/eller varer ud af landet. Typisk overføres stjålne penge til muldyrets konto, hvorefter pengene hæves i kontanter og sendes til udlandet. Muldyret rekrutteres oftest gennem spammails, der udsendes til mange tusinde modtagere på samme tid, og som lokker med hurtigt og lettjente penge.

Ved kriminelt misbrug af identitetsoplysninger anvender gerningspersonen offerets/muldyrets identitet, når og hvis han anholdes af politiet. Formålet med identitetsmisbrug er i dette tilfælde at undgå strafforfølgelse. I offerundersøgelsen oplyser meget få respondenter, at deres identitetsoplysninger er blevet misbrugt i forbindelse med vildledning af myndighederne.

Tabel 3.3 Hensigten med misbrug af identitetsoplysninger

	2013 (n=64)	2014 (n=51)
Køb på kredit	27 %	43 %
Leje af noget/tegning af abonnement	5 %	10 %
Overførsel af penge	42 %	32 %
Uspecificeret økonomisk misbrug	5 %	-
Kriminelt misbrug	3 %	2 %
Uoplyst formål	19 %	14 %
I alt	**100 %**	**100 %**

Tabel 3.3 viser, at der er to hovedformål med misbrug af identitetsoplysninger: køb på kredit og (at lokke andre til) overførsel af penge. Selvom mange webbutikker har lukket for muligheden for at købe på kredit, findes der stadig butikker, som opretholder denne praksis. Et eksempel på at lokke andre til overførsel af penge er en såkaldt "strandet i udlandet"-besked. Det foregår ved, at en e-mailkonto er blevet hacket, og at der derefter afsendes en besked til bekendte om, at kontoens

[13] 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 kunne slippe for problemet. Dette kaldes *pseudocide* (afledt af suicide), skrev Nyhedsavisen i oktober 2006 (Stove & Valeur, 2007, s. 37).

ejermand (under ferie) er strandet i udlandet og har brug for penge. Den kriminelle opfordrer herefter modtagerne til at overføre penge til fx Western Union.

3.3 Opdagelse og anmeldelse af identitetsmisbrug

Offeret opdager på et tidspunkt, at hans eller hendes identitetsoplysninger er blevet (forsøgt) misbrugt. I halvdelen af tilfældene bliver offeret gjort opmærksom på det af en tredjepart. Det kan være en virksomhed – fx et pengeinstitut, en webbutik eller en it-virksomhed som Facebook – eller en bekendt. Når man bliver kontaktet af en virksomhed og får at vide, at der er noget galt, er der en stor chance for, at skaden endnu ikke er sket. For to ud af tre respondenter inden for denne kategori viser det sig således, at der ikke har været et tab.

En anden måde at opdage misbrug af identitetsoplysninger på er ved modtagelse af udskrifter, regninger eller opkrævninger. I offerundersøgelsen rapporterede ca. hver tredje af ofrene for identitetsmisbrug, at han eller hun blev alarmeret på denne måde. Det er indlysende, at skaden er sket, så snart der opkræves betaling.

Den sidste mulighed er, at misbruget opdages rent tilfældigt. Godt 10 procent af respondenterne henhører i denne kategori. En af dem opdagede misbruget ved udskiftning af passwordet til en e-mailadresse. En anden blev mistænksom, da han igen opfordredes til at overføre penge i forbindelse med "strandet i udlandet"-fidusen. Et tredje eksempel er en respondent, der opdagede misbruget, mens han tilfældigt kontrollerede sin forsikring. Også for denne kategori gælder det, at forbrydelsen først erkendes efter, at den er fuldbyrdet.

I offerundersøgelsen spørges der om, hvorvidt de respondenter, der har været udsat for identitets-misbrug, har meldt sagen til politiet. I 2013-målingen angav 27 procent af respondenterne, at de havde anmeldt sagen. Undersøgelsen fra 2014 viste næsten det samme resultat; her havde 25 procent af respondenterne anmeldt (forsøg på) misbruget til politiet. Når misbruget opdages gennem en tredje person, anmeldes sagen mindre hyppigt til politiet (se tabel 3.4). Det er ikke overraskende, eftersom respondenterne i denne kategori ofte ikke oplever tab.[14]

[14] På grund af det begrænsede antal respondenter kan statistisk signifikans ikke påvises; en X^2-test af 'opdagelse gennem tredje person' versus 'udskrifter mm samt egen opdagelse' giver en p-værdi af 0,18.

Tabel 3.4 Opdagelse og politianmeldelse ved misbrug af identitetsoplysninger

	Ikke anmeldt	Anmeldt
Opdagelse gennem tredje person (n=26)	81 %	19 %
Udskrifter, regning, opkrævning (n=16)	62 %	38 %
Egen opdagelse (n=6)	67 %	33 %
Ukendt (n=3)	100 %	-
I alt	**75 %**	**25 %**

Når forurettede melder sagen til politiet, er det ikke altid ensbetydende med, at anmeldelsen optages. Fire af de 13 respondenter, der havde anmeldt sagen, tilkendegav således, at politiet afviste at modtage anmeldelsen. Der er ikke i undersøgelsen blevet spurgt om årsagen.

3.4 Tab på grund af identitetsmisbrug

Ved økonomisk misbrug af identitetsoplysninger kan der opstå et tab, men det sker ikke altid. I offerundersøgelsen angav 56 procent (2013) og 54 procent (2014) af de respondenter, der havde været udsat for misbrug, at der var sket et tab. Tabel 3.5 viser oversigten. Det gennemsnitlige tab (blandt de respondenter, der rapporterede om et sådant) var både i 2013 og i 2014 lidt under 9.000 kr. Gennemsnittet trækkes op på grund af enkelte større beløb. Derfor lå medianen på et lavere beløb, nemlig 3.280 kr. i 2013 og 3.500 kr. i 2014.

Tabel 3.5 Tabets omfang ved misbrug af identitetsoplysninger

	2013 (n=64)	2014 (n=51)
Intet tab	44 %	46 %
<= 1.000 kr.	16 %	13 %
1.001 – 5.000 kr.	19 %	17 %
5.001 – 10.000 kr.	9 %	4 %
>= 10.001 kr.	12 %	20 %
I alt	**100 %**	**100 %**
Gennemsnitligt tab	8.642 kr.	8.878 kr.
Mediane tab	3.280 kr.	3.500 kr.

I de fleste tilfælde hæfter ofrene ikke for tab, der knytter sig til identitetsmisbrug. I 2013 hæftede kun 31 procent af de bestjålne således selv for (en del af) tabet. Det drejede sig endda kun om en meget beskeden del af det samlede tab, nemlig 5 procent. I 2014 hæftede 24 procent af de bestjålne selv for (en del af) tabet. Her var deres andel af det samlede tab imidlertid større, nemlig 19 procent. Det skyldtes, at to respondenter havde relativt store tab, som de selv måtte dække, eftersom de var blevet lokket til at overføre penge.

3.5 Offerprofil i forbindelse med identitetsmisbrug

Som nævnt i kapitel 1 udarbejdes offerprofilen på baggrund af bopæl og uddannelsesniveau. Det giver i alt fire profiler, og tabel 3.6 viser, at offerrisikoen er 1,1 procent for dem, der bor i en bykommune (uanset uddannelsesniveau), og henholdsvis 0,8 procent (højtuddannede) og 0,5 procent (lavtuddannede) for de respondenter, der ikke bor i en bykommune. Vi må antage, at livsstil og (risiko)adfærd har en indflydelse på offerrisikoen. Hvorledes en persons bopælsadresse og uddannelsesniveau hænger sammen med livsstil og adfærd, kan ikke fastslås med denne undersøgelse.

Tabel 3.6 Offerrisiko ved identitetsmisbrug

	Offerrisiko
Højtuddannet, i bykommune (n=1.221)	1,1 %
Højtuddannet, *ikke* i bykommune (n=742)	0,8 %
Lavtuddannet, i bykommune (n=1.803)	1,1 %
Lavtuddannet, *ikke* i bykommune (n=2.364)	0,5 %

3.6 Netbankindbrud

Der findes stort set ingen registeroplysninger om misbrug af identitetsdata. Undtagelsen er netbankindbrud, som Finansrådet offentliggør oplysninger om. Anvendelse af internetbanker er de seneste år steget støt, og i 2014 benyttede 88 procent af de 16-74-årige danske internetbrugere en netbank (Danmarks Statistik, 2014). Af Danmarks Statistiks undersøgelse af danskernes it-anvendelse i 2014 fremgik det dog, at sikkerhedsbekymringer har afholdt 16 procent af internetbrugerne fra at benytte netbank. Det lyder lidt forvirrende – 88 plus 16 er lig med 104 procent – men de 16 procent refererer til aldersgruppen 16-89 år, mens de 88 procent refererer til aldersgruppen 16-74 år. Konklusionen må være, at årsagen til at fravælge netbank er frygt for misbrug.

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

- *Netbankindbrud*: Samtlige antal forsøg på netbankindbrud – både dem, der lykkes, og dem, der mislykkes. Forsøg, der mislykkes, skal forstås på den måde, at gerningspersonen skaffer sig adgang til en kundes netbank, men ikke formår at overføre penge. Forsøg, hvor "døren står åben", og gerningspersonen ikke er til stede til at gennemføre *real time phishing*, tælles ikke med. Dog tilkendegiver interviewrespondenten fra Finansrådet, at sidstnævnte sker en del for tiden (dvs. i efteråret 2012).

- *Netbankindbrud med tab*: Samtlige netbankindbrud, hvor det lykkes for gerningspersonen at slippe af sted med penge.
- *Tabets omfang:* Det beløb, som gerningspersonen tilegner sig. Dette korrigeres, såfremt nogle af pengene kommer retur. Banken dækker tabet for privatkunder, mens erhvervskunder selv hæfter.[15] Erhvervskunder kan tegne en forsikring mod netbankindbrud – separat eller som en del af en kriminalitetsforsikring – hos deres forsikringsselskab.

Omfang og udvikling af netbankindbrud

Antallet af netbankindbrud (inkl. forsøg) går op og ned. I nogle kvartaler finder der slet ingen indbrud sted, mens der i andre kvartaler registreres over 50. Rekorden blev sat i 3. kvartal 2008 med 106 indbrud. I perioden 2006-2014 blev der registreret 1.043 netbankindbrud, og i 448 tilfælde førte de til tab. Det svarer til et tab ved 43 procent af alle indbrud. Figur 3.1 viser, at tendensen stiger og falder i to bølger. Den første stigning fandt sted i årene 2007-2009 og den anden i årene 2012-2013. I mellemperioden (2010-2011) faldt antallet af indbrud til næsten nul, og det samme gjaldt for 2014. Den oplagte forklaring på det første fald (2010-2011) er introduktionen af NemID, Danmarks digitale signatur. NemID introduceredes 1. juli 2010 og anvendes til at få adgang til både netbank og offentlige services. Den afgørende forskel mellem NemID og den tidligere opkobling[16] til netbank er nøglekortet eller nøgleviseren. Hver gang, en kunde logger ind på sin netbank, kræves en unik, sekscifret nøgle, der aflæses på kortet/viseren. Dermed er der indlagt en væsentlig ekstra teknisk sikring. Figur 3.1 viser imidlertid også, at antallet af netbankindbrud allerede faldt til nul i det første halvår af 2010 – perioden umiddelbart før introduktionen af NemID. Den supplerende forklaring er, at nogle dataservere, som hackere brugte ret aktivt, blev lukket ned i løbet af 2009.

Kurven gik op igen i løbet af 2012. Via særlig malware kan it-kriminelle nemlig franarre en bankkunde hans 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.

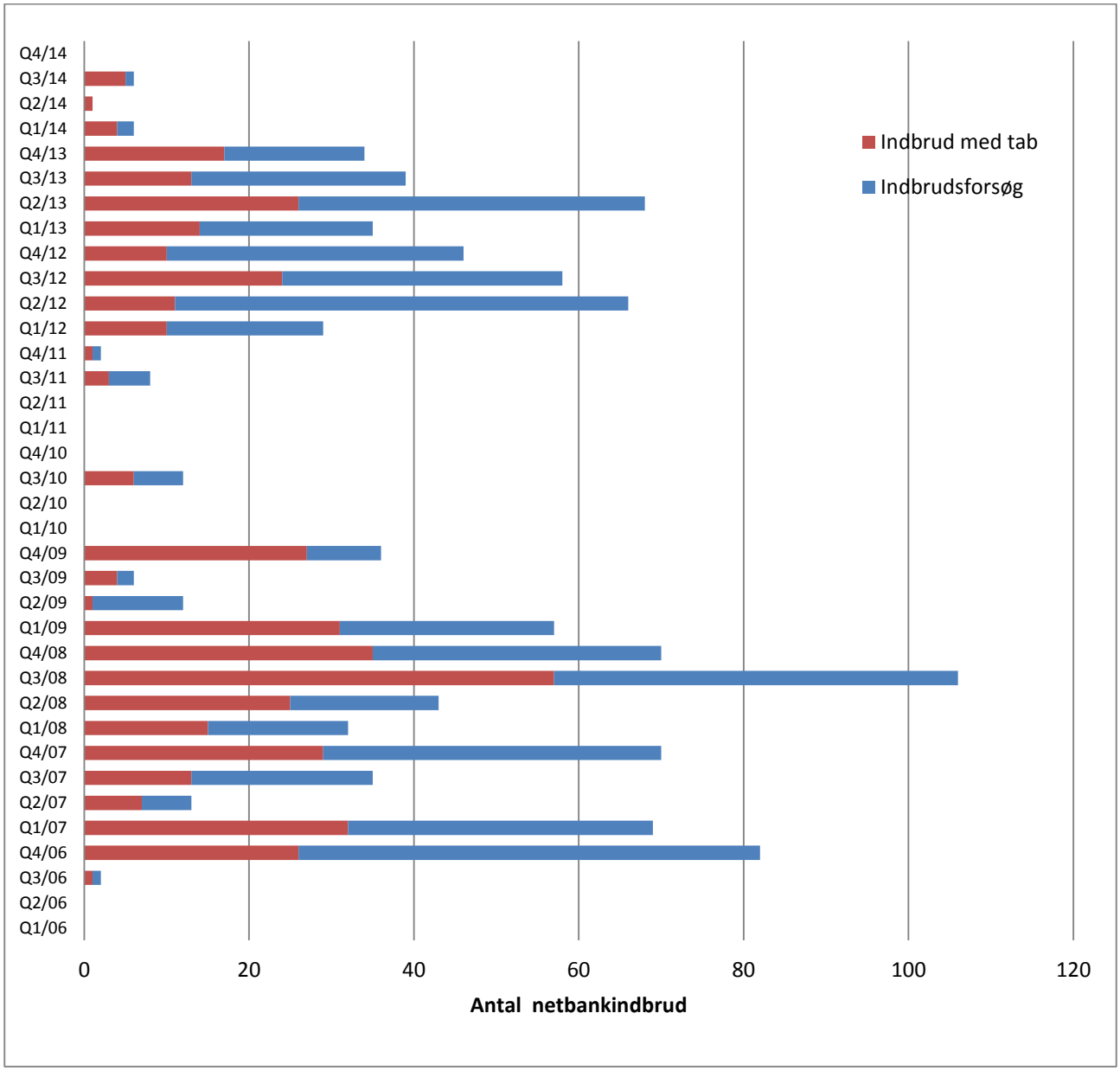
---

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

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

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.[17]

Figur 3.1 Udviklingen i antallet af netbankindbrud 2006-2014 (kvartalvis)



Kilde: Finansrådet.

Faldet i 2014 forklares ikke med et kriminalpræventivt tiltag, men med en ændring i de kriminelles adfærd. På Finansrådets hjemmeside gives følgende forklaring på 2014-faldet:

[17] Kunden kan undgå at blive franarret sin NemID-nøgle, hvis vedkommende ikke indtaster en ny nøgle.

> Vi ser lige nu en ændring i angrebsmønstret hos de it-kriminelle og lige for tiden er de angreb der rammer kunderne ikke netbankindbrud. I stedet snydes kunderne til selv at gennemføre overførslerne eller sende deres nøglekort til de kriminelle. Desværre lykkes det ofte og derfor er der god forretning for de kriminelle i denne meget enkle kriminalitet, hvor kunden blot spørges pænt om alle sikkerhedskoder og et indbrud derfor ikke er nødvendigt. (http://www.finansraadet.dk/Tal--Fakta/Pages/netbanksikkerhed.aspx)

Tab på grund af netbankindbrud

Det samlede tab på grund af netbankindbrud var i perioden 2006-2014 på 30,8 mio. kr. Som sagt fører kun lidt over 40 procent af indbruddene dog til et tab. Tabet er forskelligt fra indbrud til indbrud, men ligger i gennemsnit på næsten 70.000 kr.[18]

Det samlede årlige tab svinger – logisk nok – i takt med antallet af indbrud (med tab). Tabet ligger i de år, hvori antallet af indbrud er højt (2007-2009, 2012-2013), på 5-7 mio. kr. årligt, mens tabet ligger under en million kr. årligt i de år, hvori antallet af indbrud er lavt (2010-2011 og 2014).

Tabel 3.7 Netbankindbrud i Danmark (2006-2014)

	Antal netbank-indbrud	Antal netbank-indbrud m. tab	Procentdel af indbrud m. tab	Tabets omfang (mio. kr.)	Gennemsnitligt tab pr. indbrud
2006	84	27	32 %	1.9	72.169
2007	187	81	43 %	3,0	37.605
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
2013	176	70	40 %	5,3	75.547
2014	13	10	67 %	0,3	32.071
I alt	**1.043**	**448**	**43 %**	**30,8**	**68.785**

Kilde: Finansrådet, egne beregninger.

[18] 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.

4 Misbrug af betalingskort

Når en forbruger benytter sit betalingskort til at betale for en vare eller ydelse, igangsættes et samspil mellem en række aktører, således at betalingen kan gennemføres. De fem centrale aktører er kortselskab, kortudsteder (bank), kortindløser (fx Nets), betalingsmodtager (forretning) og kortbruger (forbruger) (Konkurrence- og Forbrugerstyrelsen, 2014, s. 10). Der findes en række forskellige typer af betalingskort. Konkurrence- og Forbrugerstyrelsen skelner mellem hævekort, debetkort[19], kreditkort[20], forudbetalte betalingskort og internationale betalingskort[21]. Traditionelt har betalingskortmarkedet i Danmark været domineret af Dankortet.

Betalingskortoplysninger er også en slags identitetsoplysninger, og det er netop disse, der oftest misbruges. I modsætning til ved identitetsmisbrug (kapitel 3) findes der på dette felt statistikker, som til dels er offentligt tilgængelige. Misbrug af betalingskort kan både ske i den fysiske (offline) verden og på internettet (online). I denne rapport er vi primært interesserede i online misbrug. Dette misbrug kan både ske på det danske internetmarked og på det internationale marked.

4.1 Betalingskortmisbrug på det danske marked

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 dankortdelen af kortet, der benyttes. Når kortet derimod anvendes i udlandet, bruges visadelen. Nets offentliggør kun tal vedrørende dankortdelen. Sagt med andre ord: misbrug på det danske marked.

---

[19] Debetkort er et betalingskort, hvor købsbeløbet trækkes fra forbrugerens konto med det samme eller senest næste bankdag. Derfor er det tit banker, som udsteder debetkort, da det er nødvendigt at have direkte adgang til kortbrugerens konto for at kunne trække købsbeløbet med det samme. Dankortet er et eksempel på et debetkort.

[20] Kreditkort er et betalingskort, hvor der går et vist tidsrum, inden beløbet trækkes fra forbrugerens konto. Eksempler på kreditkort er MasterCard, Diners Club og American Express.

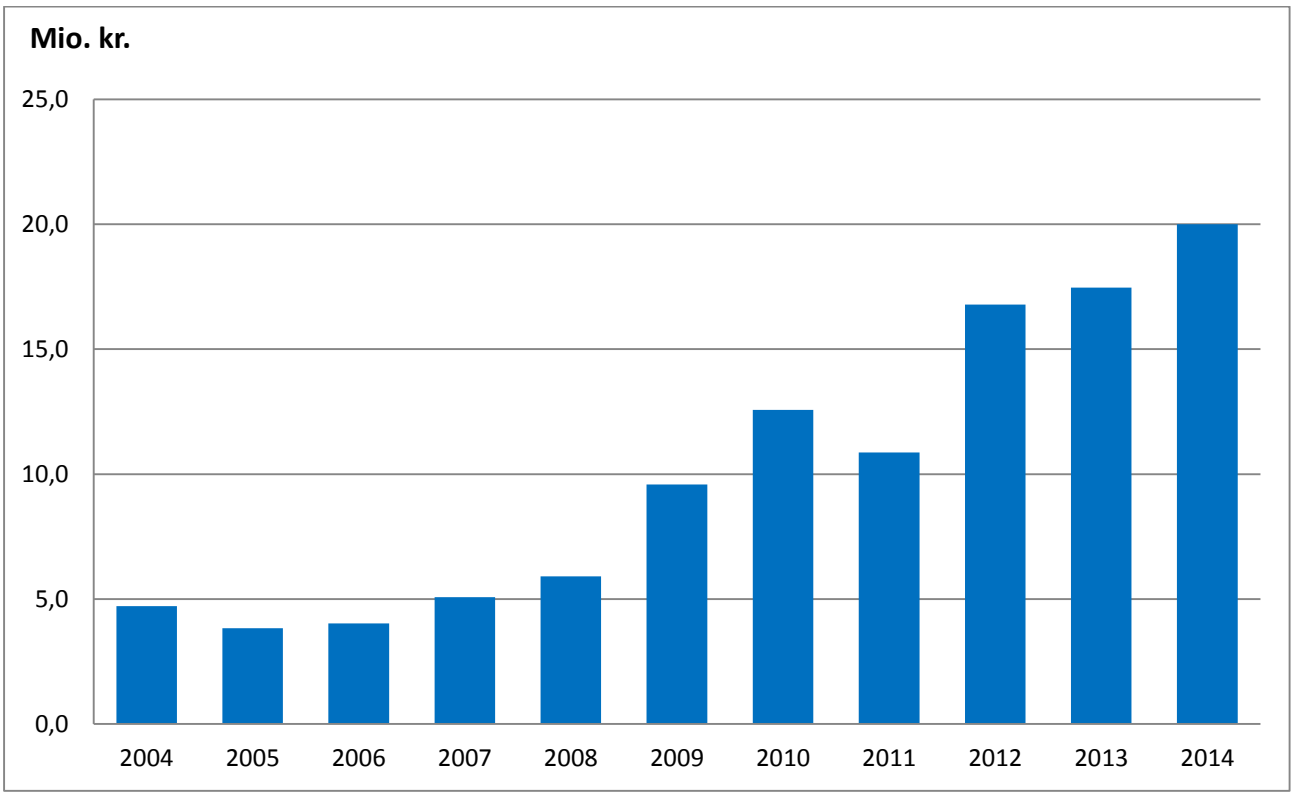
[21] Internationale betalingskort kan benyttes i flere lande. Disse kort kan være både debet- og kreditkort. Eksempler på internationale debet- og kreditkort er Visa Electron og MasterCard Debet (debetkort) samt Diners Club, AmericanExpress og MasterCard (kreditkort).

Nets offentliggør omfanget af tab på grund af dankortmisbrug. I forbindelse hermed deler Nets misbruget op i to hovedkategorier: tabt/stjålet og fjernsalg. Kategorien tabt/stjålet dækker også over fysiske afluringer, hvor dankortholdere får afluret deres PIN-kode under indtastning og derefter stjålet deres Dankort. Fjernsalg omfatter internet, postordre, telefonordre og betalingsautomater uden PIN-kode.

Figur 4.1 viser tabet ved fjernsalg i perioden fra 2004 til og med 2014. Tabet steg i denne periode fra 4,7 mio. kr. i 2004 til 20 mio. kr. i 2014, altså en firdobling. Det må antages, at misbrug på internettet står for den største del af fjernsalgstabet.

I perioden 2004-2013 viste tabet i kategorien tabt/stjålet mindre udsving, men lå omkring 30 mio. kr. om året; i 2014 steg tabet i kategorien tabt/stjålet imidlertid voldsomt til godt 45 mio. kr. Det betyder for det første, at misbrug af Dankort ved fjernsalg udgør en stigende andel af det samlede tab. I 2004 stod fjernsalg således for 14,2 procent af det samlede tab, mens andelen steg til 36,8 procent i 2013 (og 30,5 procent i 2014). Det er ikke overraskende, at internettet tegner sig for en voksende del af dankortmisbruget, eftersom internethandelen er i kraftig vækst. For det andet betyder det, at stigningen i det samlede tab kan tilskrives fjernsalg. Der ser ud til, at der altså ikke er tale om en forskydning fra offline dankortmisbrug til online misbrug, men om en vækst i online misbrug, siden offline misbrugniveauet er mere eller mindre stabilt i perioden 2004-2013.

Figur 4.1 Tab på grund af dankortmisbrug ved fjernsalg

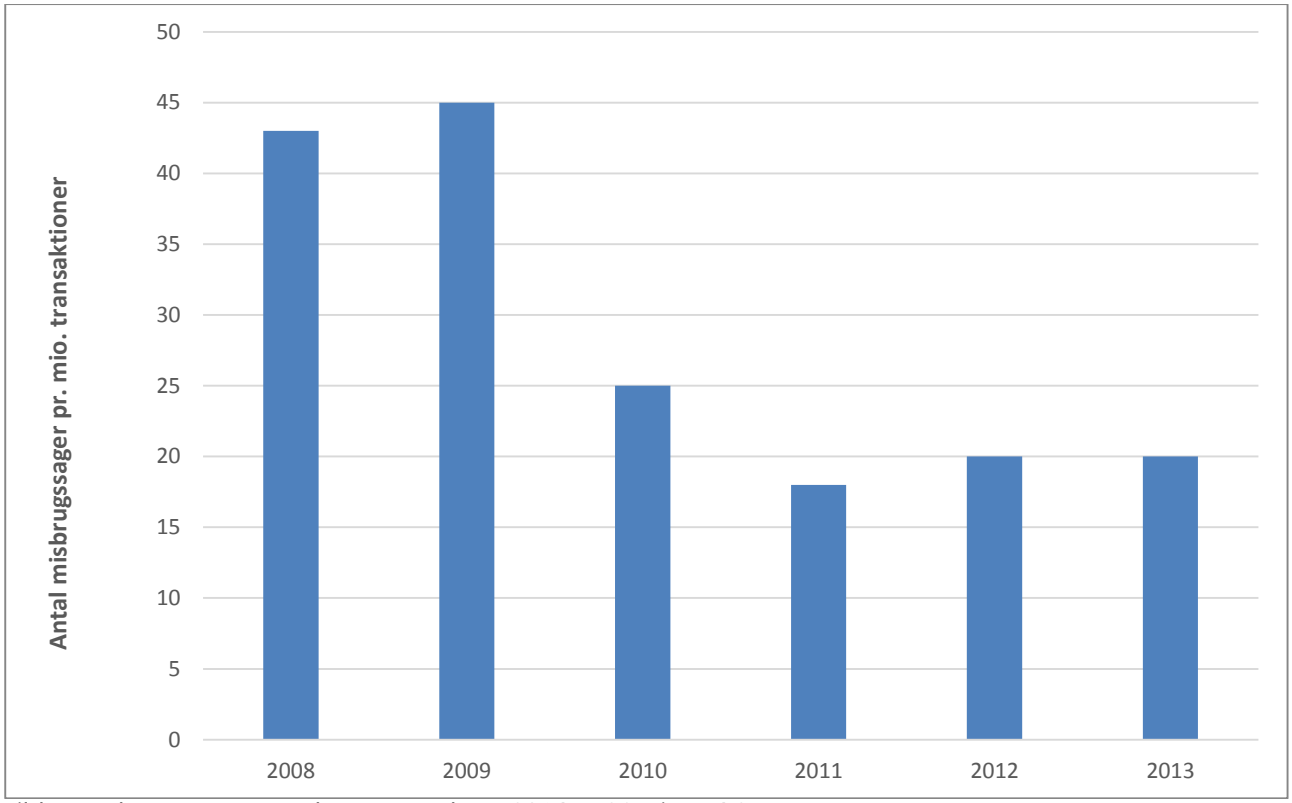


Kilde: Nets.

Hvad angår handel i offline verdenen, er forholdet mellem antallet af misbrugssager med Dankort og antallet af dankorttransaktioner faldet fra 5 til 3 sager om året pr. 1 mio. transaktioner i perioden fra 2008 til 2013 (Konkurrence- og Forbrugerstyrelsen, 2014, s. 39). Antallet af misbrugssager pr. 1 mio. transaktioner er i forbindelse med internethandel markant højere end ved fysisk handel.

På trods af at antallet af misbrugssager ved internethandel faktisk er steget fra 2008 til 2013 (se figur 4.1), er antallet af misbrugssager pr. 1 mio. transaktioner faldet i denne periode (se figur 4.2). Det skyldes, at der var langt flere transaktioner i forbindelse med internethandel i 2013, end der har været tidligere. Med andre ord; jo flere der handler på internettet, jo flere oplever misbrug, om end sandsynligheden for at blive udsat pr. transaktion var mindre i 2013 end tidligere.

Figur 4.2 Antal misbrugssager pr. 1 mio. dankorttransaktioner på internettet



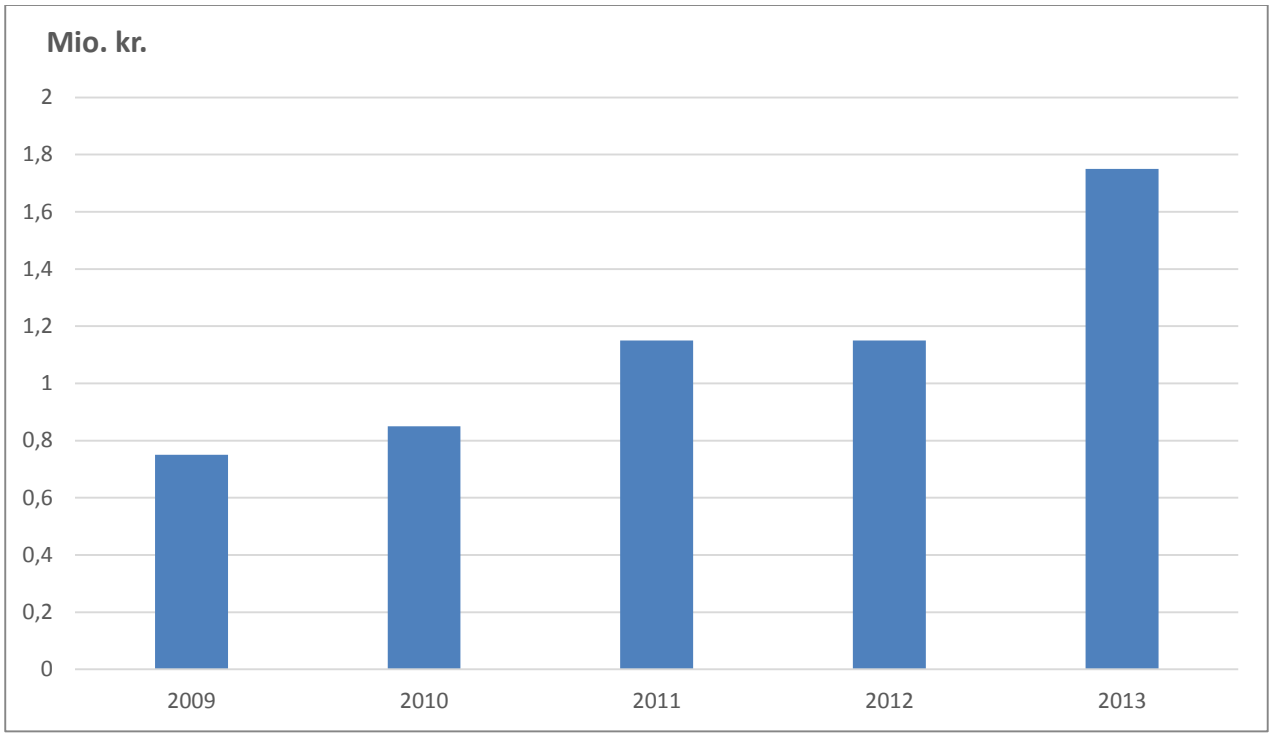
Kilde: Konkurrence- og Forbrugerstyrelsen, 2014, s. 39, Figur 4.2.

4.2 Misbrug af dansk udstedte internationale betalingskort i Danmark

Der findes som nævnt også andre betalingskort i Danmark. Størsteparten af de internationale kort indløses hos Teller – et datterselskab til Nets – men der findes også andre indløsere som Swedbank, Valitor og SEB Kort. Teller indløser op til 95 procent af al den handel, der foregår i fysiske butikker via internationale betalingskort. Ved internethandel er markedet i mindre grad domineret af Teller, men også her er dette firma den største aktør.

Der mangler et samlet overblik over misbrug af internationale kort i Danmark, da de enkelte kortselskaber ikke offentliggør deres misbrugstal. I rapporten Betalingskortmarkedet (Konkurrence- og Forbrugerstyrelsen, 2014) fremlægges dog et skøn foretaget på baggrund af oplysninger fra Mastercard, Visa, Nets, Danske Bank og SEB Bank. I perioden fra 2009 til 2013 steg tabet fra ca. 0,75 mio. kr. i 2009 til ca. 1,75 mio. kr. i 2013. Figur 4.3 viser oversigten.

Figur 4.3 Tab på internationale kort ved fjernsalg

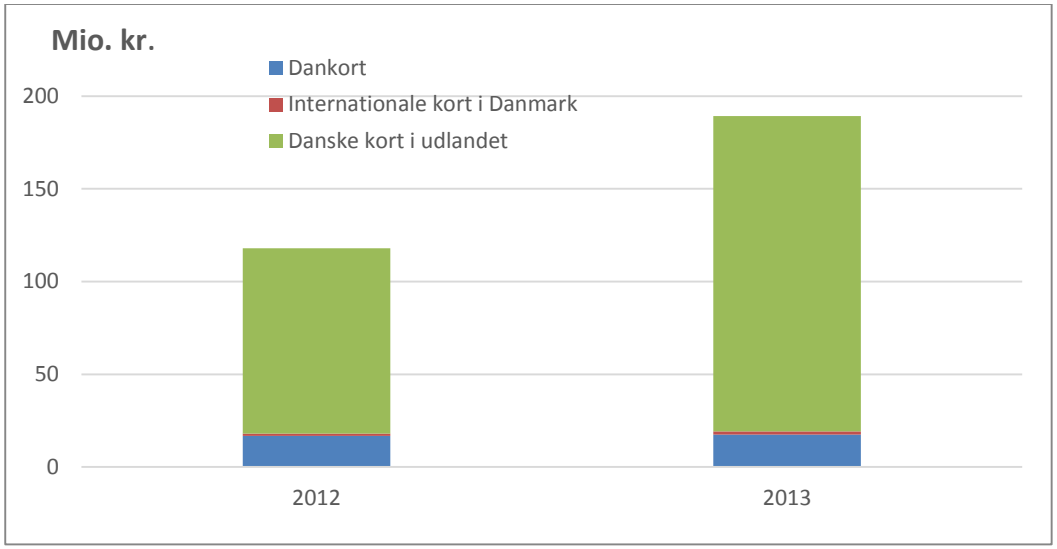


Kilde: Konkurrence- og Forbrugerstyrelsen, 2014, s. 42, Tabel 4.4.

4.3 Misbrug af dansk udstedte betalingskort i udlandet

Konkurrence- og Forbrugerstyrelsen har også undersøgt misbrug med dansk-udstedte betalingskort i udlandet, dog kun for årene 2012 og 2013. Også her gælder det, at de præcise tal er fortrolige, men opgørelsen viser klart, at det største tab med dansk-udstedte betalingskort finder sted i udlandet og hovedsageligt sker i forbindelse med fjernsalg (internethandel). I 2012 anslog Konkurrence- og Forbrugerstyrelsen tabet ved fjernslag til ca. 100 mio. kr., når der alene ses på misbrug af dansk-udstedte betalingskort i udlandet. I 2013 var dette beløb steget til ca. 170 mio. kr. Det betyder, at ca. 90 procent af alt misbrug af dansk-udstedte betalingskort ved internethandel i 2013 foregik i udlandet. Det samlede overblik findes i figur 4.4.

Figur 4.4 Samlede tab ved fjernsalg



Kilde: Konkurrence- og Forbrugerstyrelsen, 2014.

4.4 Kortmisbrug internationalt set

Den Europæiske Centralbank (ECB, 2014) publicerer tal om kortmisbrug i EU-landene.[22] I denne opgørelse anvendes den samme opdeling, som Nets benytter i forbindelse med statistik over dankortmisbrug: banker (ATM), fysiske forretninger (POS) og internettet (CNP).

Ifølge rapporten fra ECB blev 2,7 procent af danskerne udsat for kortmisbrug (online og offline) i 2012. Det svarer til, at 1,8 procent af alle udstedte kort blev misbrugt. Dermed ligger Danmark klart over gennemsnittet i SEPA-området, hvor tallene lyder på henholdsvis 1,8 og 1,2 procent.

Når vi ser nærmere på kortmisbrug i forbindelse med internethandel, viser det sig, at der er 335 misbrugssager pr. 1 mio. transaktioner med dansk-udstedte betalingskort, mens gennemsnittet i SEPA-området er 226 misbrugssager pr. 1 mio. transaktioner. Ifølge ECB steg misbruget af dansk-udstedte betalingskort i 2012 med 33 procent i forhold til 2011 (mod 12 procent i SEPA-området).

4.5 Tabsfordeling mellem parterne

Retsgrundlaget for internethandel er betalingstjenesteloven. § 74 i denne lov regulerer den såkaldte *charge back* ved fjernsalgstransaktioner (Karstoft, 2012): Betalerens udbyder er forpligtet til at undlade at gennemføre en betalingstransaktion eller til at tilbageføre et beløb, der allerede er

[22] SEPA: Single Euro Payments Areas, det vil sige alle EU-medlemsstater plus Schweiz, Island, Liechtenstein og Norge.

debiteret betalerens konto, såfremt betaleren fremsætter en eller flere af de indsigelser, der er opregnet i § 74, stk. 1, nr. 1-3:

- Nr. 1: det 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 omhandler således 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 love-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 indsigelse tabes inden for 13 måneders-fristen. Når kortindehaveren erklærer, at betalingskortet er misbrugt, skal udbyderen ifølge betalingstjenesteloven bære tabet. Indehaveren kan dog hæfte for en selvrisiko, der beskrives i betalingstjenesteloven § 62, stk. 2. Der skelnes mellem tre størrelser knyttet til selvrisikobeløbet (Karstoft, 2012):

- 1.100 kr. i selvrisiko, hvis pinkoden er mistet, uanset om det kan bebrejdes indehaveren af kortet (undtagelse: vold eller trussel om anvendelse af vold, hvorved der ikke er tale om en selvrisiko).
- 8.000 kr. hvis man har undladt at underrette kortudbyder snarest muligt; hvis indehaveren overgiver pinkoden, selvom han eller hun kunne/burde indse, at der er risiko for misbrug; hvis der er udvist groft uforsvarlig adfærd ved opbevaring af pinkoden.
- Ubegrænset. Selv oplyst pinkoden.

Reglerne for selvrisiko gælder ikke, hvis der ikke benyttes en personlig sikkerhedsforanstaltning, fx en pinkode. Ved internethandel med Dankort findes der ikke sådan en foranstaltning, og dette betyder, at indehaveren af kortet ikke hæfter for en selvrisiko. Det er anderledes, når internethandlen betales med et internationalt betalingskort. Både Visa og Mastercard benytter den såkaldte 3D Secure. Når der bruges 3D Secure, føjes der et ekstra sikkerhedstrin til betalingsforløbet. Det foregår ved, at kunden via sms modtager en engangskode, som skal indtastes umiddelbart efter, at kunden har indtastet sine kortoplysninger.

Når et Dankort bruges – i en ATM, butik eller på internettet – kontrolleres kortoplysningerne af Nets. Hvis kortet ikke er spærret, eller kortbrugen ikke virker mistænksom (fx gentagen brug af kortet inden for meget kort tid), gennemføres betalingen, uden at det hos kortudstederen (banken) kontrolleres, om der er dækning på kortet. Der er i princippet ikke et maksimumbeløb for træk på Dankortet, men en butik hæfter for tab over 4.000 kr. i forbindelse med en handel i offline-verdenen. Når en butiksejer tillader en kunde at betale et beløb over 4.000 kr., er det således på egen risiko. I

praksis reagerer butiksejerne forskelligt, når en kunde med et Dankort vil betale en vare, hvis pris overstiger 4.000 kr. Nogle butikker beder om legitimation, mens andre ikke gør. Ved internetkøb hæfter forretningen for tabet, når beløbet overstiger 1.000 kr., og der ikke er dækning.

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 med henblik på kontrol af, 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.

4.6 Misbrug af betalingskort (offerundersøgelse)

Som nævnt i kapitel 1 er offerundersøgelsen gennemført som led i Danmarks Statistiks omnibusundersøgelser. Offerundersøgelsen er baseret på stikprøver blandt tilfældigt udvalgte danskere i alderen 16-74 år. 6.130 respondenter har i perioden fra august 2014 til og med januar 2015 fået stillet spørgsmål om betalingskortmisbrug (se bilag 2). Af disse 6.130 respondenter angav 109, eller 1,8 procent, at de havde været udsat for betalingskortmisbrug inden for de sidste 12 måneder. Det skal dog tilføjes, at ikke alle disse 109 personer rent faktisk også havde lidt et tab. Det er imidlertid både i politiets anmeldelsesstatistikker og i offerundersøgelser almindelig praksis at inkludere såvel forsøg på som fuldbyrdede kriminelle handlinger.

Tabel 4.1 Offerrisiko for betalingskortmisbrug i Danmark

	2009	2013	2014
Omfang af stikprøver	1.853	9.582	6.130
Andel af kortmisbrugsofre (vægtet)	0,8 %	0,7 %	1,8 %
95 %-sikkerhedsinterval	0,4 – 1,2 %	0,6 – 0,9 %	1,5 – 2,1 %
Antal ofre i Danmark (estimat)	32.796	29.408	74.463
95 %-sikkerhedsinterval (estimat)	16.398 – 49.194	23.526 – 35.290	62.052 – 86.873

Stikprøverne er repræsentative for befolkningen som helhed. Der kan dog være en skævhed i bortfaldet. For at teste, om der er tale om en sådan skævhed, udarbejder Danmarks Statistik vægte baseret på personoplysninger. Når disse vægte anvendes, er offerrisikoen for betalingskortmisbrug stadig 1,8 procent. Dette svarer til, at ca. 75.000 danskere været udsat for betalingskortmisbrug i løbet af de sidste 12 måneder. Eftersom opgørelsen er baseret på stikprøver, er der en vis statistisk usikkerhed. Hvis en stikprøve – som antaget – er a-selektiv, kan et 95 %-sikkerhedsinterval beregnes. Intervallet ligger mellem 1,5 og 2,1 procent, eller, når det ganges op til at gælde hele befolkningen, mellem 62.052 og 86.873 danskere.

Offerundersøgelsen er behæftet med en række metodiske problemer (se bilag 1), og derfor bør estimatet tolkes med forbehold. Det er mere interessant at se på udviklingen i andelen af ofre. De tre målinger viser, at offerrisikoen var stabil i perioden fra 2009 til 2013. Målingen fra 2014 viser derimod en markant stigning i forhold til målingen fra 2013.

4.7 Opdagelse og anmeldelse af betalingskortmisbrug

Ofrene opdager på et tidspunkt, at deres kortoplysninger er blevet (forsøgt) misbrugt. Det sker typisk på to måder: enten ved, at betalingskortet spærres af kortudsteder/kortindløser, eller ved, at den forurettede modtager bankudskrifter, hvori der figurerer fratrukne beløb, som ikke kan genkendes. Det forekommer også, at forurettede ringes op af banken, eller at alarmklokkerne ringer på grund af modtagelse af en sms med opfordring til at indtaste en sikkerhedskode (3D Secure).

I offerundersøgelsen spørges der om, hvorvidt de respondenter, der har været udsat for kortmisbrug, har meldt sagen til politiet. Tabel 4.2 viser, at 61 procent af respondenterne svarede nej, og i de tilfælde, hvor sagen faktisk er blevet politianmeldt, er det ofte sket på foranledning af bank eller kortselskab.

Tabel 4.2 Opdagelse og politianmeldelse ved misbrug af kortoplysninger

	Ikke anmeldt	Bank/kortselskab anmelder	Respondenten anmelder
Udskrifter (n=47)	68 %	17 %	15 %
Kort spærret (n=46)	54 %	30 %	15 %
Ringet op af banken (n=7)	57 %	29 %	14 %
Sms om sikkerhedskode (n=2)	100 %	-	-
Ukendt (n=7)	57 %	-	43 %
I alt	**61 %**	**22 %**	**17 %**

Når forurettede anmelder sagen, er det ikke ensbetydende med, at politiet også optager anmeldelsen. To ud af de 18 respondenter, der selv har meldt sagen til politiet, tilkendegav således, at politiet afviste at modtage anmeldelsen. I undersøgelsen er der ikke blevet spurgt om årsagen hertil.

4.8 Tab på grund af kortmisbrug (offerundersøgelse)

Ved misbrug af kortoplysninger kan der opstå et tab, men ikke nødvendigvis. Nets fungerer som indløser af (Visa/)Dankort og sørger dermed for, at betalingen overføres fra køberens konto til forretningens. Dermed er Nets den mest centrale aktør i forbindelse med overvågningen af

dankortbetalinger, og overvågningen sker fra Nets' datacentral i Ballerup. Idéen bag overvågningen er at kunne slå ned på unormale betalingsmønstre. Kriterierne for disse er erfaringsbaserede og justeres løbende. Det kan fx dreje sig om en såkaldt hurtigløbsovervågning: Et kort benyttes inden for en kort tidsperiode både i kortudstederens egen bank og i en anden bank, og der indkøbes også for op til 4.000 kr. i en butik. I et sådant tilfælde spærres kortet præventivt. Derefter kontakter Nets banken, som efterfølgende informerer sin kunde.

I offerundersøgelsen angav 71 procent (2013) og 86 procent (2014) af de respondenter, der havde været udsat for misbrug af deres kortoplysninger, at de var blevet påført et tab. Tabel 4.3 viser oversigten. Det gennemsnitlige tab (blandt de respondenter, der havde lidt et sådant) var markant højere i 2013 end i 2014. Gennemsnittet trækkes op af enkelte større beløb. Derfor ligger medianen lavere, men også her var beløbet større i 2013 end i 2014. Årsagen til denne forskel er ukendt.

Tabel 4.3 Tabets omfang ved misbrug af kortoplysninger

	2013 (n=71)	2014 (n=109)
Intet tab	29 %	14 %
<= 1.000 kr.	10 %	16 %
1.001-5.000 kr.	26 %	41 %
5.001-10.000 kr.	12 %	12 %
>= 10.001 kr.	23 %	17 %
I alt	**100 %**	**100 %**
Gennemsnitligt tab	13.044 kr.	6.250 kr.
Mediane tab	4.995 kr.	3.250 kr.

I de fleste tilfælde hæfter ofrene ikke for tab, der knytter sig til betalingskortmisbrug. I 2013 hæftede 12 procent af de skadeslidte respondenter selv for (en del af) tabet. Det var imidlertid en meget beskeden del, og i alt betalte betalingskortmisbrugsofre selv kun 3 procent af det samlede tab. I 2014 måtte 23 procent selv dække (en del af) tabet. Her var andelen af det samlede tab samtidig også større, nemlig 8 procent. Det vides ikke, hvorfor andelen af respondenter, der selv hæftede, var større i 2014 end i 2013, men det er logisk, at de så også hæftede for en større andel af det samlede beløb.

Når det samlede tab i 2014 vægtes i forhold til den danske befolkning, er resultatet 200 mio. kr. Dette beløb ligger ikke ret langt fra det samlede tab, som Konkurrence- og Forbrugerstyrelsen har beregnet for 2013 (190 mio. kr.).

4.9 Offerprofil i forbindelse med betalingskortmisbrug

Som omtalt i kapitel 1 udarbejdes offerprofilen på baggrund af respondentens bopæl og uddannelsesniveau. Det giver i alt fire profiler, og tabel 4.4 viser, at offerrisikoen for kortmisbrug er størst for dem, der bor i en bykommune: 2,6 procent for højtuddannede og 2,1 for lavtuddannede. For de respondenter, der ikke bor i en bykommune, er offerrisikoen henholdsvis 1,6 (højtuddannede) og 1,2 procent (lavtuddannede). Også her bemærkes, at livsstil og (risiko)adfærd antageligt har en indflydelse på offerrisikoen. Hvorledes en persons bopælsadresse og uddannelsesniveau hænger sammen med livsstil og adfærd, kan ikke fastslås med denne undersøgelse.

Tabel 4.4 Offerrisiko for betalingskortmisbrug

	Offerrisiko
Højtuddannet, i bykommune (n=1.221)	2,6 %
Højtuddannet, *ikke* i bykommune (n=742)	1,6 %
Lavtuddannet, i bykommune (n=1.803)	2,1 %
Lavtuddannet, *ikke* i bykommune (n=2.364)	1,2 %

5 Chikane på internettet

Som nævnt i kapitel 2 kan identitetstyveri have flere ansigter. Der kan være tale om identitetsmisbrug (som omtalt i kapitel 3), misbrug af betalingskortoplysninger (omtalt i kapitel 4) og misbrug af personoplysninger med henblik på chikane mod offeret. I kapitel 2 blev det også beskrevet, at oprettelse af en falsk profil på internettet, altså tilfælde, hvor man udgiver sig for at være en anden, som udgangspunkt ikke i sig selv kan betragtes som strafbart. Suzanne Bjerrehuus oplevede misbrug af sine personoplysninger, da en person oprettede en profil i hendes navn og med billeder af hende på Facebook. Da hun politianmeldte sagen, fik hun det svar, at det ikke er strafbart at oprette falske profiler på Facebook (Stove & Valeur, 2007, s. 37).

Mobning eller chikane er heller ikke altid strafbart. Anklagemyndigheden har udgivet en pjece med råd og vejledning for dem, der er udsat for forfølgelse, chikane eller såkaldt stalking. Det anerkendes, at henvendelser, der ikke i sig selv er strafbare, kan opleves som ubehagelige og forstyrrende. Den konkrete vurdering af, hvorvidt der er tale om strafbar chikane, ligger hos politiet. På politiets hjemmeside kan man læse, at en række af bestemmelserne i straffelovens kapitel 27 om freds- og ærekrænkelser også gælder, når chikane eller lignende sker på internettet. Disse bestemmelser er imidlertid, med enkelte undtagelser, undergivet privat påtale; det vil sige, at det er op til den, chikanen retter sig imod, at anlægge en civil sag vedrørende spørgsmålet.

Når chikane består i misbrug af andres e-mailkonto, Facebook-profil eller lignende, kan straffelovens § 263, stk. 2 anvendes. Denne paragraf hører under straffelovens kapitel 27 om freds- og ærekrænkelser og er kendt som hacking-paragraffen: "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". Chefredaktøren på Berlingske Tidende, Lisbeth Knudsen, var i maj 2007 ude for, at der afsendtes en stribe e-mails til personer i hendes adressekartotek bl.a. med ordlyden: "Jeg vil gerne frabede mig alle jeres sleske e-mails." Knudsens computer var blevet angrebet af en hacker, der havde overtaget hendes e-mail-identitet (Stove & Valeur, 2007, s. 37). Misbrug af en Facebook-profil er i pressen døbt Facerape. Politiken[23] berettede i 2013 om en sag, hvori to teenagedrenge ved retten i Helsingør idømtes bøder på henholdsvis 2.000 og 4.000 kr. for at logge ind på en jævnaldrende piges Facebook-konto og ændre hendes profil.

[23] "Drenge får bøde for at ændre i piges Facebook profil", Politiken, 20. februar 2013.

Drengene sigtedes for overtrædelse af brevhemmeligheden, blufærdighedskrænkelse og for at viderebringe meddelelser om andres forhold.

Privat påtale kan ske med henvisning til persondataloven. Det er derimod mere oplagt at rette henvendelse til Datatilsynet. Ifølge persondataloven kan man protestere mod offentliggørelse af oplysninger og/eller billeder, men kun hvis indehaveren ikke selv har lagt dem ud på internettet. Datatilsynet skriver i denne forbindelse: "Når du offentliggør billeder af eller oplysninger om dig selv, gør du det samtidig muligt for andre at bruge oplysningerne. Datatilsynet vil som oftest ikke kunne hjælpe dig med at få andre til at slette de oplysninger eller billeder, som du selv har offentliggjort. Du kan eventuelt påberåbe dig ophavsret til dine billeder – men Datatilsynet kan ikke hjælpe dig med spørgsmål om ophavsret."

5.1 Omfanget af chikane

Som beskrevet i kapitel 1 er offerundersøgelsen gennemført som led i Danmarks Statistiks omnibus-undersøgelser. Offerundersøgelsen er baseret på stikprøver blandt tilfældigt udvalgte danskere i alderen 16-74 år. Der blev stillet spørgsmål om chikane på nettet (se bilag 2) til 6.130 respondenter i perioden august 2014 til og med januar 2015. Af disse 6.130 respondenter angav 22, eller 0,4 procent, at de havde været udsat for chikane inden for de sidste 12 måneder.

Stikprøverne er repræsentative for befolkningen som helhed. Der kan dog være en skævhed i bortfaldet. For at teste, om der er tale om en sådan skævhed, udarbejder Danmarks Statistik vægte baseret på personoplysninger. Når disse vægte anvendes, er offerrisikoen for chikane stadig 0,4 procent. Dette svarer til, at 15.955 danskere har været udsat for chikane i løbet af de sidste 12 måneder. Eftersom opgørelsen er baseret på stikprøver, er der en vis statistisk usikkerhed. Hvis en stikprøve – som antaget – er a-selektiv, kan et 95 %-sikkerhedsinterval beregnes. Intervallet ligger mellem 0,2 og 0,5 procent, eller, når det ganges op til at gælde hele den danske befolkning, mellem 9.117 og 22.793 danskere.

Tabel 5.1 Offerrisiko for chikane i Danmark

	2009	2013	2014
Omfang af stikprøver	1.853	9.582	6.130
Andel af chikaneofre (vægtet)	0,05 %	0,29 %	0,38 %
95 %-sikkerhedsinterval	0,0 – 0,3 %	0,2 – 0,4 %	0,2 – 0,5 %
Antal ofre i Danmark (estimat)	2.802	14.027	15.955
95 %-sikkerhedsinterval (estimat)	0 – 16.812	9.351 – 18.703	9.117 – 22.793

Offerundersøgelsen er behæftet med en række metodiske problemer (se bilag 1), og derfor bør estimatet tolkes med forbehold. Det er mere interessant at se på udviklingen i offerandelen. De tre

målinger viser, at offerrisikoen tiltog i perioden fra 2009 til 2013. Målingen fra 2014 viser derimod ikke yderligere vækst i forhold til målingen fra 2013, idet den begrænsede stigning ikke er statistisk signifikant.

I offerundersøgelsen blev der spurgt om, hvorledes chikanen ytrede sig, og der var tale om flere forskellige måder. Tallene er forholdsvis små, men den mest scorende kategori var modtagelse af uønskede e-mails (ikke spam, men målrettet mod ens egen person). Tabel 5.2 viser oversigten.

Tabel 5.2 Fremgangsmåde ved chikane

	Antal	Procentdel
Modtagelse af uønskede e-mails (ej spam)	8	36 %
Afsendelse af e-mails i offerets navn	4	18 %
Profilændringer	2	9 %
Chat i offerets navn	1	5 %
Flere hændelser	3	14 %
Andet (uspecificeret)	4	18 %
I alt	**22**	**100 %**

5.2 Hensigt med og varighed af chikane

I en rapport om stalking (Tambour Jørgensen, 2013) sagde to ud af tre respondenter, at de kendte stalkeren. Det kunne være en ekskæreste, men også en arbejdskollega, studiekammerat eller en person, man havde mødt ved en fest. I denne offerundersøgelse af chikane på nettet svarede kun to af de 22 ramte respondenter (9 procent), at de kendte den person, der stod bag chikanen mod dem. Når gerningspersonen er ukendt, er det heller ikke muligt at fastslå, hvad det formodede formål med chikanen har været. Kun fem respondenter var således i stand til at besvare dette. To respondenter tilkendegav, at det handlede om opmærksomhed eller kontrol. To respondenter svarede, at den person, der stod bag chikanen var psykisk syg. Den sidste respondent havde ingen anelse om motivet.

Ovenstående tyder på, at respondenterne ikke havde stalking eller mobning i tankerne ved besvarelse af spørgsmålet om chikane.[24] I spørgeskemaet blev chikane beskrevet som følgende: "En eller flere personer har brugt internettet til at chikanere dig. Fx ved at skrive negative beskeder om dig på sociale medier, at sende beskeder fra din mailkonto, chatte i dit navn eller ved ændringer på din Facebook-profil uden tilladelse."

[24] Det målte omfang peger også i denne retning. I undersøgelsen af stalking tilkendegav 2,9 procent af respondenterne, at de havde været udsat for stalking inden for de seneste 12 måneder (Tambour Jørgensen, 2013, s. 9).

For 15 af de 22 chikaneofre var der tale om et kortvarigt forløb, formentlig en enkeltstående begivenhed (svaret "op til en uge" ved spørgsmålet om varighed). To respondenter tilkendegav, at chikanen varede op til to måneder, mens fem svarede, at den stadig stod på.

5.3 Politianmeldelse af chikane

I offerundersøgelsen blev der spurgt om, hvorvidt de respondenter, der havde været udsat for chikane, havde anmeldt sagen til politiet. I 2013-målingen svarede tre ud af 28 respondenter (11 procent) ja, og i offerundersøgelsen fra 2014 angives nogenlunde samme resultat; her havde to ud af 22 respondenter (10 procent) anmeldt chikanen. Dette kan afspejle, at offeret ikke betragter chikanen som en kriminel handling, eller er usikker på, om sagen er alvorlig nok til at blive anmeldt.

5.4 Offerprofil i forbindelse med chikane

De 22 respondenter, der havde været udsat for chikane, adskilte sig ikke fra de respondenter i stikprøverne, som ikke var blevet ramt. Det gælder både for kønsfordeling, alder, herkomst, husholdning, uddannelse, erhverv og bopælskommune.

6 Bedrageri ved internethandel

Der handles mere og mere på internettet. Ifølge en analyse fra Foreningen for Dansk Internet Handel (FDIH) gennemførte danskerne således i 2014 132 mio. handler, en stigning på 27 procent i forhold til 2013. Det svarer til en omsætning på 73,7 mia. kr. i 2014. De tre vigtigste årsager til indkøb på nettet er pris, udvalg og bekvemmelighed. Unge på 18-25 år og børnefamilier køber oftest ind i kategorien tøj, smykker og sko, mens kunder over 50 år mest køber rejser og kulturoplevelser. Langt de fleste kunder (94 procent) er meget tilfredse med internethandelen. Dankort og andre betalingskort bliver brugt i 81 procent af internetkøbene (FDIH, 2014). Internethandelen foregår dog ikke kun i webbutikker – også privatpersoner sælger ud, fx via dba.dk, qxl.dk og lauritz.com.

6.1 Falske internetbutikker

På ethvert sted, hvor der handles for så mange penge, findes der kriminelle, der forsøger at få fat i en del af pengene. Derfor har man bl.a. indført e-mærket, der er en mærkningsordning for sikker nethandel, med henblik på at beskytte danskere, som handler på internettet. E-mærket administreres af handelsfonden, der er en non profit-organisation, som blev stiftet i 2000 af en række brancheorganisationer. Der er i alt 1.775 e-mærkede internetbutikker (pr. 19. marts 2015).

På e-mærkets internetside opfordres forbrugerne til at være opmærksomme på falske internetbutikker (fupbutikker). I slutningen af 2013 bekendtgjorde e-mærkets direktør, at "Vores undersøgelse viser, at der lige nu er mindst 755 butikker på nettet, der forsøger at sælge kendte mærkevarer til danske forbrugere under dække af at være ægte. Det er vores klare formodning, at der er flere fupbutikker, som endnu ikke er opdaget. Fælles for dem alle er, at de sælger populære produkter som tøj, sko, tasker, solbriller og smykker fra mærker som Nike, Burberry, Mulberry, Marc Jacobs og Ralph Lauren." I september 2014 holdt e-mærket øje med 1.141 såkaldte fupbutikker, der markedsførte sig over for danske forbrugere fra baser i lande som Kina, Malaysia og Rusland (emaerket.dk).

Den 1. oktober 2014 oplyste e-mærket, at Statsadvokaten for Særlig Økonomisk og International Kriminalitet (SØIK), også kaldet Bagmandspolitiet, havde lukket en udenlandsk fupbutik (med en .dk-internetadresse), hvor man kunne købe falske Ray-Ban-solbriller, der blev markedsført som ægte. E-

mærket forsøger også at begrænse skaden ved at forebygge, at danskerne handler i en fupbutik. I samarbejde med DR Skole er der udviklet et nyt undervisningstema under navnet "Fup på nettet", hvor skoleeleverne kan træne deres færdigheder inden for netsikkerhed. Projektet er støttet af Det Kriminalpræventive Råd. Ifølge e-mærket kan en fupbutik gennemskues, hvis man er opmærksom på sprogfejl, skæve priser, alt for billige mærkevarer, mangelfulde eller falske virksomheds-oplysninger, mistænkelige betalingsmuligheder og en omdirigeret webadresse.

6.2 Private handler på internettet

Danskere handler også privat på internettet, og der findes utallige internetsider, hvor man kan opslå en salgs- eller købsannonce. Mange af disse internetsider retter sig mod et bestemt publikum. Fx findes både 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.

Mange private sælgere annoncerer på dba.dk, og som udgangspunkt er der ingen fortrydelsesret i handler private imellem. Men også mange erhvervsdrivende benytter DBA som platform, og indgås der handler med disse, gælder 14 dages returret ifølge forbrugeraftaleloven. Ifølge DBA gennemføres der hver eneste måned mere end 700.000 handler på sitet (mere end 8 mio. handler om året). I princippet blander DBA sig ikke i handlerne, men på siden kan læses gode råd til, hvordan der købes sikkert. Bl.a. er der advarsler mod falske annoncer og hælervarer.

For at øge sikkerheden ved køb tilbyder DBA NemID-validering af sælgeren. Dette er udelukkende et tilbud og 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.

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

6.3 Bedrageri ved internethandel

Som beskrevet i kapitel 1 er offerundersøgelsen gennemført som led i Danmarks Statistiks omnibus-undersøgelser. Offerundersøgelsen baserer sig på stikprøver blandt tilfældigt udvalgte danskere i alderen 16-74 år. Der er stillet spørgsmål om bedrageri ved internethandel (se bilag 2) til 6.130 respondenter i perioden august 2014 til og med januar 2015. Af disse 6.130 respondenter angav 34, eller 0,55 procent, at de havde været udsat for bedrageri ved internethandel inden for de sidste 12 måneder. Dette procentantal dækker over både bedrageri ved køb i en internetbutik og bedrageri ved privat nethandel. Af de 34 ofre er 25 blevet bedraget ved køb i en netbutik, otte ved privathandel og en enkelt respondent er blevet ramt ved begge former for internethandel.

Stikprøverne er repræsentative for befolkningen som helhed. Der kan dog være en skævhed i bortfaldet. For at teste, om der er tale om en sådan skævhed, udarbejder Danmarks Statistik vægte baseret på personoplysninger. Når disse vægte anvendes, er risikoen for handelsbedrageri 0,54 procent. Dette svarer til, at ca. 22.500 danskere har været udsat for internethandelsbedrageri i løbet af de sidste 12 måneder. Eftersom opgørelsen er baseret på stikprøver, er der en vis statistisk usikkerhed. Hvis en stikprøve – som antaget – er a-selektiv, kan et 95 %-sikkerhedsinterval beregnes. Intervallet ligger mellem 0,4 og 0,8 procent, eller, når det ganges op til at gælde hele den danske befolkning, mellem 16.876 og 28.690 danskere.

Tabel 6.1 Offerrisiko for bedrageri ved internethandel i Danmark

	2013	2014
Omfang af stikprøver	9.582	6.130
Andel af ofre for handelsbedrageri (vægtet)	2,4 %	0,54 %
95 %-sikkerhedsinterval	2,1 – 2,7 %	0,4 – 0,8 %
Antal ofre i Danmark (estimat)	109.940	22.783
95 %-sikkerhedsinterval (estimat)	96.197 – 123.682	16.876 – 28.690

Offerundersøgelsen er behæftet med en række metodiske problemer (se bilag 1), og estimatet bør derfor tolkes med forbehold. Det er således mere interessant at se på udviklingen i andelen af ofre. 2013- og 2014-målingerne viser, at offerrisikoen faldt markant i 2014 i forhold til 2013. Der kan kun spekuleres over årsagen eller årsagerne. Muligvis har (medie)opmærksomheden på falske internetbutikker haft en positiv effekt. Det er også muligt, at danskerne er blevet mere varsomme ved private handler og holder øje med NemID-valideringen på handelsplatforme som DBA.

6.4 Handelssted og handelsvare

I alt tilkendegav 26 respondenter, at de havde været udsat for bedrageri ved køb i en internetbutik. På spørgsmålet om, hvorvidt det var en dansk eller en udenlandsk webbutik, var otte respondenter

ikke i stand til at svare. Af de resterende respondenter svarede 13, at det havde drejet sig om en udenlandsk netbutik, mens fem var blevet bedraget i en dansk butik. Selvom tallene er små, tyder det på, at bedrageri er mere hyppigt i udenlandske butikker. Dette står i modsætning til, hvor de fleste danskere handler på nettet. Ifølge FDIH (2014) finder 68 procent af alle internethandler (foretaget af danskere) sted i en dansk netbutik, 22 procent i en udenlansk butik, mens 10 procent er ukendt.

Ni personer har rapporteret om bedrageri i forbindelse med privathandel. Fem var blevet bedraget som købere, mens fire var blevet snydt som sælgere. Fire oplyser, at de havde benyttet sig af DBA som handelsplatform, mens andre fire havde handlet på en anden webside. Den sidste bedragne respondent havde handlet på Facebook.

Der er også blevet spurgt om, hvilken vare respondenten ville købe eller sælge i forbindelse med bedrageriet. Selvom omfanget af handelsbedragerier er faldet markant i 2014 i forhold til 2013, er fordelingen i de forskellige varekategorier ikke væsentlig anderledes. Undtagelserne er kategorien "Elektronik og hvidevarer", der scorede relativt højere i 2014, og kategorien "IT, tele og foto", som scorede relativt lavere i 2014. Det skyldes formentlig kategoriseringen. I 2013-undersøgelsen blev der spurgt om den konkrete vare, mens man i 2014-undersøgelsen spurgte om varekategorien. Bedrageri med mobiltelefoner er i 2013-undersøgelsen opført under "IT, tele og foto". Muligvis har 2014-respondenterne opfattet en mobiltelefon som henhørende til "Elektronik og hvidevarer".

Varekategorien "Tøj, sko og smykker" placerer sig øverst på listen over produkter, der snydes med i forbindelse med internethandel. En fjerdedel af respondenterne har således oplevet snyd i forbindelse med køb/salg i denne varekategori, hvilket er en større andel, end kategorien tegner sig for i nethandelsomsætningen. En anden kategori, der skiller sig negativt ud i forhold til andelen af omsætningen, er "Kosmetik, medicin og kosttilskud". Denne kategori står for 16-18 procent af bedragerierne, mens dens andel af nethandelsomsætningen kun udgør omkring 5 procent. Tabel 6.2 viser hele oversigten.

Tabel 6.2 Handelsbedrageri: varekategorier

	2013 (n=233)	2014 (n=34)	Nethandel*
Tøj, sko og smykker	26 %	25 %	16 %
IT, tele og foto	24 %	11 %	13 %
Elektronik og hvidevarer	2 %	25 %	9 %
Kosmetik, medicin og kosttilskud	16 %	18 %	5 %
Anden kategori	32 %	21 %	57 %

* FDIH handelsanalyse 2012, s. 17; analyser af nyere dato er kun tilgængelige mod betaling.

6.5 Politianmeldelse af internethandelsbedrageri

Ofrene opdager på et tidspunkt, at de er blevet snydt i forbindelse med en internethandel. Når det drejer sig om køb, modtager de måske aldrig den bestilte vare, eller også lever varen ikke op til forventningerne (fx kopivarer). Bedrageri ved internetsalg består i, at den forurettede part ikke modtager betaling.

I offerundersøgelsen spørges der til, hvorvidt de respondenter, der har været udsat for handelsbedrageri, har meldt sagen til politiet. Tabel 6.3 viser, at ca. 80 procent af respondenterne svarede nej. I de tilfælde, hvor sagen er blevet politianmeldt, er det tit sket på foranledning af banken eller kortselskabet.

Tabel 6.3 Opdagelse og politianmeldelse ved internethandelsbedrageri

	2013 (n=233)	2014 (n=34)
Ikke anmeldt	82 %	78 %
Respondent anmelder	18 %	13 %
Bank/kortselskab anmelder		9 %

Når forurettede anmelder sagen, er det ikke ensbetydende med, at politiet faktisk optager anmeldelsen. 10 af de 46 respondenter (otte i 2013 og to i 2014), der selv meldte sagen til politiet, tilkendegav, at anmeldelsen blev afvist. Der er i undersøgelsen ikke blevet spurgt om årsagen hertil.

6.6 Tab på grund af bedrageri ved internethandel

I 2013-undersøgelsen berettede nogle respondenter om store tab. En enkelt havde lidt et tab på 95.000 kr. i forbindelse med et bilsalg, mens en anden havde mistet 100.000 kr. til en ejendomsmægler. Så store beløb nævnes ikke i 2014-undersøgelsen. Derimod tilkendegav 13 procent af respondenterne i 2014-undersøgelsen, at de ikke havde lidt tab. Målingerne fra 2013 og 2014 har tilfælles, at tabsbeløbet af internethandelsbedragerisagerne sjældent overstiger 5.000 kr. Tabel 6.4 viser oversigten.

I de fleste tilfælde hæfter ofrene selv for tab, der knytter sig til handelsbedrageri. I 2013 gjaldt det således 74 procent af de respondenter, der havde lidt tab. I alt betalte ofre for handelsbedrageri selv 46 procent af det samlede tab. I 2014 hæftede 70 procent af de respondenter, der havde mistet penge, selv for (en del af) tabet. Her var andelen af det samlede tab 38 procent.

Tabel 6.4 Tabets omfang ved internethandelsbedrageri

	2013 (n=233)	2014 (n=34)
Intet tab	-	13 %
<= 1.000 kr.	59 %	52 %
1.001-5.000 kr.	30 %	35 %
5.001-10.000 kr.	5 %	-
>= 10.001 kr.	6 %	-
I alt	**100 %**	**100 %**
Gennemsnitligt tab	3.865 kr.	1.184 kr.
Mediane tab	800 kr.	600 kr.

6.7 Offerprofil i forbindelse med bedrageri ved internethandel

De 34 respondenter, der ifølge 2014-målingen havde været udsat for handelsbedrageri, adskilte sig ikke ret meget fra de respondenter i stikprøverne, som ikke var blevet ramt. Det gælder både for kønsfordeling, alder, herkomst, uddannelse, erhverv og bopælskommune. Undtagelsen er respondenternes husholdning. Det viser sig, at børnefamilier (par med børn) er hyppigere udsat for handelsbedrageri end respondenter i de øvrige husholdninger; 71 procent af de udsatte for handelsbedrageri hører under kategorien børnefamilie, mens 51 procent af de ikke-udsatte for handelsbedrageri hører under denne kategori. Forskellen er statistisk signifikant.[25]

[25] X^2=5,516; df=1; p=0,019.

7 Forskudsbedrageri

Forskudsbedrageri henviser til de former for bedrageri, hvor offeret bliver lokket til at betale et forskud med henblik på at opnå et eller andet. I øjeblikket findes to kendte varianter af forskudsbedrageri på nettet: de såkaldte Nigeria-breve og datingbedrageri (eller romance scam).

7.1 Nigeria-breve

Nigeria-breve er det udtryk, der i Danmark typisk bruges som henvisning til forskudsbedrageri. Et Nigeria-brev er et brev (e-mail) fra en person, der påstår, at han eller hun har en stor sum penge, som vedkommende ønsker at få ud af sit land, og til det formål har personen brug for hjælp fra adressaten. Som belønning skal det store pengebeløb deles. Svindelen består i, at offeret først skal sende et beløb, inden den store sum kan overføres. Det stopper dog som regel ikke, når man har sendt den første portion penge. Offeret får at vide, at der lige mangler lidt mere, hvis det hele skal falde i hak, og mange bliver dermed fanget i en negativ spiral: Man har investeret et beløb, men gevinsten udløses kun, hvis man investerer lidt mere.

Videnskab.dk citerer en repræsentant for bagmandspolitiet (SØIK) for, at politiet jævnligt modtager anmeldelser om forskellige former for svindel og bondefangeri, der alle henhører under kategorien Nigeria-breve:

- Falske arvemeddelelser
- Ordrer til firmaer om vareleverancer til Vestafrika
- Salg af sortfarvede pengesedler
- Tilbud om penge fra krigsbytte eller konti i krigsramte lande
- Falske gevinstmeddelelser i lotterier
- Tiggerbreve fra afrikanske børn.

Disse breve kommer nogle gange fra Nigeria, men langtfra altid. Årsagen til, at de kaldes Nigeria-breve, er, at afsenderne oprindeligt udgav sig for at være nigerianske embedsmænd. Nigeria-breve kaldes i øvrigt også 419-svindel (419-scam) efter paragraf 419 i den nigerianske straffelov, der forbyder sådanne bedragerier.

I en undersøgelse foretaget af Microsoft (Herley, 2012) spørges: "Why do Nigerian scammers say they are from Nigeria?" Med en mere professionelt udseende e-mail ville svindlerne formentlig modtage langt flere svar. På den anden side betyder flere svar også mere arbejde. Ved at holde indholdet på et amatøragtigt niveau er man sikker på kun at fange de mest naive, der formentlig vil være mest tilbøjelige til at overføre penge.

7.2 Datingbedrageri

En nyere variant af forskudsbedrageri er datingbedrageri. Datingbedrageri opstår typisk som følge af en chatkontakt. Offer og gerningsperson indleder et virtuelt forhold, og offeret lokkes til at overføre penge til den andens fattige familie eller til rejseudgifter (med det formål at kunne møde hinanden i virkeligheden). Efterfølgende viser der sig at være tale om rent bedrageri.

I skrivende stund (23. marts 2015) finder man på Udenrigsministeriets hjemmeside følgende advarsel om Rusland (http://rusland.um.dk/da/rejse-og-ophold/internetsvindel/):

> *Pas på internetsvindel, særligt ved online dating*.
> Chat og dating via internettet er i dag meget udbredt. Det betyder større bekendtskabskredse for alverdens folk. Desværre betyder det også større risiko for at blive snydt og bedraget. Foranlediget af en række beklagelige episoder, hvor personer via internettet har forsøgt at franarre danskere penge, ser ambassaden sig nødsaget til at udsende følgende advarsel:
> Såfremt De har etableret kontakt med en russisk kvinde eller mand via internettet, ikke har truffet vedkommende og har mistanke om, at der er tale om svindel, kan det under ingen omstændigheder tilrådes at overføre penge til vedkommende.
> (…) Kontakt eventuelt ambassaden, som kan undersøge, om den pågældende person har søgt visum til Danmark. Ambassaden modtager gerne information fra danske statsborgere, der har været udsat for svindel af ovennævnte karakter.

Også på datingsites advares mod svindlere, specifikt fra Rusland, Østeuropa og Afrika. På nogle sites findes også en beskrivelse af, hvilke signaler man skal være opmærksom på i forbindelse med datingbedrageri, såsom professionelle fotos (modellignende), medlidenhedshistorier eller angivelse af et specielt erhverv: general, major, civilingeniør i olieindustrien, guldindustrien, smykkedesigner (mænd) og sygeplejerske eller modedesigner (kvinder).

Ligesom ved Nigeria-breve stopper bedragere som regel ikke efter første runde. I en artikel i Fyens Stiftstidende giver en politikommissær et eksempel på et typisk forløb: "Kvinden vil jo rigtigt gerne over til denne danske mand – der skal bare lige sendes nogle penge til flybilletter og så videre. Og så udvikler sagen sig med, at kvinden bliver involveret i et færdselsuheld og har brug for lægehjælp

og så videre – og lige pludseligt er det rigtigt mange penge, der er blevet sendt over på den anden side i det håb, at der kommer denne smukke, skønne kvinde over og besøger ham. Og det gør hun jo sjældent – eller det har jeg endnu ikke hørt, at hun nogensinde gør."
(http://www.fyens.dk/indland/Politiet-advarer-Svindel-og-humbug-i-stor-stil/artikel/2105964).

7.3 Omfanget af forskudsbedrageri

Som beskrevet i kapitel 1 er offerundersøgelsen gennemført som led i Danmarks Statistiks omnibusundersøgelser. Offerundersøgelsen er baseret på stikprøver blandt tilfældigt udvalgte danskere i alderen 16-74 år. 6.130 respondenter har i perioden august 2014 til og med januar 2015 fået stillet spørgsmål om forskudsbedrageri (se bilag 2). Af disse 6.130 respondenter angav tre personer, at de havde været udsat for forskudsbedrageri i løbet af de sidste 12 måneder.

Tre ud af 6.130 respondenter lyder som forsvindende få ofre, hvilket det også er set i forhold til andre typer af internetkriminalitet. Stikprøverne er repræsentative for befolkningen som helhed. Der kan dog være en skævhed i bortfaldet. For at teste, om der findes en sådan skævhed, udarbejder Danmarks Statistik vægte baseret på personoplysninger. Når disse vægte anvendes, har 2.108 danskere været udsat for forskudsbedrageri inden for de sidste 12 måneder. Statistisk usikkerhed gør, at dette tal kun er et estimat, men det viser, at forskudsbedrageri findes i Danmark, og det stemmer overens med mediehistorier og politiets erfaringer. Det viser imidlertid også, at forskudsbedrageri ikke er udbredt, hvilket tyder på, at de fleste potentielle danske ofre kan gennemskue fidusen.

7.4 Nærmere om forskudsbedrageri

De tre respondenter, der i offerundersøgelsen tilkendegav, at de havde været udsat for forskudsbedrageri, var alle mænd. En af episoderne hørte under kategorien Nigeria-breve (påstået arving til et ukendt familiemedlem), mens de to øvrige handlede om datingbedrageri. Ofrene var blevet kontaktet pr. e-mail (to gange) og gennem en hjemmeside (én gang). To af dem havde overført forholdsvis beskedne beløb (henholdsvis 1.000 og 1.100 kr.), mens det tredje offer gennemskuede svindelen, inden han overførte penge. Ingen af de tre har politianmeldt episoderne.

8 Afpresning

Afpresning på internettet kan rette sig mod virksomheder – fx ved trusler om et DDoS-angreb, der lammer en forretnings websalg – men her ser vi på afpresning af privatpersoner. Nærmere bestemt belyser undersøgelsen to former for internetafpresning: ransomware og sexafpresning.

8.1 Ransomware

Ransomware er en sammentrækning af ordene ransom (løsesum) og software. Ransomware er en type malware (se afsnit 2.3.2), der er i stand til at spærre en computer. Computerbrugeren får besked om at betale en løsesum for atter at få adgang til programmer og/eller data. Der findes mange forskellige varianter af ransomware. For nogle år tilbage florerede de såkaldte politi-ransomware. Her får brugeren at vide, at adgangen er spærret af politiet, fordi brugeren er blevet grebet i at bruge piratkopier eller børneporno. Effektiviteten af politi-ransomware forklares med en kombination af autoritetstro og frygten for, at andre tror, at der er noget om snakken (DKCERT Trendrapport 2012).

I en undersøgelse foretaget af Digitaliseringsstyrelsen og DKCERT (2015) er 1.111 personer i alderen 16-74 år blevet udspurgt om deres erfaringer med informationssikkerhed. Et af undersøgelsens emner var ransomware. Formuleringen af spørgsmålene er uoplyst, men vi må antage, at der er blevet spurgt om, hvorvidt respondenten har været udsat for ransomware (livstids prævalens). 8 procent af respondenterne havde været udsat for ransomware. Over halvdelen (56 procent) havde benyttet et sikkerhedsprogram til at få fornyet adgang til deres data og fjerne ransomware-programmet. 2 procent af ofrene havde betalt løsesummen. 22 procent havde fået deres data tilbage "på anden vis", mens 18 procent aldrig fik deres data tilbage (Digitaliseringsstyrelsen & DKCERT, 2015, s. 11).

8.2 Sexafpresning

Sexafpresning eller – på engelsk – sextortion (en sammentrækning af ordene sex og extortion) er formentlig en ny type afpresning. I hvert fald er den først for nylig blevet omtalt i medierne. Her anvendes erotiske eller intime billeder eller videofilm med ofrene til ren afpresning. Disse

billeder/videoer kan være afsendt frivilligt til afpresseren i den tro, at der blev chattet med en person med "rene" hensigter. I andre tilfælde stammer optagelsen fra et webcam. Der findes eksempler på, at offeret ikke har været klar over, at han eller hun er blevet filmet via webcam, men i de fleste afpresningssager lokkes offeret til at udføre seksuelle handlinger. For at undgå, at materialet bliver offentliggjort – til eksempelvis offerets Facebook-venner – skal offeret derefter indbetale penge til afpresseren.

Sexafpresning kan have voldsomme konsekvenser for ofrene. Ydmygelsen ved at få delt disse billeder eller videoer kan i yderste konsekvens føre til selvmord, således som man har set i de verdenskendte historier om skotske Daniel Perry og canadiske Amanda Todd.

8.3 Omfanget af afpresning

Som beskrevet i kapitel 1 er offerundersøgelsen gennemført som et led i Danmarks Statistiks omnibusundersøgelser. Offerundersøgelsen er baseret på stikprøver blandt tilfældigt udvalgte danskere i alderen 16-74 år. 6.130 respondenter har i perioden august 2014 til og med januar 2015 fået stillet spørgsmål om afpresning (se bilag 2). Af disse 6.130 respondenter angav syv personer, at de havde været udsat for afpresning (ransomware) i løbet af de sidste 12 måneder.

Syv ud af 6.130 respondenter er ikke ret mange i forhold til andre former for internetkriminalitet. Stikprøverne er repræsentative for befolkningen som helhed, men der kan dog være en skævhed i bortfaldet. For at teste, om der er tale om en sådan skævhed, udarbejder Danmarks Statistik vægte baseret på personoplysninger. Ifølge de vægtede data har 3.758 danskere været udsat for afpresning inden for de sidste 12 måneder. Statistisk usikkerhed gør, at dette tal kun er et estimat, men det understreger, at afpresning (ransomware) findes i Danmark, hvilket harmonerer med mediehistorier og politiets erfaringer.

Der er en iøjnefaldende forskel mellem Digitaliseringsstyrelsens og DKCERT's undersøgelse og offerundersøgelsen. Den første rapporterede om en offerrisiko i forbindelse med ransomware på hele 8 procent, mens offerundersøgelsen peger på kun 0,1 procent. Nu er de 8 procent (formentligt) en livstid prævalens, men derfra er der stadig langt til de 0,1 procent i offerundersøgelsen. En af forklaringerne kan være registreringseffekter, altså at spørgsmålene er formuleret forskelligt. Det er dog svært at tro, at dette skulle resultere i en så stor forskel. En anden forklaring kan være, at fænomenet ransomware har toppet, og at der i 2014 ikke fandtes ret mange nye ofre. Denne forklaring stemmer overens med de oplysninger, jeg fik under en samtale med en ansat ved politiets Nationale Cyber Crime Center, NC3.

Sexafpresning så vi slet ikke i offerundersøgelsen. Det er et klart tegn på, at fænomenet ikke er ret udbredt i Danmark. Det stemmer til dels overens med det billede, politiet tegner i medierne. Til DR Nyhederne oplyste NC3, at "… der i Asien og andre steder i Europa faktisk har været rigtig, rigtig mange sager. Så mon ikke der også er en del sager herhjemme, som vi blot ikke hører noget om (…) Der er selvfølgelig nogle gange nogle, der falder i. Men jeg tror ikke, at vi vil få et kæmpe boom." (http://www.dr.dk/Nyheder/Indland/2015/01/15/114205.htm). Offerundersøgelsen peger i hvert fald ikke i denne retning.

8.4 Nærmere om afpresning

Blandt de 6.130 respondenter i stikprøverne havde fire mænd og tre kvinder været udsat for afpresning i forbindelse med ransomware. Det er bemærkelsesværdigt, at fem af de udsatte respondenter er i tresserne, mens én er i halvtresserne og en anden er fyldt halvfjerds. Ofrene er med andre ord ældre danskere. Ingen af de udsatte har betalt afpresseren. Én af de syv respondenter har anmeldt sagen til politiet.

Litteratur

Boesen Pedersen, Anne-Julie, Britta Kyvsgaard & Flemming Balvig (2014) Udsathed for vold og andre former for kriminalitet 2005-2013. Københavns Universitet, Justitsministeriet, Det Kriminalpræventive Råd, Rigspolitiet.

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

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

Danmarks Statistik, IT-anvendelse i befolkning, adskillige årgange.

Digitaliseringsstyrelsen & DKCERT (2015). Borgernes informationssikkerhed 2014.

DKCERT, Trendrapport, adskillige årgange.

European Central Bank (2014). Third report on card fraud.

Europol, Organised Crime Threat Assessment (OCTA), adskillige årgange.

Europol (2012). Identity Theft: Do's and Don'ts.

FDIH, Dansk e-handelsanalyse, adskillige årgange.

Herley, Cormac (2012). Why do Nigerian scammers say they are from Nigeria? Microsoft.com.

Jewkes, Y. & M. Yar (eds.) (2010) Handbook of Internet Crime. 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.

Konkurrence- og Forbrugerstyrelsen (2014). Betalingskortmarkedet 2014.

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

Kruize, Peter (2013). Kriminalitet i en digitaliseret verden. Københavns Universitet: Det Juridiske Fakultet.

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: Crimnal 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.

Meyer, Christian (2015). Nedgang i ID-tyverier. Norsk senter for informasjonssikring.

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.

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.

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

Undersøgelsens metode

Bilag 1

Offerundersøgelser er det vigtigste datagrundlag for denne rapport. Der har været tre undersøgelser i henholdsvis 2009, 2013 og 2014. Spørgeskemaerne for de tre undersøgelser har ikke været identiske, men de er dog sammenlignelige. Denne påstand uddybbes i dette bilag. Ellers beskrives her de almene begrænsninger af offerundersøgelser som dataindsamlingsmetode.

Filterspørgsmål i de tre offerundersøgelser

Sammenlignelighed mellem de tre undersøgelser er i høj grad afhængig af, hvordan respondenterne er blevet spurgt, om de har været udsat for forskellige former for internetkriminalitet. I 2009-undersøgelsen lød dette spørgsmål:

> Har du inden for de seneste 12 måneder været udsat for misbrug af personoplysninger eller identitetsbeviser?

I 2013-undersøgelsen var spørgsmålet om identitetstyveri identisk med spørgsmålet i 2009. Undersøgelsen i 2013 omfattede dog også handelsbedrageri, og spørgsmålet i forbindelse hermed lød som følgende:

> Har du inden for de seneste 12 måneder været udsat for bedrageri ved køb eller salg af varer/ydelser over internettet?

I 2014 kom der yderligere emner til undersøgelsen – forskudsbedrageri og afpresning – og der var et ønske om at opdele identitetstyveri i misbrug af identitetsoplysninger, misbrug af betalingskort-oplysninger og chikane. Undersøgelsen ville blive for dyr, hvis alle disse emner skulle dækkes separat, og der er derfor introduceret et filterspørgsmål til at selektere alle relevante rspondenter. Dette spørgsmål lød som følgende:

> Har du inden for de seneste 12 måneder personligt, som privatperson, været udsat for identitetstyveri eller en form for internetkriminalitet?
>
> Ved identitetstyveri forstås, at en anden person har anvendt dine personoplysninger (fx navn, CPR-nr., mailkonto) eller identitetsbeviser (fx kørekort, sygesikringsbevis) uden din tilladelse for at opnå en økonomisk gevinst. Identitetstyveri kan både ske på internettet og i den 'reelle' verden.
>
> Ved internetkriminalitet forstås, at dine betalingskortoplysninger er blevet misbrugt til at købe varer/ydelser på nettet, at du er blevet udsat for chikane på internettet (fx har nogen misbrugt din mailadresse eller din profil på Facebook), at du har været udsat for bedrageri ved køb eller salg af varer/ydelser på internettet, at du over internettet er blevet lokket til at

sende penge til en person, som viste sig at være en bedrager (fx via et datingsite eller Facebook), eller at du er blevet afpresset over internettet (fx med trusler om at dine computerdata vil blive slettet eller at personfølsomme oplysninger vil blive offentliggjort).

Forskellen mellem undersøgelserne i 2009/2013 og 2014 er, at spørgsmålene i 2014 er mere præcise. Det bliver gjort mere klart, hvornår man falder inden for den kategori, der spørges til. Det er svært at sige, om denne ændring i spørgeteknik har haft væsentlig betydning for respondenternes svar, men her forsøges at redegøre for det.

Spørgsmålet om identitetsmisbrug (tyveri) er mere eller mindre identisk. I 2009/2013 beskrives det som misbrug af identitetsoplysninger og identitetsbeviser. De samme begreber anvendes i 2014, men her gøres det klart, at misbrug af betalingskortoplysninger og chikane er kategorier for sig selv. Resultaterne fra 2014-undersøgelsen giver ikke anledning til at tro, at identitetsmisbrug eller chikane er blevet opfattet forskelligt i 2009/2013 i forhold til 2014.

Spørgsmålet er, om misbrug af betalingskortoplysninger er blevet opfattet forskelligt i de forskellige undersøgelser. I 2009/2013 nævnes misbrug af betalingskortoplysninger ikke som en selvstændig kategori i modsætning til 2014-undersøgelsen. Resultaterne fra 2014 viser også en markant vækst i antallet af udsatte personer for betalingskortbedrageri. Det kunne tyde på, at den særskilte kategori i 2014 har ført til, at flere respondenter siger 'ja' til betalingskortmisbrug i forhold til 2009/2013. Modargumentet er, at andre kilder – analyser fra Konkurrence- og Forbrugerstyrelsen – også peger i retning af en markant vækst i betalingskortmisbrug på nettet. Konklusionen i forhold til misbrug af betalingskortoplysninger må sandsynligvis være, at der muligvis er en begrænset registreringseffekt på grund af en ændring i spørgsmålet, men at den markante stigning må anses som reel.

Ordlyden af spørgsmålet om handelsbedrageri – udsat for bedrageri ved køb eller salg af varer/ydelser over internettet – er identisk i 2013 og 2014. Dermed er der ingen grund til at antage, at det skulle føre til registreringseffekter på grund af spørgeteknikken. Samtidig viser resultaterne fra 2014 et meget markant fald i antal udsatte for handelsbedrageri. Er dette fald reelt, eller kan der være andre forklaringer? Kan det være, at en del af respondenterne er blevet byttet rundt fra handelsbedrageri til betalingskortbedrageri i 2014-undersøgelsen? Ved internethandel anvendes betalingskort ofte som betalingsmiddel.

Når en respondent i 2014-undersøgelsen har svaret 'ja' til filterspørgsmålet, bliver misbrug af betalingskortoplysninger på internettet beskrevet som: "at en anden person har anvendt dit Dankort eller andet betalingskort, uden din tilladelse, til at købe en vare/ydelse på internettet". Handels-bedrageri er forelagt respondenterne i to, separate, spørgsmål: (1) bedrageri ved køb af varer/ydelser over internettet (at du ikke har modtaget det, du har betalt for, eller at den leverede vare viste sig at være en kopivare) og (2) bedrageri ved salg af varer/ydelser over internettet (at du har solgt og leveret en vare/ydelse, men ikke har modtaget betaling). Der er ikke meget tvivl om, at spørgsmålene i 2014-undersøgelsen er præcise og retvisende.

I 2013-undersøgelsen var spørgsmålet som sagt, om respondenten inden for de seneste 12 måneder havde været udsat for bedrageri ved køb eller salg af varer/ydelser over internettet. Det næste spørgsmål gik ud på, hvilken form for bedrageri respondenten havde været udsat for. Svarmulighederne for dette spørgsmål var: (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 og (4) solgt varer/ydelser til en privat person, men har aldrig modtaget betaling. Hvis en respondent havde været udsat for misbrug af betalingskortoplysninger, ville vedkommende ikke kunne svare på dette uddybende spørgsmål. I alt besvarer 224 af de 233 respondenter, der har været udsat for handelsbedrageri på dette spørgsmål med en af de fire svarmuligheder. Kun ni svarer 'ved ikke'.

Det næste uddybende spørgsmål i 2013-undersøgelsen var, hvad for en vare eller ydelse respondenten ville købe eller sælge. Dette var stillet som et åbent spørgsmål. Svarene afspejler alle mulige slags varer, men seks svar indikerer, at det handler om betalingskortmisbrug og ikke handelsbedrageri. Disse seks svar er: 'en anden person har brugt mit Dankort', 'credit card fraud', 'cyberkriminalitet', 'kortmisbrug', 'kreditkortdata blev hacket' og 'misbrug af Mastercard'. Udover det, er der en respondent, der oplyser 'telefonopringning af mit software ikke var optimal, og at de ville løse problemet ved at installere nyt program over nettet og derved fik de adgang til min bankkonto', som heller ikke hører hjemme under handelsbedrageri.

Konklusionen i forhold til, at der eventuelt skulle være byttet rundt på handelsbedrageri og betalingskortbedrageri i 2014 i sammenligning med 2013 er, at det er sket i meget begrænset omfang. Der er mindst seks tilfælde af fejlrubricering i 2013 ved handelsbedrageri, hvilket svarer til 2,6 procent af de 233 respondenter, der har været udsat for handelsbedrageri, og maksimalt 15 (seks plus de ni 'ved ikke' besvarelser ved type bedrageri), hvilket svarer til 6,4 procent af de 233 respondenter, der har været udsat for handelsbedrageri.

Almene begrænsninger af offerundersøgelser

Dette afsnit tager udgangspunkt i beskrivelsen af begrænsninger af offerundersøgelser i rapporten Udsathed for vold og andre former for kriminalitet (Boesen Pedersen, Kyvsgaard & Balvig, 2014, s. 13-14). Der nævnes følgende punkter:

- Det er befolkningens oplevelse, der aflæses og denne oplevelse er ikke nødvendigvis i overensstemmelse med den juridiske afgrænsning af kriminalitet. Konsekvensen heraf er blandt andet, at forskellige måder at spørge og formulere spørgsmålene på udløser forskellige svar og giver forskellige hyppigheder. Man må derfor være særdeles opmærksom på den anvendte spørgsmålsformulering og på, at konstaterede forskelle mellem selv

ensartet gennemførte undersøgelser over tid kan bero på ændrede opfattelser af, hvad former for kriminalitet er.

- Det er aldrig hele befolkningen, der udspørges. Der er fx altid en nedre aldersgrænse og ofte også en øvre. Den nedre aldersgrænse betyder typisk, at undersøgelser kun i ringe grad eller slet ikke kommer til at omfatte kriminalitet mod (mindre) børn.

- Det er næsten aldrig hele den afgrænsede del af befolkningen, undersøgelsen omfatter, der udspørges. Det er så godt som altid et (meget) mindre udsnit. Dette betyder, at tallene er forbundet med den såkaldte stikprøveusikkerhed. Størrelsen af denne kan under visse forudsætninger og omstændigheder beregnes.

- Nogle af de former for kriminalitet, der spørges om, er relativt sjældne hændelser. Det betyder, at stikprøveudvalget helst skal være meget stort for nærmere at kunne analysere de hændelser, der berettes om. Med stigende udvalgsstørrelse øges imidlertid også omkostningerne og andre praktiske problemer med at gennemføre undersøgelsen, således at det kan være svært at realisere det undersøgelsesmæssigt mest ideelle.

- Der er forskellige måder at finde frem til dem, man vil interviewe, på. Disse måder har hver deres fordele og ulemper. En af mulighederne er et fuldstændigt tilfældigt udvalg (lodtrækningsprincip) baseret på CPR-registret.

- Det lykkes aldrig at få besvarelser fra alle, der er med i det endelige udvalg. Der er nogen, det ikke lykkes at træffe, og andre, der ikke ønsker at deltage. Der er en betydelig risiko for, at de, man ikke får med, udgør et skævt udsnit af alle, og at tallene derfor forvrides i den ene eller den anden retning. Dette kompenseres der dog i hvert fald i nogen grad for ved vægtning af besvarelserne.

- Der er forskellige måder at udspørge på. De fire standardmetoder er det personlige interview, telefoninterviewet, postspørgeskemaet og internetspørgeskemaet. Hver af disse metoder har deres fordele og ulemper, fx med hensyn til svarvillighed og mulige hukommelsesproblemer (se de følgende punkter).

- Der kan være et problem med svarvillighed. Der kan være nogen, der ikke ønsker at berette i et spørgeskema eller over for en interviewer om den kriminalitet, de har været udsat for. Denne svarvillighed kan tænkes at variere med forskellige omstændigheder ved kriminaliteten. Fx kan der være grund til at tro, at svaruvillighed er et større problem ved kortlægning af sexafpresning end ved kortlægning af handelsbedrageri.

- Der kan være hukommelsesproblemer. Også kriminalitet glemmes i en eller anden udstrækning, igen formentlig afhængig af dens karakter, tid siden hændelsen, og hvem man i øvrigt er m.v. Hukommelsesfaktorens indvirkning på undersøgelsens resultater kan begrænses ved alene at spørge om hændelser inden for en forholdsvis kort periode forud for interviewet.

- Ved introduktion af en afgrænset tidsperiode, hvori kriminaliteten søges kortlagt, introduceres det såkaldte teleskoperingsproblem, dvs. at man ganske vist husker selve hændelsen, men fejlhusker tidspunktet. Man taler om fremadteleskopering for de tilfælde, som reelt er sket forud for tidsperioden, og bagudteleskopering for de tilfælde, man ikke beretter om, fordi man fejlagtigt tidsmæssigt placerer dem uden for tidsperioden. Problemet er, at bagudteleskopering og fremadteleskopering ikke nødvendigvis går lige op i sidste ende, hverken antalsmæssigt eller med hensyn til type af hændelse (fx med hensyn til alvorlighed, anmeldelse/ikke-anmeldelse m.v.).

- Der er forskel på ofre (personer) og episoder (handlinger). Mennesker risikerer at blive udsat for kriminalitet mere end én gang inden for den tidsperiode, der spørges til. Offerundersøgelserne er ikke altid velegnede til at udsige noget om alle de episoder, der har fundet sted, idet det forudsætter, at de udspurgte spørges detaljeret om hver hændelse (fx om anmeldelse, ikke-anmeldelse).

- Der kan endelig også opstå fejl i forbindelse med registrering af svar, databehandling m.v

Spørgeskema offerundersøgelse

Bilag 2

1. Har du *inden for de seneste 12 måneder* personligt, som privatperson, været udsat for **identitets-tyveri** eller en form for **internetkriminalitet**?

   Ved **identitetstyveri** forstås, at en anden person har anvendt dine personoplysninger (fx navn, CPR-nr., mailkonto) eller identitetsbeviser (fx kørekort, sygesikringsbevis) uden din tilladelse for at opnå en økonomisk gevinst. Identitetstyveri kan både ske på internettet og i den 'reelle' verden.

   Ved **internetkriminalitet** forstås, at dine betalingskortoplysninger er blevet misbrugt til at købe varer/ydelser på nettet, at du er blevet udsat for chikane på internettet (fx har nogen misbrugt din mailadresse eller din profil på Facebook), at du har været udsat for bedrageri ved køb eller salg af varer/ydelser på internettet, at du over internettet er blevet lokket til at sende penge til en person, som viste sig at være en bedrager (fx via et datingsite eller Facebook), eller at du er blevet afpresset over internettet (fx med trusler om at dine computerdata vil blive slettet eller at personfølsomme oplysninger vil blive offentliggjort).

   O Ja (til spørgsmål 2)
   O Nej (slut)

2. Har du *inden for de seneste 12 måneder* været udsat for:

   a) **misbrug af dine personoplysninger/identitetsbeviser**, det vil sige, at en anden person har anvendt dine personoplysninger (fx navn, cpr-nr. eller mailkonto) eller identitetsbeviser (fx kørekort eller sygesikringsbevis) uden din tilladelse, og derved opnåede en økonomisk gevinst. Fx ved at bestille varer/ydelser på nettet, ved at oprette abonnementer i dit navn, ved at leje en bil i dit navn, ved at din mailkonto er blevet brugt til at sende beskeder til din adressebog med besked om, at du har brug for en pengeoverførelse via fx Western Union. Misbrug af betalingskortoplysninger hører ikke under betegnelsen identitetstyveri. Misbrug af personoplysninger med det formål at chikanere dig hører heller ikke under betegnelsen identitetstyveri.

      O Ja (besvarer spørgsmål 3-14)
      O Nej

   b) **misbrug af dine betalingskortoplysninger på internettet**, det vil sige, at en anden person har anvendt dit Dankort eller andet betalingskort, uden din tilladelse, til at købe en vare/ydelse på internettet.

      O Ja (besvarer spørgsmål 15-20)
      O Nej

c) **chikane på internettet**, det vil sige, at en eller flere personer har brugt internettet til at chikanere dig. Fx ved at skrive negative beskeder om dig på sociale medier, at sende beskeder fra din mailkonto, chatte i dit navn eller ændringer på din Facebook profil uden tilladelse.

O Ja (besvarer spørgsmål 21-26)
O Nej

d) **bedrageri ved køb af varer/ydelser over internettet**, det vil sige, at du ikke har modtaget, det du har betalt for, eller at den leverede vare viste sig at være en kopivare.

O Ja (besvarer spørgsmål 27-31)
O Nej

e) **bedrageri ved salg af varer/ydelser over internettet**, det vil sige, at du har solgt og leveret en vare/ydelse, men har ikke modtaget betaling.

O Ja (besvarer spørgsmål 32-35)
O Nej

f) **forskudsbedrageri på internettet**, det vil sige, at du har betalt et pengebeløb i forskud for at modtage et større beløb (fx arv fra et ukendt familiemedlem, lotterigevinst, glemte konti), eller at du har betalt penge til en person, som du har mødt på en datingsite (fx penge til rejseudgifter), som efterfølgende viste sig at være en bedrager.

O Ja (besvarer spørgsmål 36-40)
O Nej

g) **afpresning på internettet**, det vil sige, at du er blevet afpresset til at overføre penge, fx fordi du er blevet truet, med at dine computerdata vil blive slettet, din computer ikke ville forblive låset (ransomware), eller at følsomme oplysninger om dig ville blive offentliggjort på internettet (fx webcam optagelser).

O Ja (besvarer spørgsmål 41-44)
O Nej

A. Misbrug af dine personoplysninger/identitetsbeviser

Hvis du har oplevet det flere gange inden for de seneste 12 måneder, besvares spørgsmål i forbindelse med den sidste begivenhed.

3. Blev dine personoplysninger og/eller identitetsbeviser misbrugt?
    a) Kun personoplysninger
    b) Kun identitetsbeviser (*til spørgsmål 5*)
    c) Både personoplysninger og identitetsbeviser
    d) Ved jeg ikke (*til spørgsmål 6*)

4. Hvilke personoplysninger blev misbrugt?
   (*Flere svar muligt*)
   a) Navn
   b) CPR-nummer
   c) Postadresse
   d) Nem-ID
   e) Brugernavn og password til e-mail og/eller sociale medier
   f) Bankoplysninger (konto-nummer, adgangskode osv.)
   g) Andet. Angiv venligst

5. Hvilke identitetsbeviser blev misbrugt?
   (*Flere svar muligt*)
   a) Pas
   b) Sygesikringsbevis
   c) Kørekort
   d) Andre identitetsbeviser. Angiv venligst

6. Til hvilket formål misbrugte gerningspersonen dine personoplysninger eller identitetsbeviser?
   (*Flere svar muligt*)
   a) At købe varer/ydelser på nettet på kredit
   b) At overføre penge fra min konto til en anden konto
   c) At leje noget (fx en bil) i mit navn
   d) At oprette/ændre et abonnement (fx abonnement på mobiltelefon)
   e) At lokke andre til at overføre penge til mig (fx 'strandet i udlandet' e-mails)
   f) Andet. Angiv venligst

7. Hvordan opdagede du, at dine oplysninger blev misbrugt?
   a) Gennem udskrifter (på papir eller netbank)
   b) Regning/opkrævning fra en virksomhed for en vare/ydelse
   c) Blev kontaktet af en tredjeperson (fx venner, familie, bank)
   d) Andet. Angiv venligst

8. Har du en idé om, hvordan gerningspersonen har fået fat i dine identitetsoplysninger?
   a) Nej (*til spørgsmål 10*)
   b) Jeg har en formodning
   c) Ja

9. Hvordan (tror du) har gerningspersonen fået fat i dine identitetsoplysninger?
   a) En/flere af mine identitetsbeviser er blevet stjålet (indbrud, tricktyveri, røveri, lommetyveri mm)
   b) Jeg har oplyst identitetsoplysninger gennem en falsk e-mail (phishing)
   c) Jeg har oplyst identitetsoplysninger gennem en falsk hjemmeside (pharming)
   d) Min computer er blevet udsat for hacking/spyware
   e) Ved at handle på internettet (internetbutik mm)
   f) Andet. Angiv venligst

10. Har du en idé om, hvem der har misbrugt dine personoplysninger/identitetsbeviser?
    a) Nej (*til spørgsmål 12*)
    b) Jeg har en formodning
    c) Ja

11. Hvem (tror du) har misbrugt dine oplysninger?
    a) Partner
    b) Ekspartner
    c) Familiemedlem
    d) Nabo/ven
    e) En fra mit arbejde
    f) Anden bekendte
    g) En som jeg ikke kender personligt

12. Hvor stort et beløb er der blevet trukket fra din konto eller opkrævet pga. misbrug af personoplysninger/identitetsbeviser?
    Angiv beløb i danske kroner

13. Hvor stor en del af dette beløb, har du selv betalt? (Fx hvis banken eller dit forsikringsselskab kun har dækket noget af beløbet?)
    Angiv beløb i danske kroner

14. Har du anmeldt misbruget til politiet?
    a) Nej
    b) Ja, men politiet afviste anmeldelsen
    c) Ja, og politiet optog anmeldelsen

B. Misbrug af dine betalingskortoplysninger på nettet

Hvis du har oplevet det flere gange inden for de seneste 12 måneder, bedes du besvare spørgsmålet i forbindelse med den seneste begivenhed.

15. Hvordan opdagede du, at dit betalingskort blev misbrugt?
    a) Betalingskortet blev spærret af Nets/banken
    b) Gennem udskrifter (på papir eller netbank)
    c) Andet. Angiv venligst

16. Har du en idé om, hvordan gerningspersonen har fået fat i dine betalingskortoplysninger?
    a) Nej (*til spørgsmål 18*)
    b) Jeg har en formodning
    c) Ja

17. Hvordan (tror du) har gerningspersonen fået fat i dine betalingskortoplysninger?
    a) Jeg har oplyst dem gennem en falsk e-mail (phishing)
    b) Jeg har oplyst dem gennem en falsk hjemmeside (pharming)
    c) Min computer er blevet udsat for hacking/spyware
    d) Ved at handle på internettet (Fx i en internetbutik)
    e) Ved afluring/kopiering (skimming)
    f) Kortet er blevet stjålet (indbrud, tricktyveri, røveri, lommetyveri osv.)
    g) Andet. Angiv venligst

18. Hvilket beløb blev der trukket fra dit kort, før det blev spærret?
    Angiv beløb i danske kroner

19. Hvor stor en del af dette beløb, har du selv betalt? (Fx hvis din bank eller kreditkortselskab kun har dækket noget af beløbet?)
    Angiv beløb i danske kroner

20. Har du anmeldt kortmisbruget til politiet?
    a) Nej
    b) Nej, det gjorde banken/kreditkortselskabet
    c) Ja, men politiet afviste anmeldelsen
    d) Ja, og politiet optog anmeldelsen

C. Chikane på internettet

Hvis du har oplevet det flere gange inden for de seneste 12 måneder, besvares spørgsmål i forbindelse med den sidste begivenhed.

21. Hvordan blev du chikaneret på internettet?
    (*Flere svar muligt*)
    a) Modtog uønskede mails (ikke spammail, men rettet mod din person)
    b) E-mails blev mod min vilje udsendt i mit navn
    c) Der blev chattet på internettet i mit navn mod min vilje
    d) Der blev spredt pinlige billeder, rygter eller historier af/om mig på internettet
    e) Der blev gennemført ændringer mod min vilje på personlige sider, eksempelvis sociale medier, websider, blogs
    f) Andet. Angiv venligst

22. I hvor lang tid forgik chikanen?
    a) Op til en uge
    b) Op til en måned
    c) 1-2 måneder
    d) 3-6 måneder
    e) 7-12 måneder
    f) Mere end et år
    g) Er stadig ikke afsluttet

23. Hvem stod bag chikanen?
    a) Partner
    b) Ekspartner
    c) Familiemedlem
    d) Nabo/ven
    e) En fra mit arbejde
    f) Anden bekendt
    g) Nogen jeg ikke kender personligt
    h) Ved ikke

24. Ved du – eller har du en idé om – hvorfor du blev chikaneret?
    a) Nej (*til spørgsmål 26*)
    b) Jeg har en formodning
    c) Ja

25. Hvorfor (tror du) blev du chikaneret?
    a) Med henblik på at fortsætte/genoprette et forhold
    b) At indlede et forhold/få min opmærksomhed
    c) For at kontrollere dig
    d) For at få hævn
    e) For at skræmme dig
    f) For at påvirke dit arbejde
    g) Fordi personen er ude af kontrol (psykisk syge, alkohol, piller m.m.)
    h) Andet. Angiv venligst
    i) Ved ikke

26. Har du anmeldt chikanen til politiet?
    a) Nej
    b) Ja, men politiet afviste anmeldelse
    c) Ja, og politiet optog anmeldelsen

D. Bedrageri ved køb af varer/ydelser over internettet

Hvis du har oplevet det flere gange inden for de seneste 12 måneder, besvares spørgsmål i forbindelse med den sidste begivenhed.

27. Hvad for en vare/ydelse ville du købe? (*valg en kategori*)
    a) Tøj, sko og smykker
    b) Kosmetik, medicin og kosttilskud
    c) IT, tele og foto
    d) Bolig, have og blomster
    e) Sports- og fritidsudstyr
    f) Auto-, båd- og cykeludstyr
    g) Film, musik, bøger, spil og legetøj
    h) Rejser og kulturoplevelser

i) Elektronik og hvidevarer
j) Andet. Angiv venligst

28. Har du købt denne vare/ydelse ved en internetbutik eller en privatperson?
    a) Internetbutik: dansk
    b) Internetbutik: udenlandsk
    c) Internetbutik: ukendt om det er dansk eller udenlandsk
    d) Privatperson: Den Blå Avis (dba.dk)
    e) Privatperson: anden webside
    f) Privatperson: Facebook
    g) Privatperson: andre sociale medier

29. For hvilket beløb er du blevet bedraget?
    Angiv beløb i danske kroner

30. Hvor stor en del af dette beløb, har du selv betalt? (Fx hvis bank eller kreditkortselskab kun har dækket noget af beløbet?)
    Angiv beløb i danske kroner

31. Har du anmeldt bedrageriet til politiet?
    a) Nej
    b) Nej, det gjorde banken/kreditkortselskabet
    c) Ja, men politiet afviste anmeldelsen
    d) Ja, og politiet optog anmeldelsen

E. Bedrageri ved salg af varer/ydelser over internettet

Hvis du har oplevet det flere gange inden for de seneste 12 måneder, besvares spørgsmål i forbindelse med den sidste begivenhed.

32. Hvad for en vare/ydelse ville du sælge? (*valg en kategori*)
    a) Tøj, sko og smykker
    b) Kosmetik, medicin og kosttilskud
    c) IT, tele og foto
    d) Bolig, have og blomster
    e) Sports- og fritidsudstyr
    f) Auto-, båd- og cykeludstyr
    g) Film, musik, bøger, spil og legetøj
    h) Rejser og kulturoplevelser
    i) Elektronik og hvidevarer
    j) Andet. Angiv venligst

33. Hvordan har du sat denne vare/ydelse til salg?
    a) På Den Blå Avis (dba.dk)
    b) Anden webside
    c) Facebook
    d) Andre sociale medier. Angiv venligst

34. For hvilket beløb er du blevet bedraget?
    Angiv beløb i danske kroner

35. Har du anmeldt bedrageriet til politiet?
    a) Nej
    b) Ja, men politiet afviste anmeldelsen
    c) Ja, og politiet optog anmeldelsen

F. Forskudsbedrageri på internettet

Hvis du har oplevet det flere gange inden for de seneste 12 måneder, besvares spørgsmål i forbindelse med den sidste begivenhed.

36. Hvilket slags forskudsbedrageri er du blevet udsat for?
    a) Jeg havde vundet et lotteri
    b) Jeg var arving til et ukendt familiemedlem
    c) Jeg blev bedt om at hjælpe med at overføre penge fra fx Nigeria ved at stille min bankkonto til rådighed
    d) Ved at betale udgifter for en internetdate (fx rejseudgifter)
    e) Andet. Angiv venligst

37. Hvordan blev du kontaktet af bedrageren?
    a) Via e-mail
    b) Sociale medier
    c) Andet. Angiv venligst

38. Hvor mange gange overførte du penge, før du opdagede, at der var tale om bedrageri?
    Angiv antal gange

39. For hvilket beløb er du blevet bedraget?
    Angiv beløb i danske kroner

40. Har du anmeldt bedrageriet til politiet?
    a) Nej
    b) Ja, men politiet afviste anmeldelsen
    c) Ja, og politiet optog anmeldelsen

G. Afpresning/trusler på nettet

Hvis du har oplevet det flere gange inden for de seneste 12 måneder, besvares spørgsmål i forbindelse med den sidste begivenhed.

41. Hvordan blev du afpresset på nettet?
    a) Min computer var låst (ransomware)
    b) Mine computerdata ville blive slettet
    c) Min hjemmeside ville blive nedlagt/ændret
    d) Kompromitterende (stødende) billeder af mig ville blive offentliggjort
    e) Andet. Angiv venligst

42. Har du udbetalt penge en eller flere gange til den/dem, der afpressede dig?
    a) Ja, en enkelt gang
    b) Ja, flere gange
    c) Nej (*til spørgsmål 43*)

43. Hvor stort et beløb har du i alt betalt til personen, der afpressede dig?
    Angiv beløb i danske kroner

44. Har du anmeldt afpresningen til politiet?
    a) Nej
    b) Ja, men politiet afviste anmeldelsen
    c) Ja, og politiet optog anmeldelsen