Peter Kruize, Det Juridiske Fakultet, Københavns Universitet

INTERNET-KRIMINALITET 2017

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

Denne undersøgelse er støttet økonomisk af Det Kriminalpræventive Råd.
Undersøgelsens udførelse, indhold og resultater er alene forfatternes ansvar. De vurderinger og synspunkter, der fremgår af materialet, er forfatternes egne og deles ikke nødvendigvis af Det Kriminalpræventive Råd.

Denne publikation er kun udgivet som PDF på dkr.dk

Maj 2018

DKR.nr: 17-221-0167

ISBN 978-87-92966-49-0

Forord

Det er nu fjerde gang, jeg udgiver en rapport om internetrelateret kriminalitet i Danmark. Den første rapport udkom i 2009 og handlede om identitetstyveri. Den næste fik titlen "Kriminalitet i en digitaliseret verden" og så dagens lys i 2013, mens den tredje rapport – "Internetkriminalitet 2014" – udkom i 2015. Den her foreliggende udgave er en opdatering af rapporten fra 2015. Dermed er der så småt ved at blive opbygget historiske data om internetrelateret kriminalitet og skabt større indsigt i dennes udvikling.

En vigtig del af de spørgsmål, der ligger til grund for denne undersøgelse, er fra og med 2018 blevet inkorporeret i den brede offerundersøgelse, som udarbejdes af Justitsministeriets forskningskontor og vil blive publiceret i slutningen af 2019.

Undersøgelsen er finansieret af Det Kriminalpræventive Råd.

Jægerspris, den 6. marts 2018
Peter Kruize

Ordliste[1]

Computervirus er et program, som kan skade andre programmer. Virusprogrammer kan for eksempel slette vigtige data eller programfiler på den inficerede computer. En computervirus skal aktiveres manuelt, ved at brugeren for eksempel åbner en fil, som vedkommende har tillid til.

Datingbedrageri er, når en person indleder et virtuelt forhold, og vedkommende eksempelvis lokkes til at overføre penge til rejseudgifter med det formål, at vedkommende kan møde den person, han/hun dater, i virkeligheden. Senere viser det sig dog, at den person, som modtog pengene, er en bedrager, og at forholdet kun var indledt for at franarre offeret penge.

DDos-angreb er en betegnelse for en ondsindet metode til at overbelaste en hjemmeside, så den ikke virker. DDos-angreb udføres ved, at en person, som kontrollerer en masse computere, får dem alle til på én gang og i én uendelighed at forespørge den samme internetadresse med det resultat, at ingen andre kan komme i forbindelse med hjemmesiden. DDoS står for Distributed Denial of Service (distribueret servicenægtelse).

Forskudsbedrageri er, når offeret lokkes til at betale et beløb for at kunne modtage et eller andet ønskværdigt. Det kan for eksempel være Nigeriabreve, hvor det potentielle offer anmodes om et pengebeløb til gengæld for senere at modtage en stor arv fra en ukendt person. Det kan også være forudbetaling for at modtage en stor lotterigevinst fra et lotteri, man ikke har deltaget i. Der er også tale om forskudsbedrageri, hvis man lokkes til at overføre penge til en person, man dater i udlandet, men som i virkeligheden er en bedrager (se datingbedrageri). Ved forskudsbedrageri opnår man ikke det, man er blevet lovet, men mister i stedet de overførte penge.

Identitetstyveri er, når en persons identitetsoplysninger bliver misbrugt – typisk med henblik på, at gerningspersonen opnår en økonomisk gevinst. Identitetsmisbruget kan for eksempel bestå i, at der optages lån, købes ting eller oprettes abonnementer i offerets navn. De personlige oplysninger kan for eksempel være CPR-nummer, adgangskoder, sundhedsoplysninger eller andre følsomme persondata.

En **keylogger** er et program, der registrerer, hvad der skrives på tastaturet på en computer inficeret med keylogger programmet. Det bruges til at spionere mod brugeren af den inficerede computer oftest med henblik på at opsnappe passwords, kontonumre og andre følsomme oplysninger.

Malware er et skadeligt softwareprogram designet til at ødelægge eller skade data på computere inficeret med det pågældende program. Der findes mange forskellige typer af malware, der opererer på forskellige må- der. Eksempler er vira, orme, trojanske heste, keyloggers og ransomware.

Et **Nigeriabrev** er typisk en e-mail fra en ukendt person, som har til formål at få modtageren til at overføre et mindre beløb mod at vedkommende efterfølgende modtager en stor økonomisk genvist – enten i form af en lotterigevinst, en arv fra et ukendt familiemedlem, et godt forretningstilbud eller et

[1] Efter Ordbog i Når forbrydelser bliver digitale (DKR, 2016, s. 79-82)

større beløb som tak for, at man har hjulpet en person med eksempelvis at smugle guld eller kontanter ud af et afrikansk land. Svindlen består i, at offeret aldrig modtager den lovede gevinst, men derimod blot mister de penge, vedkommende har overført.

En **orm** minder om en computervirus, men til forskel fra en virus kan en orm sprede sig fra computer til computer automatisk. En orm skal dermed ikke aktiveres af en person for at kunne inficere en computer og skabe ødelæggelser og funktionsforstyrrelser.

Pharming er en metode til typisk at stjæle person- eller betalingskortoplysninger ved at oprette en falsk hjemmeside, som kan forveksles med ægte hjemmesider. Svindlere kan eksempelvis oprette en fupbutik, hvor den uvidende forbruger indtaster kreditkortoplysninger i forbindelse med et (falsk) køb.

Phishing er en metode, hvor svindlere forsøger at narre internetbrugere til at oplyse brugernavn, adgangskode, kreditkort- eller netbanksoplysninger med videre. Brugeren får tilsendt en e-mail, hvor afsenderen tilsyneladende er en virksomhed, som man generelt har tillid til, eksempelvis ens bank, SKAT, en fragtvirksomhed eller lignende. I mailen opfordres modtageren til at indsende oplysningerne per e-mail eller logge ind på en falsk internetside, der til forveksling ligner bankens eller SKATs rigtige hjemmeside.

Ransomware er en form for virus, der gør skade på den inficerede computer ved at kryptere og dermed spærre brugerens data. Herefter modtager offeret en meddelelse om, at vedkommende kun kan få sine data frigjort, hvis vedkommende betaler en løsesum (løsesum = ransom). Sexafpresning (sextortion) er når gerningspersonen har skaffet sig adgang til seksuelle billeder eller lignende af offeret, som bruges til at true offeret til enten at sende flere billeder eller til at betale et pengebeløb, hvis offeret vil undgå, at billederne offentliggøres.

Social engineering henviser til sager, hvor brugeren ved hjælp af falske e-mails, sms'er eller telefonopkald lokkes til at afgive eller indtaste oplysninger (id, password og nøglekortkoder) til it-kriminelle, som udgiver sig for at være eksempelvis et velrenommeret selskab, en myndighed eller en ven.

En **trojansk hest** er et skadeligt computerprogram (malware), der er gemt i et softwareprogram, som virker godartet, så offeret narres til at downloade programmet.

Oversigt og resumé

Hovedkonklusioner om identitetsmisbrug, betalingskortmisbrug, chikane, handelsbedrageri, forskudsbedrageri og afpresning i cyberspace

1. Alle undersøgte former for internetrelateret kriminalitet viser vækst i 2017 i forhold til 2014 (i modsætning til berigelseskriminalitet i den fysiske verden).
2. Anno 2017 er betalingskortmisbrug den dominerende form for internetrelateret berigelseskriminalitet.
3. Set over perioden 2009-2017 er antallet af ofre for identitetsmisbrug fordoblet. Offerrisikoen er således steget fra 0,46 % i 2009 til 0,90 % i 2017.
4. Hvad angår betalingskortmisbrug, er offerrisikoen i perioden 2009-2017 blevet tredoblet med en risiko på 0,8 % i 2009 mod 2,5 % i 2017.
5. Chikane var næsten ikke-eksisterende i 2009, mens offerrisikoen i 2017 er på 0,48 %.
6. Handelsbedrageri faldt fra 2013 til 2014 markant (fra 2,4 % til 0,5 %), men er i 2017 steget til 1,0 %.
7. Forskudsbedrageri og afpresning er stadig sjældne fænomener. Målingen fra 2017 viser imidlertid en noget hyppigere forekomst end i 2014.
8. Den sammenlagte risiko for at blive offer for internetrelateret kriminalitet er markant lavere for de 50-74-årige (3,8 %) end for aldersgrupperne 16-29 år (6,1 %) og 30-49 år (5,8 %). Dette skyldes hovedsagelig, at de 50-74-årige sjældnere udsættes for kort- og handelsbedrageri end de øvrige aldersgrupper.
9. Lidt over en tredjedel af sagerne (36 %) vedrørende internetrelateret kriminalitet bliver politianmeldt. Kortmisbrug anmeldes hyppigst (som regel af banken eller kortselskabet).
10. To ud af tre respondenter oplever risikoen for internetkriminalitet som meget grænseoverskridende. Denne følelse forstærkes med alderen og optræder gennemsnitligt noget hyppigere hos kvinder.

.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.

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, politianmeldelse og oplevelse.

Datagrundlag

For at få indblik i omfanget, tabet, offerprofilerne, oplevelsen og anmeldelsesraten benyttes en offerundersøgelse. De forskellige data er blevet indsamlet som led i Danmarks Statistiks omnibusundersøgelse i perioden juni – september og november – december 2017. Ca. 1.000 personer blev udspurgt hver måned, og man har dermed i alt haft kontakt med 5.996 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 har nogen misbrugt din mailadresse, din profil på Facebook eller delt mod din vilje krænkende billeder af dig), 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, oplevelse og politianmeldelse af sagen.

Hermed er den måde, hvorpå respondenterne er blevet udspurgt, identisk med spørgemåden fra 2014, men adskiller sig fra 2013-målingen. Alligevel kan resultaterne 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 (Finans Danmark), misbrug af Dankort (Nets og Nationalbanken) og misbrug af andre betalingskort (Konkurrence- og Forbrugerstyrelsen og Nationalbanken).

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 identitetsmisbrug. 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 personoplysninger med henblik på chikane af offeret.

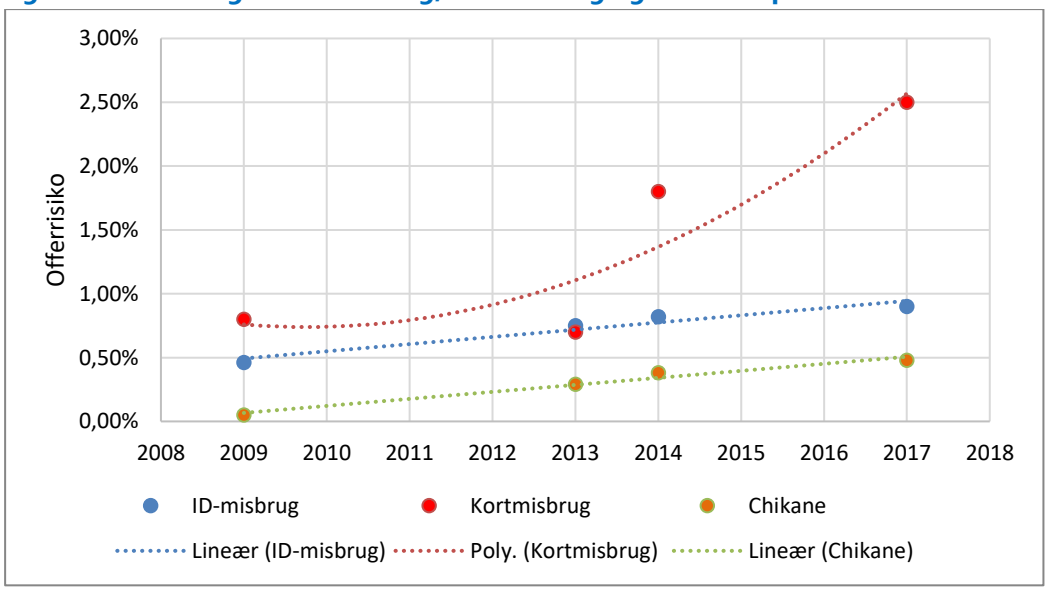
En gerningsperson kan overordnet tilegne sig en andens identitetsoplysninger på tre forskellige måder: Oplysningerne kan enten blive fremlagt af offeret selv, de kan blive franarret, eller de kan blive stjålet. Tilegnelse kan ske online, men også offline. I denne rapport beskrives internetkriminalitet, 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.

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.

Udviklingen i økonomisk og chikanøs misbrug af identitets- og betalingskortoplysninger

Misbrug af identitetsoplysninger, kortoplysninger og digitale profiler (chikane) var emnet for offerundersøgelserne i 2009, 2013, 2014 og 2017. Der findes således fire målinger for den forløbne niårsperiode. Figur O.1 viser, hvordan disse tre former for misbrug af oplysninger knyttet til ofrets person/identitet har udviklet sig. For både identitetsmisbrug og chikane er væksten mere eller mindre lineær. Offerrisikoen i 2017-målingen er på henholdsvis 0,9 procent (identitetsmisbrug) og 0,5 procent (chikane). Misbruget af betalingskortoplysninger betegner derimod en kurve, der svarer til et andengradspolynomium, og hvis denne udvikling fortsætter, kan vi forvente en markant vækst i omfanget af denne kriminalitetstype. Offentlige statistikker for betalingskortmisbrug ved e-handel viser den samme tendens, men tallene for første halvår i 2017 peger i retning af, at kurven muligvis er knækket. I 2017-målingen er offerrisikoen 2,5 procent og ligger dermed på et klart højere niveau end risikoen for misbrug af identitetsoplysninger henholdsvis chikane.

Figur O.1 Udviklingen i id-misbrug, kortmisbrug og chikane i perioden 2009-2017



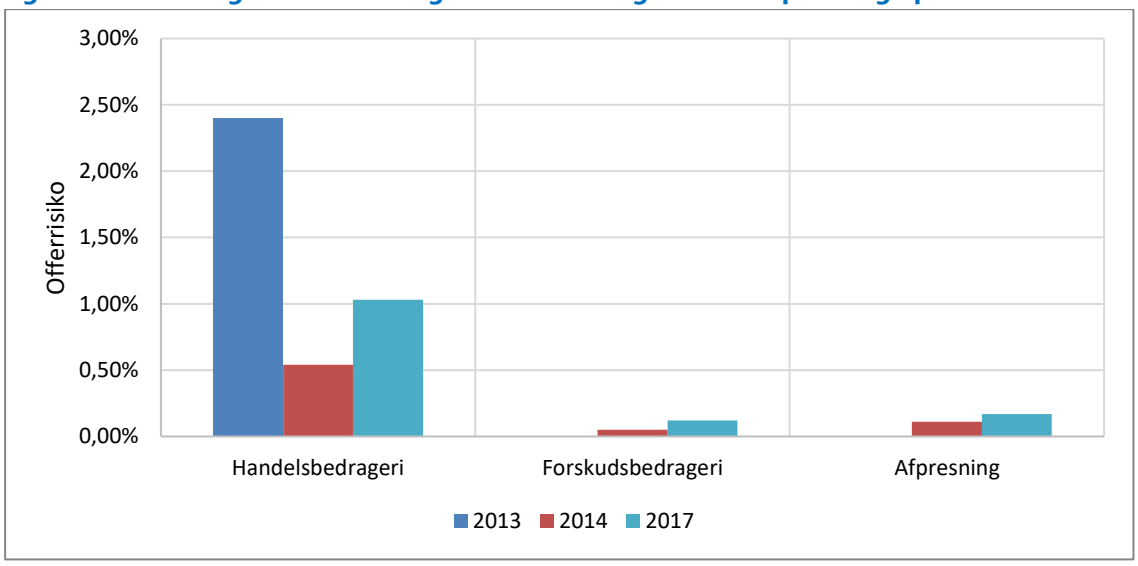
En opgørelse fra Konkurrence- og Forbrugerstyrelsen viser, at tabet på misbrug af dansk-udstedte betalingskort i forbindelse med e-handel steg fra ca. 117 mio. kr. i 2014 til 191 mio. kr. i 2015. Nationalbankens tal for 2016 viser et tab på 350 mio. kr. Kun ca. 20 procent af det samlede tab på dansk-udstedte betalingskort skyldes kortmisbrug i danske netbutikker, mens hele 80 procent af tabet kan tilskrives udenlandske netbutikker. Det danske erhvervslivs tab er dermed forholdsvis beskedent, for så vidt angår dansk-udstedte kort. Hertil kommer tabet på misbrug af udenlandske betalingskort, der ifølge Nationalbanken var 52 mio. kr. Det samlede tab for den danske e-handel lå dermed i 2016 på 123 mio. kr. (71 mio. kr. på dansk-udstedte kort og 52 mio. kr. på udenlandske kort).

Udvikling af bedrageri og afpresning

Handelsbedrageri var genstand for offerundersøgelserne i både 2013, 2014 og 2017, mens forskudsbedrageri[2] og afpresning[3] kun indgik i de to sidstnævnte. Dermed findes der kun data for henholdsvis fem- og fireårige perioder. Forskudsbedrageri og afpresning forekommer ret sjældent, men målinger fra 2014 og 2017 indikerer, at lidt flere danskere blev udsat for disse former for internetkriminalitet i 2017 end i 2014. Tallene er dog alt for små til at kunne påvise en statistisk signifikans. Den målte vækst giver derfor kun et fingerpeg og udgør ikke en solid dokumentation.

Fra 2013 til 2014 var der et markant fald i risikoen for at blive udsat for handelsbedrageri. I 2014-rapporten tolkedes faldet således: "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". 2017-målingen viser til gengæld en voksende risiko i forhold til 2014. Igen kan vi kun spekulere på årsagerne, men ifølge FDIH shopper danskere mere og mere i udenlandske netbutikker, hvorved bedrageririsikoen muligvis tiltager.

Figur O.2 Udviklingen i handels- og forskudsbedrageri samt afpresning i perioden 2013-2017



[2] Forskudsbedrageri er de former for bedrageri, hvor offeret bliver lokket til at betale et forskud for at opnå et eller andet.

[3] 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 vores offerundersøgelse peger på 0,1 procent inden for de sidste 12 måneder. De 8 procent er en livstidsprævalens, men under alle omstændigheder er der langt ned til vores 0,1 procent. Formodningen er, at en betydelig del af respondenterne i Digitaliseringsstyrelsens og DKCERT's undersøgelse har været udsat for malware, men ikke ransomware.

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 dem, der udsættes for misbrug af betalingskort online. Personer, der rammes af identitetsmisbrug, melder sjældnere om et tab, men deres andel er i 2017 vokset markant.

Tabel O.1 Procentdel af ofre, der melder om tab (uanset om de selv hæfter for det)

	2013	*2014*	*2017*
Identitetsmisbrug	56 %	54 %	73 %
Misbrug af betalingskortoplysninger	71 %	86 %	89 %
Bedrageri ved internethandel	100 %	87 %	86 %

Tabel O.2 viser det gennemsnitlige tab for respondenterne i offerundersøgelsen. I 2017 lå det gennemsnitlige tab ved identitetsmisbrug, kortmisbrug og handelsbedrageri på samme niveau, men dette var ikke tilfældet i 2013- og 2014-målingerne. Det er vanskeligt at fortolke denne udvikling, men det gennemsnitlige tab ved handelsbedrageri i 2017 kan skyldes større opmærksomhed på denne form for bedrageri, eftersom tallet er klart højere end i de tidligere målinger.

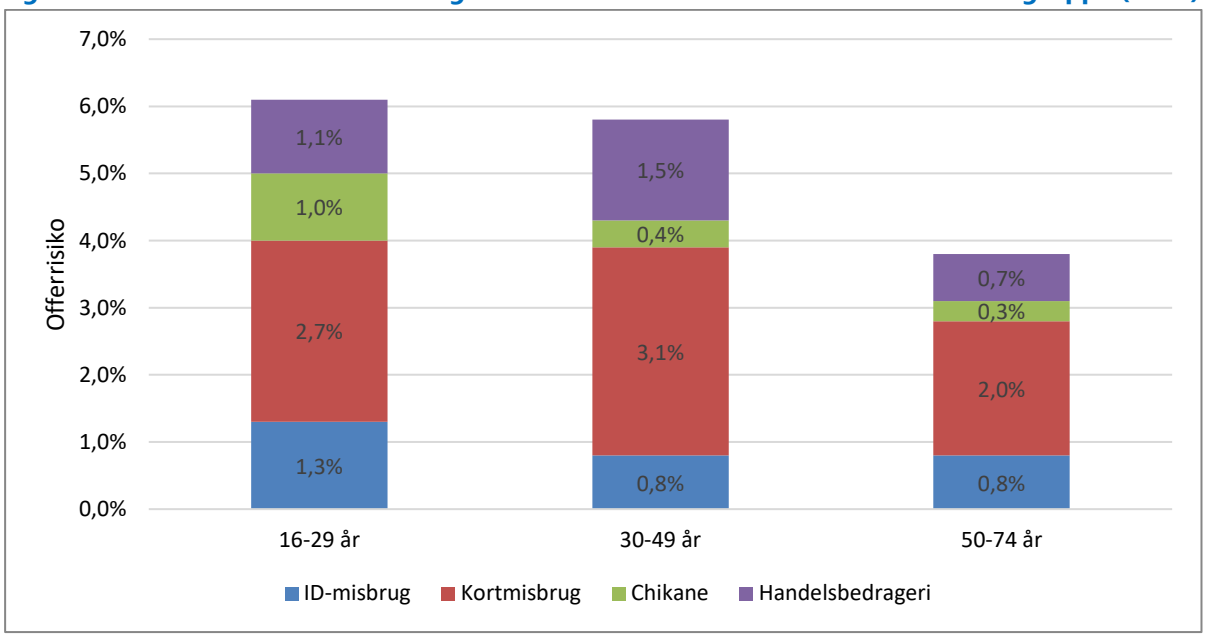
Tabel O.2 Gennemsnitlige tab (uanset om offeret selv hæfter)

	2013	*2014*	*2017*
Identitetsmisbrug	8.642	8.878	7.595
Misbrug af betalingskortoplysninger	13.044	6.250	6.103
Bedrageri ved internethandel	3.865	1.184	5.227

I offerundersøgelsen findes oplysninger om respondenternes køn, alder, herkomst, kommunetype, husholdning, uddannelse og erhverv. Disse baggrundsvariabler er blevet anvendt til at tegne en offerprofil. Dette er sket ved hjælp af en logistisk regressionsanalyse, og der er dermed taget højde for, at baggrundsvariablerne påvirker hinanden indbyrdes. Analysen viser, at tre variabler har en signifikant indflydelse på offerrisikoen: herkomst, alder og uddannelse. Stikprøven omfatter imidlertid kun et begrænset antal indvandrere og efterkommere, og offerprofilen tegnes derfor alene ud fra alder og uddannelsesniveau.

Figur O.3 viser offerrisikoen for tre aldersgrupper.[4] For den yngste (16-29 år) og den mellemste gruppe (30-49 år) ligger offerrisikoen på samme niveau, mens den ældste gruppe (50-74 år) har en betydeligt lavere risiko. Især kortmisbrug og handelsbedrageri bidrager til forskellen. Vi antager, at den ældre aldersgruppes lavere risiko skyldes en anderledes netadfærd, men offerundersøgelsen dokumenterer ikke kausaliteten.

Figur O.3 Offerrisikoen ved forskellige former for internetkriminalitet efter aldersgruppe (2017)

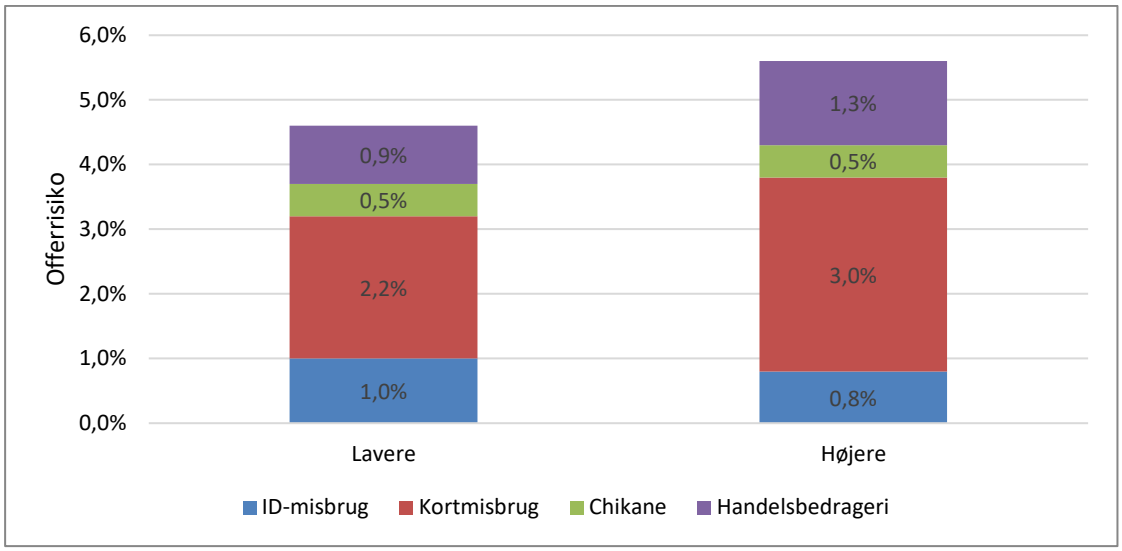


Figur O.4 viser offerrisikoen ved et henholdsvis lavere og højere uddannelsesniveau. Mellemlange og lange, videregående uddannelser medregnes begge under højere uddannelsesniveau, mens alle andre uddannelser regnes for et lavere uddannelsesniveau. Som det fremgår, har respondenter med et højere uddannelsesniveau en større risiko for at blive udsat for internetkriminalitet end dem, der er uddannet på et lavere niveau. Vi må antage, at den forklarende faktor ikke er uddannelsesniveauet i sig selv, men at det korrelerer med den reelle år-

[4] Figuren indeholder en kumuleret oversigt. Det vil sige, at en person, der har været udsat for to typer af internetkriminalitet, tæller med to gange. Hvis vi ser på, hvilke unikke dele af aldersgrupperne der har været udsat for en eller flere former for internetkriminalitet, er resultatet 5,6 % (16-29 år), 5,3 % (30-49 år) og 3,6 % (50-74 år).

sag, som fx kan være købekraften. Det er kortmisbrug og handelsbedrageri, der forårsager forskellen.

Figur O.4 Offerrisikoen ved forskellige typer internetkriminalitet efter uddannelsesniveau (2017)



Politianmeldelse

Lidt over en tredjedel af sagerne (36 %) vedrørende internetrelateret kriminalitet bliver ifølge offerundersøgelsen i 2017 politianmeldt. Det er ikke nødvendigvis respondenten, der anmelder sagen, men ved misbrug af betalingskort ofte banken eller kortselskabet.

Tabel O.3 Politianmeldelse (procentdel af incidenter)

	2013	*2014*	*2017*
Identitetstyveri	27 %	25 %	24 %
Misbrug af betalingskortoplysninger		39 %	49 %
Chikane	11 %	11 %	15 %
Bedrageri ved internethandel	18 %	22 %	34 %
Forskudsbedrageri		-	29 %
Afpresning		14 %	-

I 14 af de 107 politianmeldte sager (13 procent) har politiet ifølge respondenten afvist anmeldelsen. I undersøgelsen er der ikke blevet spurgt om begrundelsen, men vi må antage, at politiet har vurderet, at den konkrete sag ikke indebar en strafbar handling, eller at det ikke var respondenten – men fx banken – der burde anmelde sagen.

Grænseoverskridende

I 2017-offerundersøgelsen er de respondenter, der har været udsat for internetkriminalitet, blevet bedt om med et tal at bedømme, hvor grænseoverskridende oplevelsen har været for dem. På skalaen, der går fra 1 til 10, står 1 for ikke-grænseoverskridende og 10 for meget

grænseoverskridende. Ca. to tredjedele af respondenterne betragter oplevelsen som stærkt grænseoverskridende (score fra 8 og opefter), mens den for én tredjedels vedkommende har føltes lidt mindre alvorlig (score fra 7 og nedefter).

Forventningen var, at respondenterne ville bedømme kortmisbrug som mindre grænseoverskridende end identitetsmisbrug eller chikane, men denne antagelse holdt ikke stik for der er ikke store forskelle ved de forskellige former for internetkriminalitet. Jo højere alder, jo mere grænseoverskridende bedømmes oplevelsen. Kvinder har desuden en højere gennemsnitlig score end mænd.

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 forurettedes 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: integrity crimes, assisted crimes og content crimes. Denne inddeling er på linje med politiets opdeling (Politiets National Strategisk Analyse 2017, s. 157):

1. *It-afhængig kriminalitet* er kriminalitet, som kun kan finde sted ved brug af en computer(netværk) eller en anden form for informationskommunikationsteknologi (IKT). 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. *It-faciliteret kriminalitet* omfatter kendte kriminalitetsformer såsom tyveri og bedrageri, der begås ved hjælp af IKT. 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 IKTs integritet. Men set med krimino-

logiske øjne er der også nye aspekter ved computerassisterede forbrydelser, fx spiller afstand og geografiske grænser ingen rolle i cyberspace.

3. It-facilitering af *kriminelt indhold* 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.[5] 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. Politiet har imidlertid ved hjælp af it-relaterede søgeord gennemgået anmeldelser i POLSAS.[6] På baggrund heraf er der blevet fremlagt en statistik over internetrelaterede anmeldelser af berigelseskriminalitet, trusler og seksualforbrydelser i perioden fra 2009 til 2016 (National Strategisk Analyse 2017, s. 160).

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

[5] 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.

[6] De anvendte søgeord kan ses i Metoderapporten til National Strategisk Analyse 2017 (s. 34-35). Det bemærkes i rapporten, at "metoden kan derfor bruges til at undersøge udviklingstendensen indenfor området generelt, men ikke til at angive et absolut anmeldelsestal på området" (s. 35).

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 virksomheden selv står for overvågning, og at politiet først kommer ind i billedet, når den strafferetlige vej skal benyttes. Det betyder, at virksomheder – fx banker og betalingskortselskaber – samt branche-organisationer antageligt har bedre indblik i internetkriminalitetens omfang end politiet. Finans Danmark oplyser således tal for netbankindbrud, Nets tal for misbrug af Visa/Dankort og Nationalbanken for betalingskortmisbrug. Disse statistikker inddrages i rapporten.

De sidste vigtige kilder er rapporter fra DKCERT.[7] DKCERT har siden 2013 i samarbejde med Digitaliseringsstyrelsen publiceret en årlig undersøgelse af danskernes informationssikkerhed. Undersøgelserne er baseret på stikprøver blandt ca. 1.000 danskere og belyser, hvorvidt borgerne har oplevet sikkerhedshændelser[8], hvilke konsekvenser de har fået for borgernes kontakt med det offentlige, og hvad borgerne generelt ved om informationssikkerhed.[9]

1.4 Offerundersøgelse

Mørketalsproblemet og manglen på officielle statistikker kan til dels afhjælpes af en offerundersøgelse. 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 – interviewundersøgelser, 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- og nettostikprøver varieret lidt i størrelsen gennem årene. De sidste par år deltager ca. 60 % af de udvalgte personer deltager i undersøgelserne, og der udspørges ca. 1.000 respondenter hver måned (Boesen Pedersen, Kyvsgaard & Balvig, 2017).

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 be-

[7] 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.

[8] Der er ikke blevet spurgt om sikkerhedsproblemer i en bestemt periode. Det er derfor svært at fortolke tendenser og umuligt at sige noget om offerrisikoen på årsbasis.

[9] I 2016-udgave af rapporten er både offentligt ansatte og privatansatte inddraget.

tragtning, når tallene fortolkes og forklares" (Boesen Pedersen, Kyvsgaard & Balvig, 2017, s. 10). 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, samt i perioden juni til og med december 2017 (minus oktober), 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*	***2017*** *Juni-dec. 2017 N = 5.996*
Misbrug af ID-oplysninger	X	X	X	X
Misbrug af kortoplysninger	X	X	X	X
Chikane	X	X	X	X
E-handelsbedrageri		X	X	X
Privathandelsbedrageri		X	X	X
Nigeria-breve			X	X
Afpresning			X	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=5.996).

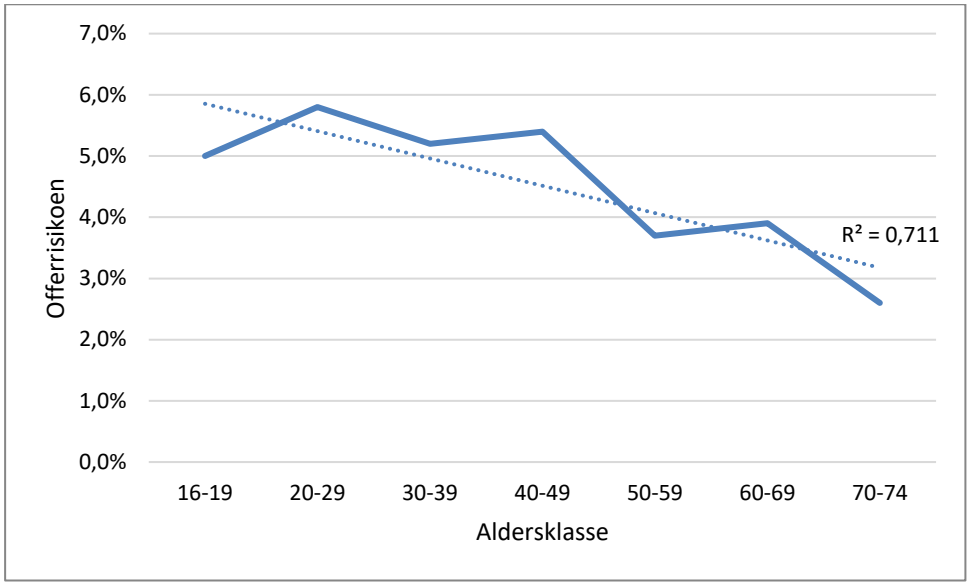
Tabel 1.2 Oversigt over baggrundsvariablernes opdeling for logistisk regressionsanalyse (n=5.996)

Variabler	*Opdeling*	*Fordeling*
Køn	Mand	49 %
	Kvinde	51 %
Alder	45 år eller yngre	42 %
	46 år eller ældre	58 %
Herkomst	Dansker	92 %
	Indvandrer/efterkommer	8 %
Kommunetype	Bykommune	47 %
	Andet	53 %
Husholdning	Par med børn	53 %
	Andet	47 %
Uddannelse	Mellem/langvarig	34 %
	Andet	66 %
Erhverv	I arbejde	60 %
	Ikke i arbejde	44 %

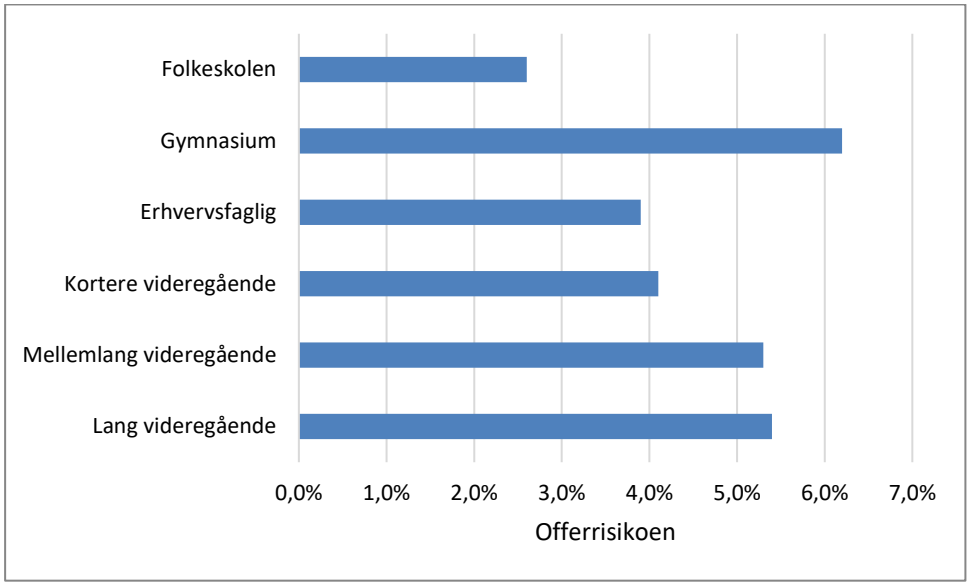
Eftersom antallet af respondenter, der er blevet ramt af internetkriminalitet, er meget begrænset i forhold til antallet af respondenter, der ikke er blevet ramt, er det svært at opnå statistisk signifikans. I første omgang er der blevet udført en logistisk regressionsanalyse af alle de førnævnte baggrundsvariabler. Analysen viser, at tre variabler er signifikante, som påviser en statistisk sammenhæng, men siger ikke noget om kausaliteten. Den første signifikante variabel er alderen: Yngre respondenter har en større risiko for at blive udsat for internetkriminalitet end ældre respondenter. 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 (2014 undersøgelsen viste den samme resultat for så vidt uddannelse angår). Vi må antage, at livsstil og (risiko)adfærd har en indflydelse på offerrisikoen. Hvorledes en persons alder og uddannelsesniveau hænger sammen med livsstil og adfærd, kan ikke fastslås med denne undersøgelse (men kunne være interessant at få nærmere belyst). Den sidste signifikante variabel er herkomst: Indvandrere og efterkommere har en større risiko for at blive udsat for internetkriminalitet end danskere. Det er oplagt at tro, at sproget er den afgørende faktor. Stikprøven omfatter imidlertid kun et begrænset antal indvandrere og efterkommere, og offerprofilen tegnes derfor alene ud fra alder og uddannelsesniveau.

269 af de 5.996 respondenter tilkendegiver, at de har været udsat for en eller flere af de omtalte former for internetkriminalitet. Det svarer til en offerrisiko på 4,5 procent inden for et år. En nærmere fordeling efter alder og uddannelsesniveau ses i nedenstående figurer.

Figur 1.1 Offerrisikoen efter aldersklasse (2017)



Figur 1.2 Offerrisikoen efter uddannelsesniveau (2017)



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.[10] Også Europol (2012) regner misbrug af finansielle 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).

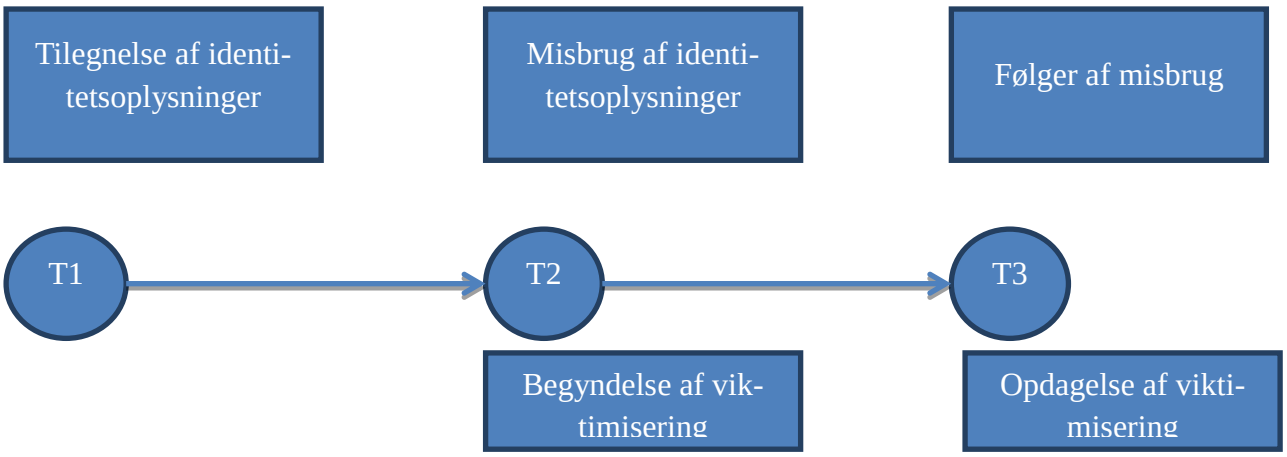
Ifølge McNally & Newman bruges begreberne identitetstyveri (identity theft) og identitetssvig (identity fraud) ofte som synonymer. Binder & Gill (2005) definerer identitetstyveri (identity theft) som det at overtage og misbruge en anden persons identitet, mens de definerer identitetssvig (identity fraud) 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 Assess-ment (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.[11]

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

[10] 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."

[11] "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).

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

Ifølge OECD har 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.

De seneste år har flere lande indskrevet identitetstyveri/-misbrug/-krænkelse i deres straffelove. 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.

I Holland er identitetsmisbrug kriminaliseret i straffelovens artikel 231b, som er indført 1. maj 2014. Strafferammen går op til 5 års fængsel. Det fremgår af artikel 231b, at der skal være tale om forsæt, at formålet enten skal være at skjule sin egen identitet eller at misbruge en andens identitet, og at der skal være forvoldt skade. Efter fremsættelsen af lovforslaget i parlamentet blev justitsministeren bl.a. spurgt om, hvorvidt han kunne redegøre for, hvilke situationer der omfattes af artikel 231b. Ministeren fremlagde derefter to eksempler: 1) en situation, hvori der lejes noget i en anden persons navn, og udlejer sender regningen til denne person. Altså et eksempel på økonomisk skade som følge af identitetsmisbrug. 2) en situation, hvori en person opretter en konto i en andens navn og efterfølgende krænker vedkommendes omdømme. Dette eksempel hører til det, vi i denne rapport betegner som chikane. Arti-

kel 231bs begreb "skade" kan så stå for økonomisk skade. Dermed får offeret mulighed for at bede anklageren/dommeren tage stilling til et erstatningskrav under den strafferetlige behandling af sagen og behøver ikke nødvendigvis at anlægge et civilretligt søgsmål.

I Sverige blev identitetsmisbrug skrevet ind i straffeloven 1. juli 2016. Ifølge paragraf 6b i straffelovens kapitel 4 skal "enhver, der ved ulovlig brug af en anden persons identitetsdata hævder at være ham eller hende og derved forårsager skade eller ulempe for ham eller hende, dømmes for uautoriseret identitetsbrug til bøde eller fængsel i højst to år".

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.

Straffelovsrådet har i sin betænkning om freds- og ærekrænkelser (2017) også overvejet, om der er grundlag for særskilt at kriminalisere brug af en andens identitet (identitetstyveri eller identitetsmisbrug). Rådet bemærker, at kun den mildeste form for identitetstyveri – at udgive sig for at være en anden, herunder ved oprettelse af en Facebook-profil i en andens navn – ikke allerede er strafbar. Derfor mener Rådet ikke, at der er behov for yderligere kriminalisering af identitetstyveri, "selvom sådanne former for identitetstyveri kan være meget generende for de personer, som får misbrugt deres identitet" (Straffelovsrådet, 2017, s. 126).

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).

I undersøgelsen *Danskernes informationssikkerhed* (Digitaliseringsstyrelsen & DKCERT, 2017) blev der spurgt om, hvorvidt respondenten har modtaget e-mails med forsøg på phishing. 58 % svarede, at de har modtaget sådanne mails. Heraf har 5 % indsendt de efterspurgte oplysninger. Spørgsmålet i denne undersøgelse dækker ikke over samtlige phishing-forsøg,[12] men omfatter formentlig størstedelen. 5 % af 58 % svarer til, at ca. 3 % af de udspurgte borgere har været udsat for phishing. Eftersom spørgsmålet ikke indeholdt en tidsbegrænsning, er det uvist, hvor mange der har været udsat for phishing på årsbasis.

[12] Spørgsmålets ordlyd: "Har du modtaget mails, hvor afsenderen beder dig indtaste private oplysninger på en webside?" Hermed udelukkes fx phishing-mails, som opfordrer til at indsende oplysningerne direkte.

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.

I DKCERT Trendrapport 2017 oplystes fordelingen af malware, som antivirusproducenten F-Secure havde identificeret på danskernes computere. Trojanske heste[13], der typisk spredes via inficerede websteder og e-mails, var i 2016 stadig klart den største malware-trussel. Trojanske heste stod således for 89 procent af alle konstaterede trusler; en mindre stigning i forhold til 2015, hvor de tegnede sig for 84 procent. Den mest udbredte trojanske hest i Danmark i 2016 var JS/Kavala, typisk sendt i en e-mail med en vedhæftet fil (DKCERT Trendrapport 2017, s. 13).

En undersøgelse i regi af Digitaliseringsstyrelsen & DKCERT udført i 2016 viser, at 31 procent af danskere har haft virus eller andre former for skadelige programmer på deres computer.

2.3.3 Offerundersøgelse

I offerundersøgelsen, der ligger til grund for denne rapport, er de 202 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. 57 af de 202 respondenter (28 procent) havde en idé om dette. Af disse 57 mente 81 procent, at det var sket online (mod 69 procent i 2014). Tabel 2.2 viser en oversigt over de metoder, der efter respondenternes egen vurdering er blevet anvendt til tilegnelse af deres identitetsoplysninger.

[13] 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.

Tabel 2.1 Identitetsoplysninger er stjålet ved:

	2014		*2017*	
	Antal	*Procentdel*	*Antal*	*Procentdel*
Handel på nettet	24	39 %	27	47 %
Indbrud/tyveri	9	15 %	5	9 %
Hacking af computer/profil	7	11 %	11	19 %
Falsk e-mail (phishing)	6	10 %	4	7 %
Falsk hjemmeside (pharming)	6	10 %	4	7 %
Skimming af kort	5	8 %	5	9 %
Betaling i udlandet	3	5 %		
Misbrug begået af bekendte/kolleger	2	3 %	1	2 %
I alt	**62**	**100 %**	**57**	**100 %**

Note: I 2014 havde 98 respondenter havde ingen anelse om, hvordan deres identitetsoplysninger var blevet stjålet. I 2017 var dette antal 145.

Oversigten viser, at der i 47 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 72 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 (betalingskortoplysninger) 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 omnibusundersøgelser. Offerundersøgelsen baserer sig på stikprøver blandt tilfældigt udvalgte danskere i alderen 16-74 år. 5.996 respondenter har i perioden fra juni til og med december 2017 (minus oktober) fået stillet spørgsmål om identitetsmisbrug (se bilag 2). Af disse 5.996 respondenter angiver 54, eller 0,9 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*	*2017*
Omfang af stikprøver	1.853	9.582	6.130	5.996
Andel af ofre for identitetsmisbrug	0,46 %	0,75 %	0,82 %	0,90 %
95 %-sikkerhedsinterval	0,3 – 0,9 %	0,6 – 0,9 %	0,6 – 1,1 %	0,7 – 1,1 %
Antal ofre i Danmark (estimat)	18.653	31.249[14]	34.471	38.502
95 %-sikkerhedsinterval (estimat)	12.165 – 36.495	24.924 – 37.386	25.181 – 46.166	28.581 – 48.423

Det svarer til, at ca. 38.500 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[15] beregnes. Intervallet ligger mellem 0,7 og 1,1 procent, eller, når det omregnes til at gælde hele den danske befolkning, mellem 28.581 og 48.423 danskere.

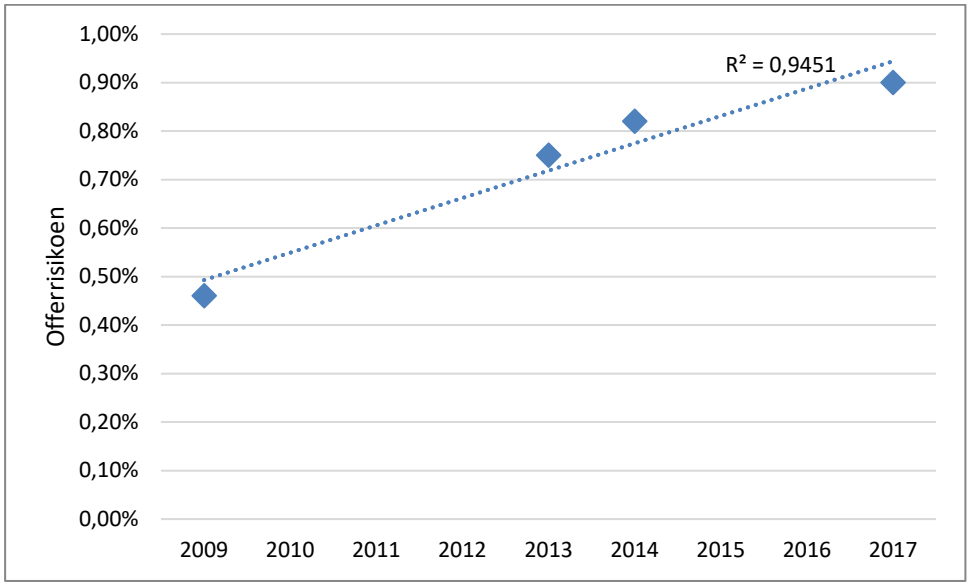
Offerundersøgelsen er behæftet med en række metodiske problemer (se bilag 1), og estimatet bør derfor tages med forbehold. Det er mere interessant at se på udviklingen i andelen af ofre. De fire målinger viser, at offerrisikoen i perioden fra 2009 til 2017 næsten er fordoblet.

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

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

Når vi tager højde for, at målingerne i 2013 og 2014 tidsmæssigt ligger tæt på hinanden, er udviklingen meget lineær. Dette fremgår af figur 3.1.

Figur 3.1 Offerrisikoen for identitetsmisbrug i Danmark i perioden 2009-2017.



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

Tabel 3.2 Offerrisiko efter type af misbrugte identitetsoplysninger

	2014		*2017*	
	Antal	*Procentdel*	*Antal*	*Procentdel*
(Bruger)navn/cpr-nummer/nem-id	11	42 %	13	42 %
Identitetsbeviser	6	23 %	2	6 %
Bankoplysninger	9	35 %	5	16 %
Kombination		-	10	32 %
Andet		-	1	3 %
I alt	**26**	**100 %**	**31**	**100 %**

Note: I 2014 havde 25 respondenter ikke svaret på hvilke identitetsoplysninger, der er blevet misbrugt. I 2017 var dette antal 23.

Lidt over halvdelen af de udsatte respondenter i 2014 og 2017-målingen har besvaret spørgsmålet om, hvilke identitetsoplysninger der er blevet misbrugt. Dermed bliver det svært at tolke tabel 3.2.

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.[16] 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 ofte 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

	2014 (n=51)	*2017 (n=54)*
Køb på kredit	43 %	43 %
Overførsel af penge	32 %	27 %
Leje af noget/tegning af abonnement	10 %	20 %
Kriminelt misbrug	2 %	-
Uoplyst formål	14 %	10 %
I alt	**100 %**	**100 %**

[16] 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). I Danmark har det siden 2014 været muligt at få et nyt cpr-nummer. I perioden fra april 2014 til og med marts 2017 har 6 personer fået tildelt et nyt cpr-nummer (KOU, Alm. del, Bilag 59, 13. maj 2015; SOU, Alm. del, Bilag 347, 7. juli 2016; SOU, Alm. del, Bilag 283, 28. juni 2017).

Selvom mange webbutikker har lukket for muligheden for at købe på kredit, findes der stadig butikker, som opretholder denne praksis. Tabel 3.3 viser, at køb på kredit i både 2014 og 2017 tegnede sig for lidt under halvdelen af sagerne. I begge målinger drejede ca. 30 procent af sagerne sig således om (at lokke andre til) overførsel af penge. Et eksempel herpå er en såkaldt "strandet i udlandet"-besked. Svindelen foregår ved, at der fra en hacket e-mailkonto afsendes en besked til bekendte, hvoraf det fremgår, at kontoens ejermand er strandet i udlandet, fx under ferie, og har brug for penge. Den kriminelle opfordrer herefter modtagerne til at overføre penge fx gennem Western Union. En anden metode, der benyttes i et vist omfang, er at leje forbrugsgoder eller tegne abonnementer i offerets navn.

3.3 Opdagelse og anmeldelse af identitetsmisbrug

Offeret opdager på et tidspunkt, at hans eller hendes identitetsoplysninger er blevet (forsøgt) misbrugt. I 37 procent af tilfældene (i 2014 halvdelen) 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 chance for, at skaden endnu ikke er sket. For halvdelen 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 mere end halvdelen 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. Dette sker for 7 procent af respondenterne. Eksempelvis fattede en respondent mistanke om misbrug og kontaktede derfor Udbetaling Danmark. Også for denne kategori gælder det, at forbrydelsen først erkendes, efter at den er fuldbyrdet.

Tabel 3.4 Opdagelse af misbrug

	2014 (n=51)	*2017 (n=54)*
Opdagelse gennem tredje person	51 %	37 %
Udskrifter, regning, opkrævning	31 %	56 %
Egen opdagelse	12 %	7 %
Ukendt	6 %	-
I alt	**100 %**	**100 %**

I offerundersøgelsen spørges der om, hvorvidt de respondenter, der har været udsat for identitetsmisbrug, har meldt sagen til politiet. I 2014-målingen angav 25 procent af respon-

denterne, at de havde anmeldt sagen. Undersøgelsen fra 2017 viste næsten det samme resultat; her havde 24 procent af respondenterne anmeldt misbruget til politiet.

Når forurettede melder sagen til politiet, er det ikke altid ensbetydende med, at anmeldelsen optages. Tre 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 73 procent (2017) af de respondenter, der havde været udsat for misbrug, at de havde lidt et tab. Denne andel er betydeligt større end i 2014, hvor kun 54 procent af respondenterne meldte om tab. Tabel 3.5 viser oversigten. Det gennemsnitlige tab (blandt de rapporterede) var i 2017 7.595 kr. Enkelte større beløb trækker dog gennemsnittet op; den største sum var således 50.000 kr. Medianbeløbet var langt lavere, nemlig 5.000 kr.

Tabel 3.5 Tabets omfang ved misbrug af identitetsoplysninger

	2014 (n=51)	*2017 (n=51)**
Intet tab	46 %	27 %
<= 1.000 kr.	13 %	18 %
1.001 – 5.000 kr.	17 %	27 %
5.001 – 10.000 kr.	4 %	12 %
>= 10.001 kr.	20 %	16 %
I alt	**100 %**	**100 %**
Gennemsnitligt tab	8.878 kr.	7.595kr.
Mediane tab	3.500 kr.	5.000 kr.

* I 2017-måling har 3 respondenter ikke oplyst omfang af tabet

I de fleste tilfælde hæfter ofrene ikke for tab, der knytter sig til identitetsmisbrug. I 2017 var det således kun 27 procent af de bestjålne, der selv måtte bære (en del af) tabet (mod 24 procent i 2014). Det drejede sig endda kun om en meget beskeden del af det samlede tab, nemlig 9 procent (mod 19 procent i 2014).

3.5 Offerprofil i forbindelse med identitetsmisbrug

Som nævnt i kapitel 1 udarbejdes offerprofilen på baggrund af alder og uddannelsesniveau.[17] Tabel 3.6 viser, at respondenter under 30 år og med en lang eller mellemlang, videregående uddannelse har den største offerrisiko. Respondenter over 30 år med en tilsvarende uddannelse har derimod den laveste risiko.

[17] Herkomst var også signifikant i regressionsanalysen, men eftersom der optræder alt for få respondenter med indvandrer-/efterkommer-status, indgår herkomsten ikke i profilen.

Tabel 3.6 Offerrisiko ved identitetsmisbrug

	Folkeskolen, gymnasium, erhvers- og korte videregående uddannelser	Mellemlange og lange videregående uddannelser	I alt
16-29 år	0,9 %	1,4 %	1,3 %
30-49 år	1,0 %	0,6 %	0,8 %
50-74 år	1,0 %	0,7 %	0,8 %
I alt	1,0 %	0,8 %	0,9 %

3.6 Netbankindbrud og social engineering

Der findes stort set ingen registeroplysninger om misbrug af identitetsdata. Undtagelsen er netbankindbrud, som Finans Danmark offentliggør oplysninger om. 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.
- *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.[18] Erhvervskunder kan tegne en forsikring mod netbankindbrud – separat eller som en del af en kriminalitetsforsikring – hos deres forsikringsselskab.

Omfang og udvikling af netbankindbrud og social engineering

Antallet af netbankindbrud (inkl. forsøg) går op og ned. I nogle kvartaler sker der slet ingen indbrud, mens der i andre kvartaler registreres over 50. Rekorden blev sat i 3. kvartal 2008 med 106 indbrud. I perioden 2006-1. halvår 2017 registreredes i alt 1.091 netbankindbrud, og i 477 tilfælde (44 procent) førte de til tab. Figur 3.1 viser, at tendensen stiger og falder i to bølger. Den første stigning fandt sted i årene 2007-2009 og den næste i 2012-2013. I de to

[18] Medmindre privatkunderne har været groft uagtsomme i deres adfærd. Langt de fleste privatkunder har ifølge Finans Danmark fået erstattet deres fulde tab. Bankerne vil ikke oplyse, hvordan fordelingen mellem privat- og erhvervskunder ser ud.

mellemliggende år (2010-2011) faldt antallet af indbrud til næsten nul, og det samme gælder for perioden 2014-2016. Det første halvår af 2017 varsler formentlig en stigning for dette år.

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[19] 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.

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.[20]

Faldet siden 2014 forklares ikke med et kriminalpræventivt tiltag, men med en ændring i de kriminelles adfærd. På Finans Danmarks (dengang Finansrådet) hjemmeside gives følgende forklaring på 2014-faldet:

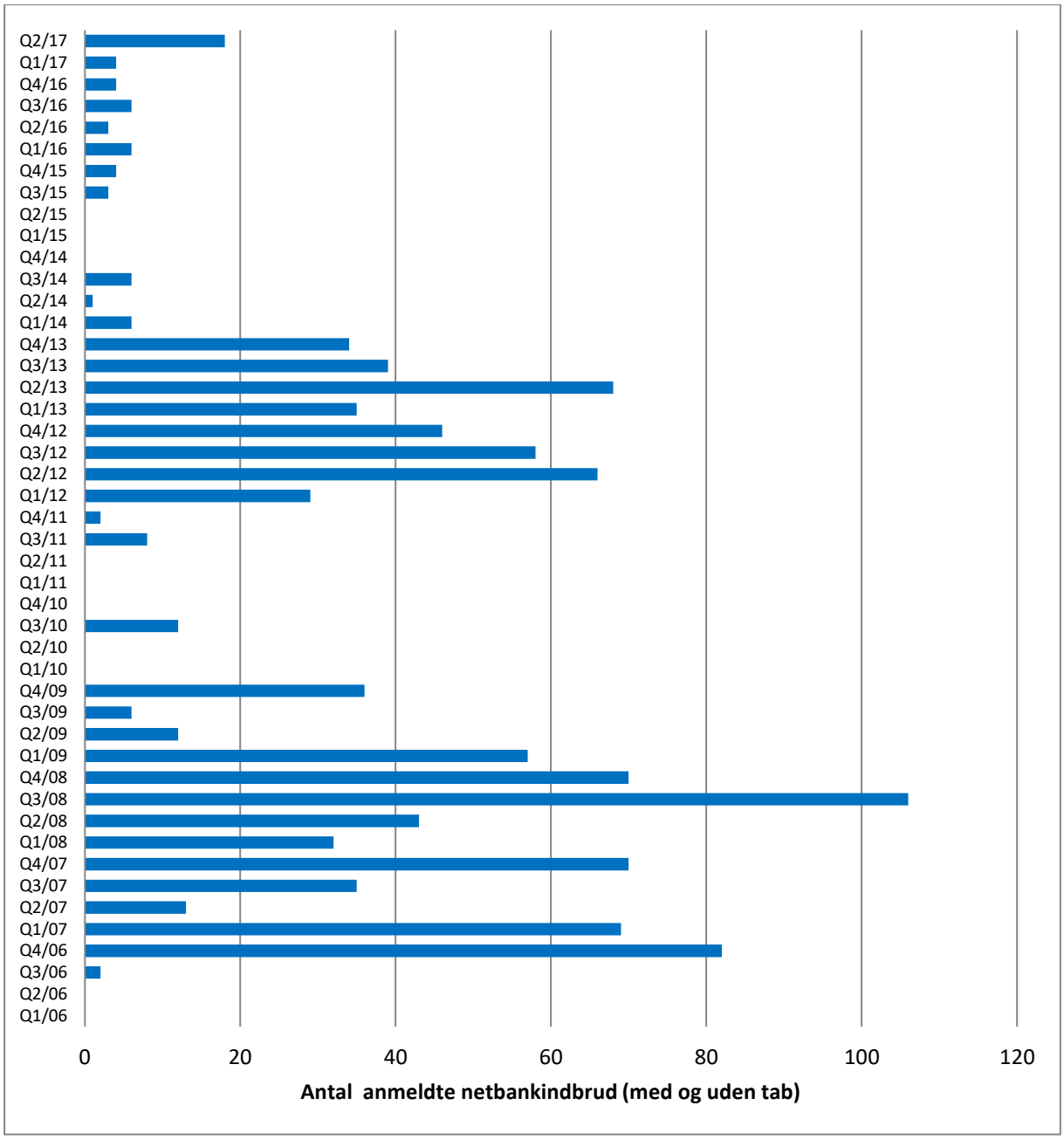
> Vi ser lige nu en ændring i angrebsmønstret hos de it-kriminelle og lige for tiden er de angreb der rammer kunderne ikke netbankindbrud. I stedet snydes kunderne til selv at gennemføre overførslerne eller sende deres nøglekort til de kriminelle. Desværre lykkes det ofte og derfor er der god forretning for de kriminelle i denne meget

[19] 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.

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

enkle kriminalitet, hvor kunden blot spørges pænt om alle sikkerhedskoder og et indbrud derfor ikke er nødvendigt.

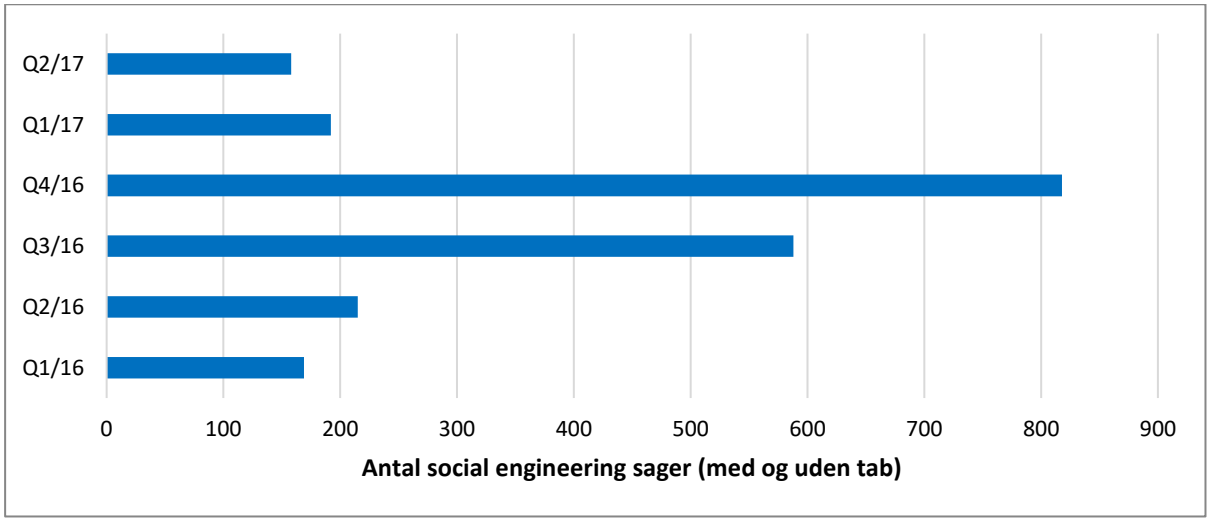
Figur 3.3 Udviklingen i antallet af netbankindbrud 2006 – 1e halvår 2017 (kvartalvis)



Kilde: Finans Danmark

Senere betegner Finans Danmark denne form for netbankkriminalitet som *social engineering* og har siden 2016 ført statistik over disse sager. På Finans Danmarks hjemmeside beskrives de som sager, hvor brugeren ved hjælp af falske e-mails, sms'er eller telefonopkald lokkes til at afgive eller indtaste oplysninger (id, password og nøglekortkoder) til it-kriminelle, som udgiver sig for at være eksempelvis et velrenommeret selskab, en myndighed eller en ven.

Figur 3.4 Udviklingen i antallet af social engineering sager 2016 – 1e halvår 2017 (kvartalvis)



Kilde: Finans Danmark

Tab på grund af netbankindbrud og social engineering

Det samlede tab på social engineering lå i perioden 2016-1. halvår 2017 på 7,8 mio. kr. En fjerdedel af sagerne førte til et tab, der i gennemsnit var på knap 15.000 kr. Dette gennemsnitstal er relativt lavt, men grundet antallet af sager var det samlede tab næsten tre gange så stort som tabet på netbankindbrud.[21]

Tabel 3.7 Netbankindbrud i Danmark (2006 – 1e halvår 2017)

	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
2015	7	5	71 %	0,8	166.031
2016	19	8	42 %	0,9	106.591
2017/1	22	16	73 %	1,9	116.908
I alt	**1.091**	**477**	**44 %**	**34,4**	**72.052**

Kilde: Finans Danmark, egne beregninger.

[21] 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.

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).

Det samlede tab på grund af social engineering var i perioden 2016-1e halvår 2017 på 7,8 mio. kr. En kvart af sagerne til et tab. Tabet er forskelligt fra sag til sag, men ligger i gennemsnit på knap 15.000 kr. I perioden 2016-1e halvår 2017 var det samlede tab på grund af social engineering næste tre gange så stor end tabet på grund af netbankindbrud. Det gennemsnitlige tab pr. sag er mindre ved social engineering, men der er mange flere sager end indbrud i netbanken.

Tabel 3.8 Bankkunder udsat for social engineering i Danmark (2016 – 1e halvår 2017)

	Antal sager	*Antal sager m. tab*	*Procentdel af sager m. tab*	*Tabets omfang (mio. kr.)*	*Gennemsnitligt tab pr. sag*
Q1/2016	169	26	15 %	0,4	15.250
Q2/2016	215	51	24 %	1,5	29.568
Q3/2016	588	126	21 %	1,9	15.017
Q4/2016	818	213	26 %	2,5	11.964
Q1/2017	192	54	28 %	1,0	18.511
Q2/2017	158	55	35 %	0,5	8.982
I alt	**2.140**	**525**	**25 %**	**7,8**	**14.931**

Kilde: Finans Danmark, egne beregninger.

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 (fx Mastercard, Visa), kortudsteder (fx en bank), kortindløser (fx Teller), betalingsmodtager (fx en forretning) og kortbruger (fx en forbruger) (Konkurrence- og Forbrugerstyrelsen, 2016, s. 9). Der findes en række forskellige typer af betalingskort. Konkurrence- og Forbrugerstyrelsen skelner mellem hævekort, debetkort[22], kreditkort[23], forudbetalte betalingskort og internationale betalingskort[24]. 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 er offentligt tilgængelige. Nationalbankens statistikbank indeholder oplysninger om betalingskortmisbrug fra og med første kvartal 2016.[25] Misbruget kan ske i både den fysiske (offline) verden og på internettet (online), men i denne rapport er vi primært interesserede i online-misbrug. Dette fænomen findes naturligvis ikke kun i Danmark, men i hele verden.

[22] 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.

[23] 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.

[24] 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).

[25] Formålet med statistikken er at belyse betalingsmarkedet i Danmark. Nationalbanken indsamler, bearbejder og offentliggør statistiske oplysninger vedrørende betalingstjenester. Betalingsrådet har bistået Nationalbanken i opbygningen af statistikken. Indsamling af oplysninger er baseret på følgende hovedkilder:

- Indberetninger fra danske banker og filialer af udenlandske banker
- Indberetninger fra betalingsinstitutter
- Indberetninger fra leverandører af kortterminaler
- Indberetninger fra indløsere af kortbetalinger.

Nationalbankens statistik går ikke længere tilbage end til 2016, men for mere historik kan man benytte oplysninger fra henholdsvis Nets og Konkurrence- og Forbrugerstyrelsen. Nets indsamler data om misbrug af Dankort og offentliggør en del af disse på sin hjemmeside. Når man betaler en vare med et Visa/Dankort i Danmark, er det dankortdelen, der benyttes, mens det i udlandet er Visadelen. Nets offentliggør kun tal vedrørende dankortdelen, altså misbrug på det danske marked.

Der mangler et samlet overblik over misbrug af internationale kort i Danmark for perioden før 2016, da de enkelte kortselskaber ikke offentliggør deres misbrugstal. I Konkurrence- og Forbrugerstyrelsens rapport Betalingskortmarkedet 2016 fremlægges dog et skøn foretaget på baggrund af oplysninger fra Mastercard, Visa, Nets, Danske Bank og SEB Bank.

Konkurrence- og Forbrugerstyrelsen har også undersøgt misbrug med dansk-udstedte betalingskort i udlandet, dog kun for årene 2014-2015. Også her gælder det, at de præcise tal er fortrolige.

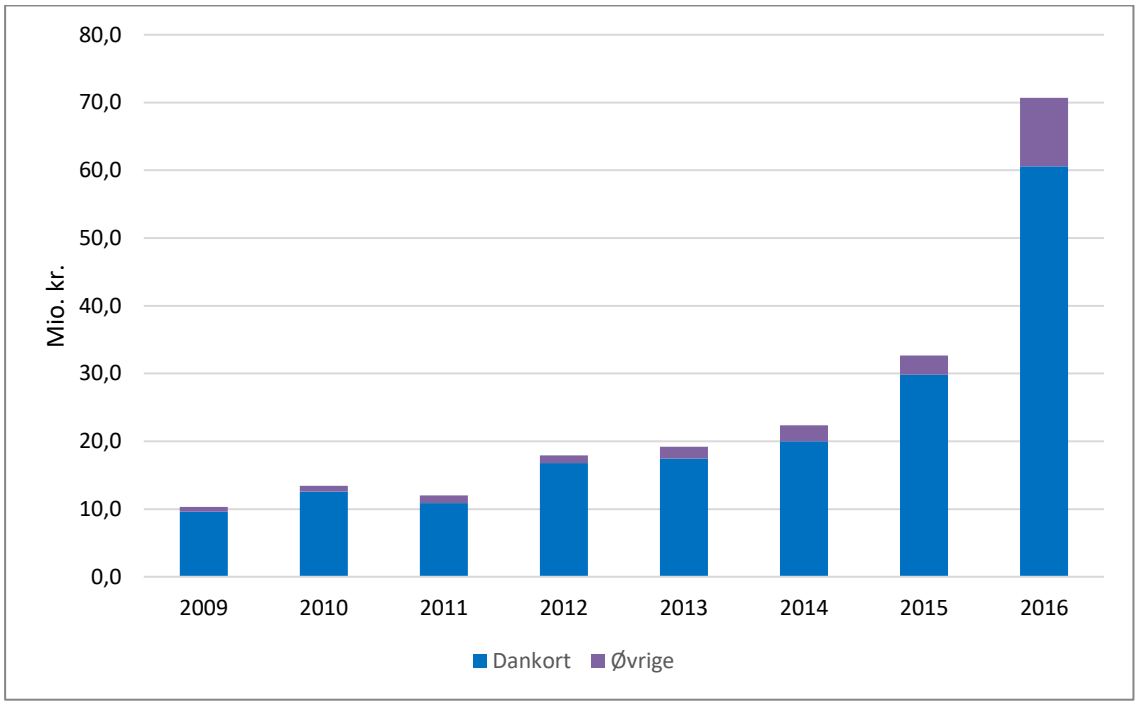
4.1 Betalingskortmisbrug på det danske marked

Misbrug på det danske marked kan ske med enten et dansk eller et udenlandsk betalingskort. Der findes offentligt tilgængelige statistikker om danske betalingskort på det danske marked fra og med 2009, mens der for udenlandske betalingskort kun er tal fra og med 2016.

Figur 4.1 viser, at tabet på misbrug af danske betalingskort på det danske e-marked steg støt i perioden 2009-2015, for nærmest at eksplodere i 2016. Der er registreret mere end en fordobling. Dette kan muligvis til dels tilskrives anvendelse af Nationalbankens statistik, der formentlig er mere fyldestgørende end de samlede oplysninger fra Nets og Konkurrence- og Forbrugerstyrelsen, men også Nets' tal for dankortmisbrug ved e-handel afslører en iøjnefaldende vækst i 2016.

Nationalbankens tal for de første to kvartaler af 2017 viser et fald på 11 procent i forhold til samme periode i 2016. Det indikerer, at betalingskortmisbruget på det danske e-handelsmarked foreløbigt toppede i 2016.

Figur 4.1 Tab på grund af misbrug af dansk-udstedte betalingskort på det danske e-handelsmarked (2009-2016)



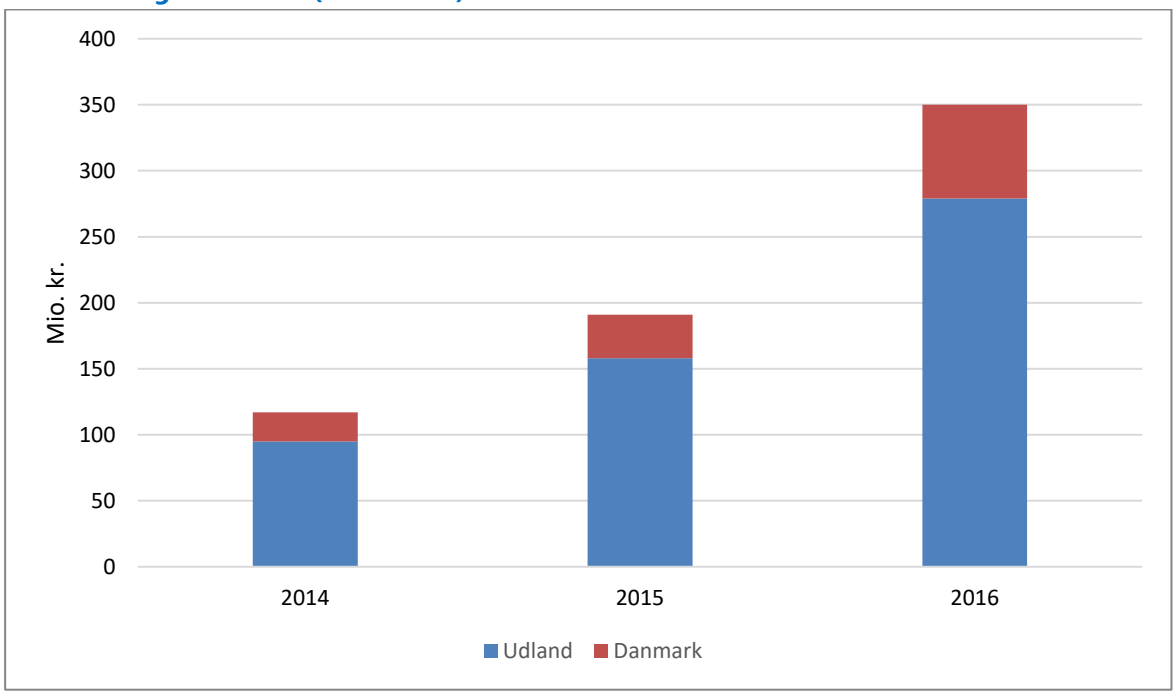
Kilder: Nets, Konkurrence- og Forbrugerstyrelsen og Nationalbanken

Det er ikke kun danske betalingskort, der misbruges i Danmark. I 2016 blev danske betalingskort misbrugt for 70,7 mio. kr. her i landet, mens udenlandske betalingskort tegnede sig for 52,2 mio. kr. De samlede tab på det danske e-handelsmarked i 2016 andrager derfor 122,9 mio. kr.

4.2 Misbrug af dansk udstedte betalingskort i Danmark og udlandet

Konkurrence- og Forbrugerstyrelsen har ligeledes undersøgt misbruget af dansk-udstedte betalingskort i udlandet, dog kun for årene 2014-2015. Også her gælder det, at de præcise tal er fortrolige, men opgørelsen understreger klart, at de største tab finder sted i udlandet og hovedsagelig i forbindelse med internethandel. I 2014 anslog Konkurrence- og Forbrugerstyrelsen tabet på nettet til ca. 95 mio. kr., når der alene ses på misbrug af dansk-udstedte betalingskort i udlandet. I 2015 var dette beløb steget til ca. 158 mio. kr. (Konkurrence- og Forbrugerstyrelsen, 2014, s. 32, Tabel 4.6). Nationalbankens statistik viser, at misbrug af dansk-udstedte betalingskort i udlandet i 2016 medførte et tab på 279 mio. kr. Det betyder, at ca. 80 procent af alt misbrug af dansk-udstedte betalingskort ved e-handel i årene 2014-2016 foregik i udlandet.

Figur 4.2 Samlede tab på grund af misbrug af dansk-udstedte betalingskort ved e-handel i Danmark og i udlandet (2009-2016)



Kilder: Nets, Konkurrence- og Forbrugerstyrelsen og Nationalbanken

4.4 Tabsfordeling mellem parterne

Retsgrundlaget for internethandel er betalingstjenesteloven.[26] § 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 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 betalingstjenestelo-

[26] Folketinget vedtog 2. juni 2017 den nye lov om betalinger. Loven trådte i kraft 1. januar 2018 og har erstattet lov om betalingstjenester og elektroniske penge. Denne rapport omhandler imidlertid året 2017, og derfor omtales her stadig lov om betalingstjenester.

ven 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[27], 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. Når en person handler på internettet og betaler med MasterCard, eller Visa/Dankort, vil der i nogle netbutikker blive bedt om at bekræfte betalingen med en engangskode (tilsendes på sms).

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.

[27] Pr. 1. januar 2018 er dette beløb som følge af indførelsen af Betalingsloven nedsat til 375 kr.

4.5 Misbrug af betalingskort (offerundersøgelse)

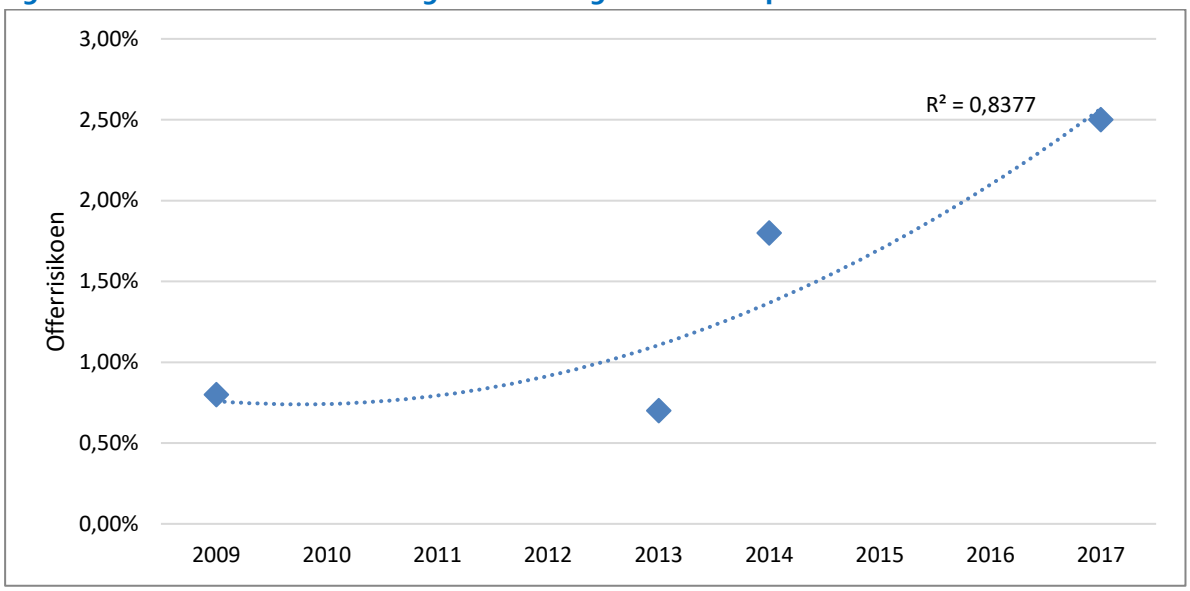
I offerundersøgelsen angav 148 af de 5.996 respondenter, eller 2,5 procent, at de havde været udsat for betalingskortmisbrug inden for de sidste 12 måneder. Det skal dog tilføjes, at ikke alle disse 148 personer rent faktisk også havde lidt et tab. Det er imidlertid både i politiets anmeldelsesstatistikker 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*	*2017*
Omfang af stikprøver	1.853	9.582	6.130	5.996
Andel ofre for betalingskortmisbrug	0,8 %	0,7 %	1,8 %	2,5 %
95 %-sikkerhedsinterval	0,4 – 1,2 %	0,6 – 0,9 %	1,5 – 2,1 %	2,1 – 2,9 %
Antal ofre i Danmark (estimat)	32.796	29.408	74.463	105.593
95 %-sikkerhedsinterval (estimat)	16.398 – 49.194	23.526 – 35.290	62.052 – 86.873	88.824 – 122.363

Dette svarer til, at ca. 105.000 danskere været udsat for betalingskortmisbrug i løbet af de sidste 12 måneder. 95 %-sikkerhedsintervallet ligger mellem 2,1 og 2,9 procent, eller, når det ganges op til at gælde hele befolkningen, mellem 88.824 og 122.363 danskere. Estimatet bør derfor tolkes med forbehold. Det er mere interessant at se på udviklingen i andelen af ofre. De fire målinger viser, at mens offerrisikoen var mere eller mindre stabil i perioden fra 2009 til 2013, fulgtes den i 2014 og 2017 af kraftige stigninger. Funktionen af de fire målinger beskrives bedst som et andengradspolynomium (linjen i figuren). [28]

Figur 4.4 Offerrisikoen for betalingskortmisbrug i Danmark i perioden 2009-2017.



[28] Et andengradspolynomium er et polynomium, hvori den uafhængige variabel indgår i op til anden potens. Formlen ser således ud: $P_2(x) = ax^2 + bx + c$

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 51 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=71)	49 %	31 %	20 %
Kort spærret (n=63)	50 %	35 %	15 %
Andet (n=14)	64 %	21 %	15 %
I alt (n=148)	**51 %**	**33 %**	**16 %**

Når forurettede anmelder sagen, er det ikke ensbetydende med, at politiet også optager anmeldelsen. Fire ud af de 22 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 86 procent (2014) og 89 procent (2017) 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 så-

dant) var i 2017 på det samme niveau som i 2014. Gennemsnittet trækkes op af enkelte større beløb. Derfor ligger medianen lavere.

Tabel 4.3 Tabets omfang ved misbrug af kortoplysninger

	2014 (n=109)	*2017 (n=142)**
Intet tab	14 %	11 %
<= 1.000 kr.	16 %	32 %
1.001-5.000 kr.	41 %	33 %
5.001-10.000 kr.	12 %	10 %
>= 10.001 kr.	17 %	14 %
I alt	**100 %**	**100 %**
Gennemsnitligt tab	6.250 kr.	6.103 kr.
Mediane tab	3.250 kr.	2.000 kr.

* I 2017 har 6 respondenter ikke oplyst tabets omfang.

I de fleste tilfælde hæfter ofrene ikke for tab, der knytter sig til betalingskortmisbrug. I 2014 hæftede 23 procent af de skadeslidte respondenter selv for (en del af) tabet. Det var imidlertid en beskeden del, og i alt betalte betalingskortmisbrugsofre selv 8 procent af det samlede tab. I 2017 måtte 18 procent selv dække (en del af) tabet. Her var andelen af det samlede tab 9 procent.

4.9 Offerprofil i forbindelse med betalingskortmisbrug

Som nævnt i kapitel 1 udarbejdes offerprofilen på baggrund af alder og uddannelsesniveau.[29] Tabel 4.4 viser på den ene side, at respondenter med en lang eller mellemlang, videregående uddannelse har en større offerrisiko end respondenter med kortere uddannelser. På den anden side falder offerrisikoen for den ældste aldersgruppe (50-74 år), muligvis på grund af færre eller sikrere nethandler.

Tabel 4.4 Offerrisiko ved betalingskortmisbrug

	Folkeskolen, gymnasium, erhvers- og korte videregående uddannelser	Mellemlange og lange videregående uddannelser	I alt
16-29 år	2,4 %	4,1 %	2,7 %
30-49 år	2,7 %	3,5 %	3,1 %
50-74 år	1,8 %	2,3 %	2,0 %
I alt	2,2 %	3,0 %	2,5 %

[29] Herkomst var også signifikant i regressionsanalysen, men eftersom der optræder alt for få respondenter med indvandrer-/efterkommer-status, indgår herkomsten ikke i profilen.

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.

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". Misbrug af en Facebook-profil er i pressen døbt Facerape. Politiken[30] 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. Drengene sigtedes for overtrædelse af brevhemmeligheden, blufærdighedskrænkelse og for at videregive 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. Data-

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

tilsynet 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

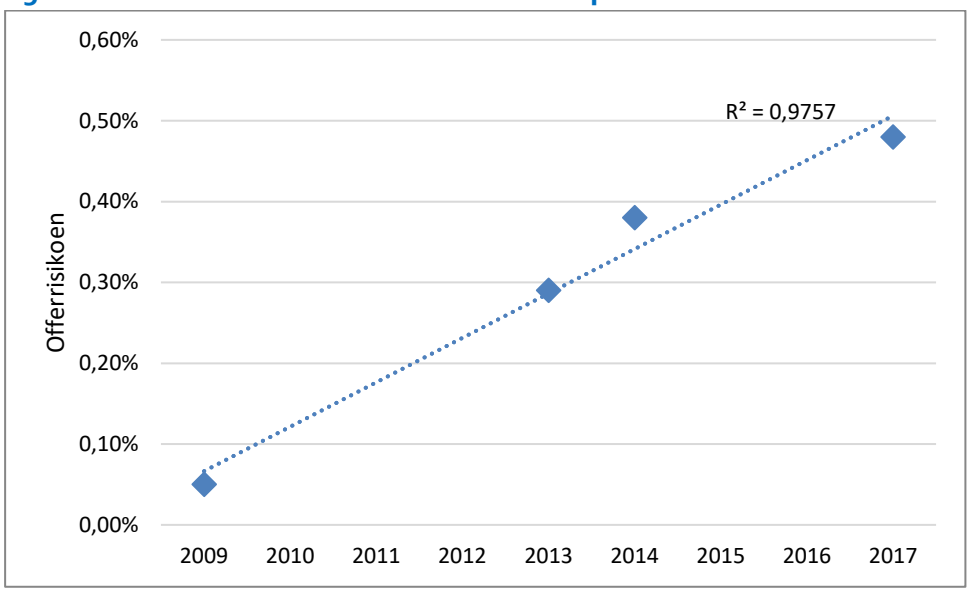
I offerundersøgelsen angav 29 af de 5.996 respondenter, eller 0,5 procent, at de havde været udsat for chikane inden for de sidste 12 måneder. Dette svarer til, at 20.690 danskere har været udsat for chikane i løbet af de sidste 12 måneder. 95 %-sikkerhedsintervallet ligger mellem 0,3 og 0,6 procent, eller, når det ganges op til at gælde hele den danske befolkning, mellem 13.191 og 28.190 danskere. Estimatet bør tolkes med forbehold

Tabel 5.1 Offerrisiko for chikane i Danmark

	2009	*2013*	*2014*	*2017*
Omfang af stikprøver	1.853	9.582	6.130	5.996
Andel af ofre for chikane	0,05 %	0,29 %	0,38 %	0,48 %
95 %-sikkerhedsinterval	0,0 – 0,3 %	0,2 – 0,4 %	0,2 – 0,5 %	0,3 – 0,6 %
Antal ofre i Danmark (estimat)	2.802	14.027	15.955	20.690
95 %-sikkerhedsinterval (estimat)	0 – 16.812	9.551 – 18.703	9.117 – 22.793	13.191 – 28.190

Når vi ser på udviklingen viser de fire målinger, at offerrisikoen næsten er tidoblet i perioden fra 2009 til 2017. Når vi tager højde for, at målingerne i 2013 og 2014 tidsmæssige ligger tæt ved hinanden, så er udviklingen meget lineær. Figur 5.1 viser den lineære udvikling.

Figur 5.1 Offerrisikoen for chikane i Danmark i perioden 2009-2017.



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 profilændringer. Tabel 5.2 viser oversigten.

Tabel 5.2 Fremgangsmåde ved chikane (multirespons)

	Antal	*Procentdel*
Profilændringer	10	27 %
Spredning af rygter/billeder i offerets navn	6	16 %
Modtagelse af uønskede e-mails (ej spam)	5	14 %
Chat i offerets navn	5	14 %
Afsendelse af e-mails i offerets navn	3	8 %
Falsk profil i offerets navn	3	8 %
Andet (uspecificeret)	5	14 %
I alt	**37**	**100 %**

5.2 Hensigt med og varighed af chikane

I en rapport om stalking (Tambour Jørgensen, 2013) udtalte to ud af tre respondenter, at de kendte stalkeren. Det kunne dreje sig om en ekskæreste, arbejdskollega, studiekammerat eller en eller anden, man havde mødt ved en fest. I denne undersøgelse af chikane på nettet svarede fem af de 27 ramte respondenter (19 procent), at de kendte personen, der stod bag chikanen (henholdsvis en partner, en ekspartner og tre "anden bekendt"). Når gerningspersonen er ukendt, er det formentlig svært at fastslå formålet med chikanen. Kun syv respondenter var således i stand til at pege på et motiv. Fire respondenter tilkendegav, at det handlede om opmærksomhed eller kontrol. En enkelt mente, at gerningsmanden var psykisk syg, mens andre angav årsager som "for jeg er pæn", "politisk motiv" og "via mit store netværk at få promoveret pornografisk indhold til mange".

Ovenstående tyder på, at respondenterne ikke havde stalking eller mobning i tankerne ved besvarelse af spørgsmålet om chikane.[31] 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."

For halvdelen chikaneofrene 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.

[31] 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).

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 2014-målingen svarede to ud af 22 respondenter (9 procent) ja, og i offerundersøgelsen fra 2017 svarede fire ud af 27 respondenter (15 procent), at de har anmeldt chikanen, men politiet afviste to af disse anmeldelser. Anmeldelsesprocenten 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

Som nævnt i kapitel 1 udarbejdes offerprofilen på baggrund af alder og uddannelsesniveau.[32] Hvad angår uddannelsesniveau, adskilte de respondenter, der havde været udsat for chikane, sig ikke fra dem, som ikke var blevet ramt. Derimod viser det sig, at offerrisikoen aftager med alderen. De 16-29-åriges offerrisiko er på 1,0 procent, mens den falder til 0,4 procent for de 30-49-årige og til 0,3 procent for de 50-74-årige.

[32] Herkomst var også signifikant i regressionsanalysen, men eftersom der optræder alt for få respondenter med indvandrer-/efterkommer-status, indgår herkomsten ikke i profilen.

6 Bedrageri ved internethandel

Der handles mere og mere på internettet. Ifølge en analyse fra Foreningen for Dansk Internet Handel (FDIH) gennemførte danskerne således 162 mio. handler i 2016, hvilket i forhold til 2015 var en stigning på 10 procent. Det svarer til en omsætning på 100,7 mia. kr. alene i 2016. Rejser er – målt på omsætning – den største varekategori med 23,8 mia. kr., efterfulgt af kategorien tøj, sko og smykker med en omsætning på 14,3 mia. kr. Hvad angår antallet af handler, toppes listen af kategorien tøj, sko og smykker med 29,1 mio. handler. På 2.-pladsen finder vi kategorien film, musik, bøger, spil og legetøj med 23,5 mio. handler (FDIH, 2017).

Internethandelen sker for 68 procents vedkommende i danske netbutikker, mens de mest populære udlande er England, Tyskland og Sverige. De vigtigste grunde til at handle i en udenlandsk netbutik er, at varen kun fås her og måske oven i købet er billigere. Ved 81 procent af handlerne benyttes Dankort og andre betalingskort (FDIH, 2017).

Internethandelen foregår dog ikke kun i webbutikker – også privatpersoner sælger ud, fx via dba.dk, guloggratis.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 godt 2.300 e-mærkede internetbutikker (pr. 1. februar 2018).

På e-mærkets internetside opfordres forbrugerne til at være opmærksomme på falske internetbutikker (fupbutikker). Ifølge e-mærket kan en fupbutik gennemskues, hvis man er opmærksom på sprogfejl, alt for billige mærkevarer, mangelfulde eller falske virksomhedsoplysninger og underlige webadresser.

I december 2017 har e-mærket overrakt en liste med 3.171 fupbutikker, der bruger danske domæner til Statsadvokaten for Særlig Økonomisk og international Kriminalitet (SØIK).

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), guloggratis.dk, qxl.dk og lauritz.com. Den Blå Avis og Gul og Gratis fungerer som en opslagstavle, mens Lauritz.com er en auktionsside.

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 MobilePay i forbindelse med betaling. MobilePay er knyttet til sælgers CPR nr., og derfor ligeledes en god sikkerhed for køberen.

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 til 400.000 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

I offerundersøgelsen angav 62 af de 5.996 respondenter, eller 1,0 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 62 ofre er 49 blevet bedraget ved køb i en netbutik, fem ved privathandel og otte respondenter er blevet ramt ved begge former for internethandel. Dette svarer til, at ca. 44.235 danskere har været udsat for internethandelsbedrageri i løbet af de sidste 12 måneder. 95 %-sikkerhedsintervallet ligger mellem 0,8 og 1,3 procent, eller, når det ganges op til at gælde hele den danske befolkning, mellem 33.303 og 55.167 danskere. Estimatet bør tolkes med et vist forbehold.

Tabel 6.1 Offerrisiko for bedrageri ved internethandel i Danmark

	2013	*2014*	*2017*
Omfang af stikprøver	9.582	6.130	5.996
Andel af ofre for handelsbedrageri	2,4 %	0,54 %	1,03 %
95 %-sikkerhedsinterval	2,1 – 2,7 %	0,4 – 0,8 %	0,8 – 1,3 %
Antal ofre i Danmark (estimat)	109.940	22.783	44.235
95 %-sikkerhedsinterval (estimat)	96.197 – 123.682	16.876 – 28.690	33.303 – 55.167

2013- og 2014-målingerne viser, at offerrisikoen faldt markant fra 2013 til 2014. Dette kan der være mange årsager til. 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. Imidlertid viser 2017-målingen, at offerrisikoen nu næsten er fordoblet i forhold til 2014, om end den stadig ligger på et betydeligt lavere niveau end i 2013.

6.4 Handelssted og handelsvare

I alt tilkendegav 37 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 ni respondenter ikke i stand til at svare. Af de resterende respondenter svarede 19, at det havde drejet sig om en udenlandsk netbutik, mens ni 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 (2017) finder 68 procent af alle internethandler (foretaget af danskere) sted i en dansk netbutik og 32 procent i en udenlandsk butik.

25 personer har rapporteret om bedrageri i forbindelse med privathandel. Af disse var 12 blevet bedraget som købere, mens 13 var blevet snydt som sælgere. 11 personer oplyser, at de havde benyttet sig af DBA eller en anden handelsplatform, mens 12 havde handlet på Facebook eller andre sociale medier.

Der er også blevet spurgt om, hvilken vare respondenten ville købe eller sælge i forbindelse med bedrageriet. Varekategorien "Tøj, sko og smykker" placerer sig øverst på listen over produkter, der snydes med i forbindelse med internethandel. En tredjedel 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 nethandelshandler. En kategori, der skiller sig positivt ud i forhold til andelen af handler, er "Rejse og kulturoplevelser". Denne kategori står for 7 procent af bedragerierne, mens dens andel af nethandel udgør omkring 14 procent. Tabel 6.2 viser hele oversigten.

Tabel 6.2 Handelsbedrageri: varekategorier

	Antal	*Procent*	*Nethandel**
Tøj, sko og smykker	20	33 %	18 %
IT, tele og foto	10	16 %	10 %
Kosmetik, medicin og kosttilskud	6	10 %	7 %
Rejser og kulturoplevelser	4	7 %	14 %
Bolig, have, blomster	4	7 %	9 %
Elektronik og hvidevarer	3	5 %	6 %
Film, musik, bøger, spil, legetøj	3	5 %	15 %
Anden kategori	11	18 %	21 %
I alt	**61**	**100 %**	**100 %**

* FDIH (2017) Årsrapport 2016, s. 17.

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 om, hvorvidt de respondenter, der har været udsat for handelsbedrageri, har meldt sagen til politiet. Det fremgår af Tabel 6.3, at to ud af tre svarede nej i 2017. Det vil sige, at en tredjedel af sagerne blev meldt til politiet, enten af respondenten eller af banken/kortselskabet. Anmeldelsestilbøjeligheden er dermed øget siden 2014.

Tabel 6.3 Opdagelse og politianmeldelse ved internethandelsbedrageri

	2014 (n=34)	*2017 (n=62)*
Ikke anmeldt	78 %	66 %
Respondent anmelder	13 %	21 %
Bank/kortselskab anmelder	9 %	13 %

Når forurettede anmelder sagen, er det ikke ensbetydende med, at politiet faktisk optager anmeldelsen. Fire af de 13 respondenter, der selv meldte sagen til politiet i 2017, 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 alt 59 respondenter oplyser, om de har lidt tab på grund af bedrageri ved internethandel. Dette er tilfældet i langt de fleste sager, og tabet ligger i gennemsnit på godt 5.000 kr. 60 procent har lidt et tab på under 1.000 kr., mens 10 procent har mistet over 10.000 kr.

I 60 procent af de sager, i hvilke der er tale om tab, hæfter ofrene selv enten helt eller delvist. Alt i alt må ofre for handelsbedrageri selv bære 58 procent af det samlede tab.

Tabel 6.4 Tabets omfang ved internethandelsbedrageri

	Antal	*Procent*
Intet tab	8	14 %
<= 1.000 kr.	28	47 %
1.001-5.000 kr.	15	25 %
5.001-10.000 kr.	2	3 %
>= 10.001 kr.	6	10 %
I alt	**59**	**100 %**
Gennemsnitligt tab	5.227	

6.7 Offerprofil i forbindelse med bedrageri ved internethandel

Som nævnt i kapitel 1 udarbejdes offerprofilen på baggrund af alder og uddannelsesniveau.[33] Tabel 6.5 viser, at respondenter med en lang eller mellemlang, videregående uddannelse har en større offerrisiko end respondenter med kortere uddannelser. Set i sammenhæng med alderen har de 30-49-årige den største offerrisiko uanset uddannelsesbaggrund. I den yngste gruppe er en lang eller mellemlang uddannelse lig med en mindre offerrisiko, mens det for de 50-74-årige er omvendt: Her stiger risikoen i takt med uddannelsesniveauet. Det er vanskeligt at pege på årsager til dette paradoks.

Tabel 6.5 Offerrisiko ved handelsbedrageri

	Folkeskolen, gymnasium, erhvers- og korte videregående uddannelser	Mellemlange og lange videregående uddannelser	I alt
16-29 år	1,3 %	0,5 %	1,1 %
30-49 år	1,5 %	1,6 %	1,5 %
50-74 år	0,5 %	1,1 %	0,7 %
I alt	0,9 %	1,3 %	1,0 %

[33] Herkomst var også signifikant i regressionsanalysen, men eftersom der optræder alt for få respondenter med indvandrer-/efterkommer-status, indgår herkomsten ikke i profilen.

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 Nigeriabreve og datingbedrageri (eller romance scam).

7.1 Nigeriabreve

Nigeriabreve[34] er det udtryk, der i Danmark typisk bruges som henvisning til forskudsbedrageri. Et Nigeriabrev 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 Nigeriabreve:

- 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

[34] Nigeriahenvendelser er et begreb, der bl.a. anvendes på dba.dk. Her fremgår det: "Nigeriahenvendelser kommer typisk fra udenlandske svindlere, som forsøger at komme i kontakt med sælgere på bl.a. DBA. Hvis man indleder en dialog på baggrund af en Nigeriahenvendelse, ender det som regel med, at man modtager enten en falsk udenlandsk check eller et 'bevis' for, at svindleren har overført penge via en anerkendt bank, PayPal eller via fx Western Union. Dokumentationen er falsk, og pengene er ikke overført." I denne rapport betragtes en sådan hændelse som handelsbedrageri (omtalt i kapitel 6).

- Tiggerbreve fra afrikanske børn.

Disse breve kommer nogle gange fra Nigeria, men langtfra altid. Årsagen til, at de kaldes Nigeriabreve, er, at afsenderne oprindeligt udgav sig for at være nigerianske embedsmænd. Nigeriabreve 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.

På Udenrigsministeriets hjemmeside findes fx en advarsel mod datingbedrageri begået af russere (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), medlidenhedshi-

stories eller angivelse af et specielt erhverv: general, major, civilingeniør i olieindustrien, guldindustrien, smykkedesigner (mænd) og sygeplejerske eller modedesigner (kvinder).

På romancescams.org bliver Asien, Rusland og Ukraine nævnt som geografiske områder i forbindelse med datingbedrageri, men man advarer også bestemte datingmålgrupper, såsom seniorer.

Ligesom ved Nigeriabreve 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."[35]

7.3 Omfanget af forskudsbedrageri

I offerundersøgelsen angav kun syv af de 5.996 respondenter, at de i løbet af de sidste 12 måneder havde været udsat for forskudsbedrageri. Syv ud af 5.996 lyder som et meget lille antal, hvilket det også er set i forhold til andre former for internetkriminalitet. I 2014-målingen tilkendegav tre ud af 6.130 respondenter, at de havde været udsat for forskudsbedrageri. Hvis vi kun ser på disse tal, har der i 2017 været tale om en fordobling i forhold til 2014. En beregning af, hvor mange danskere der inden for de sidste 12 måneder har været udsat for forskudsbedrageri, lander på ca. 5.000. Statistisk usikkerhed medfører, at dette tal kun er et estimat, men det viser, at forskudsbedrageri findes i Danmark. Dette stemmer også overens med mediehistorier og politiets erfaringer.

7.4 Nærmere om forskudsbedrageri

De syv respondenter, der i offerundersøgelsen fortalte, at de havde været udsat for forskudsbedrageri, fordelte sig kønsmæssigt på seks mænd og én kvinde. Aldersmæssigt er spredningen bredere; det yngste offer er 19 år, mens den ældste er 64. En af episoderne hørte til kategorien Nigeria-breve ("lotterigevinst"), mens to episoder handlede om datingbedrageri. De øvrige fire respondenter oplyste ikke, hvad de havde været udsat for. Ofrene var blevet kontaktet pr. e-mail (to gange) og gennem sociale medier (to gange); tre respondenter besvarede ikke dette spørgsmål. To af dem havde overført forholdsvis beskedne beløb (henholdsvis 500 og 1.800 kr.), mens et tredje offer havde overført 12.000 kr. i forbindelse med

[35] http://www.fyens.dk/indland/Politiet-advarer-Svindel-og-humbug-i-stor-stil/artikel/2105964).

datingbedrageri. Ét offer har ikke overført penge, mens de sidste tre ikke har givet oplysninger herom.

To af de syv respondenter fortæller, at de har anmeldt sagen til politiet. Den ene af disse anmeldelser blev optaget, mens den anden blev afvist. Af de øvrige har to respondenter ikke anmeldt episoden, mens tre ikke besvarer spørgsmålet.

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 (2017) er 985 personer i alderen 18-74 år blevet udspurgt om deres erfaringer med informationssikkerhed. Et af undersøgelsens emner var ransomware. Spørgsmålet lød således: "Har du oplevet, at et program spærrede for adgangen til din computer eller data og krævede betaling for at åbne for dem?" Dette svarede 8 procent af respondenterne ja til (Digitaliseringsstyrelsen & DKCERT, 2017, s. 36).[36]

8.2 Sexafpresning

Ved sexafpresning eller – på engelsk – sextortion (en sammentrækning af ordene sex og extortion) 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

[36] 8 procent af 985 respondenter svarer til 79 respondenter. I rapporten oplyses det, at 3 % betalte løsesum og fik deres data tilbage, mens 1 % betalte løsesum, men ikke fik data tilbage. De 3 og 1 procent svarer til 2 og 1 respondent(er).

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

I offerundersøgelsen angav 10 af de 5.996 respondenter, at de havde været udsat for afpresning i løbet af de sidste 12 måneder. 10 ud af 5.996 respondenter er ikke ret mange i forhold til andre former for internetkriminalitet. I 2014-målingen fortalte syv ud af 6.130 respondenter, at de havde været udsat for afpresning. Hvis vi kun ser på disse tal, var der i 2017 tale om et stigende antal udsatte i forhold til 2014. Ved en beregning af, hvor mange danskere der har været udsat for afpresning inden for de sidste 12 måneder, ender tallet på ca. 7.000. Statistisk usikkerhed betyder, at dette tal kun er et estimat, men det viser, at afpresning finder sted 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. De 8 procent er ganske vist en livstidsprævalens, men der er stadig langt til offerundersøgelsens 0,1 procent. En af forklaringerne kan være registreringseffekter, altså uens formulerede spørgsmål.

I Digitaliseringsstyrelsens og DKCERT's undersøgelse er der blevet spurgt om, hvorvidt respondenten har oplevet, at et program har spærret for adgangen til computer eller data (det kan dreje sig om alle mulige typer malware). Tilføjelsen til spørgsmålet lyder dog således: 'og krævede betaling for at åbne for dem'. Spørgsmålet er, om respondenterne har tolket denne tilføjelse som en afgrænsning til ransomware. I vores offerundersøgelse har vi spurgt om afpresning og anvendt udtrykket ransomware (se bilag 2, spørgsmål 2g).

En supplerende forklaring kan være, at fænomenet ransomware toppede før 2014; det var det første år, hvor spørgsmålet indgik i vores offerundersøgelse. Denne supplerende hypotese finder støtte i Digitaliseringsstyrelsens og DKCERT's undersøgelser. I 2014 fandt de, at 8 procent havde været udsat for ransomware. De tilsvarende tal for 2015 og 2016 var henholdsvis 7 og 8 procent. Det betyder, at der reelt ikke har været en stigning i antallet af ransomware-ramte. Eftersom der er tale om livstidsprævalens, er ransomware de sidste par år tilsyneladende kun forekommet i begrænset omfang.

Det virker overraskende, at ransomware allerede skulle have toppet for nogle år siden. Verden blev således i 2017 ramt af et omfattende ransomware-angreb under navnet WannaCry. 230.000 computere i 99 lande blev inficeret, men kun få blev ramt i Danmark, og angrebet rettede sig primært mod virksomheder.[37]

Sexafpresning så vi kun i meget begrænset omfang i offerundersøgelsen; to respondenter svarede, at de havde været udsat for denne type afpresning. Det tyder på, at fænomenet ikke er ret udbredt i Danmark. Det stemmer 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."[38]

8.4 Nærmere om afpresning

Blandt de 5.996 respondenter i stikprøverne havde seks mænd og fire kvinder været udsat for ransomware eller sexafpresning. Aldersmæssigt var der tale om en bred spredning: Det yngste offer er 19 år, og den ældste 68. Fem af episoderne hørte til kategorien ransomware, mens to handlede om sexafpresning. De tre øvrige respondenter oplyste ikke, hvad de havde været udsat for. To af dem – et offer for ransomware og et offer for sexafpresning – havde overført et beløb; i begge tilfælde 3.500 kr. De andre syv ofre har ikke overført penge. Ingen af sagerne er blevet anmeldt til politiet.

[37] For at sætte de 8 procent fra Digitaliseringsstyrelsens og DKCERT's undersøgelse i perspektiv: 8 procent af den danske befolkning svarer til ca. 350.000 computere, der skulle have været inficeret med ransomware.

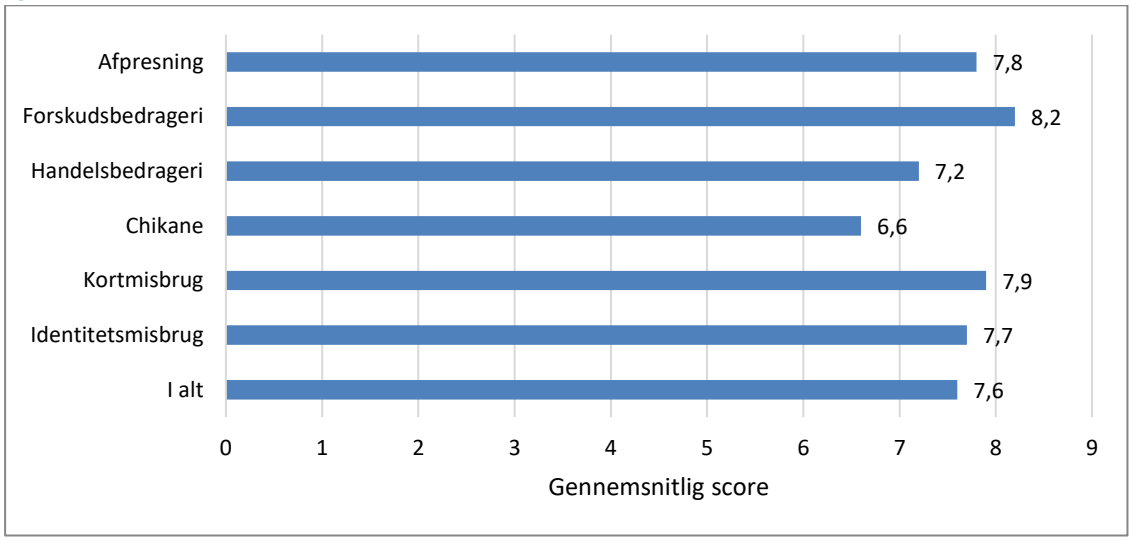
[38] http://www.dr.dk/Nyheder/Indland/2015/01/15/114205.htm

9 Syn på udsathed

I 2017-offerundersøgelsen er de respondenter, der har været udsat for internetkriminalitet, blevet bedt om med et tal at bedømme, hvor grænseoverskridende oplevelsen har været for dem. På skalaen, der går fra 1 til 10, står 1 for ikke-grænseoverskridende og 10 for meget grænseoverskridende.

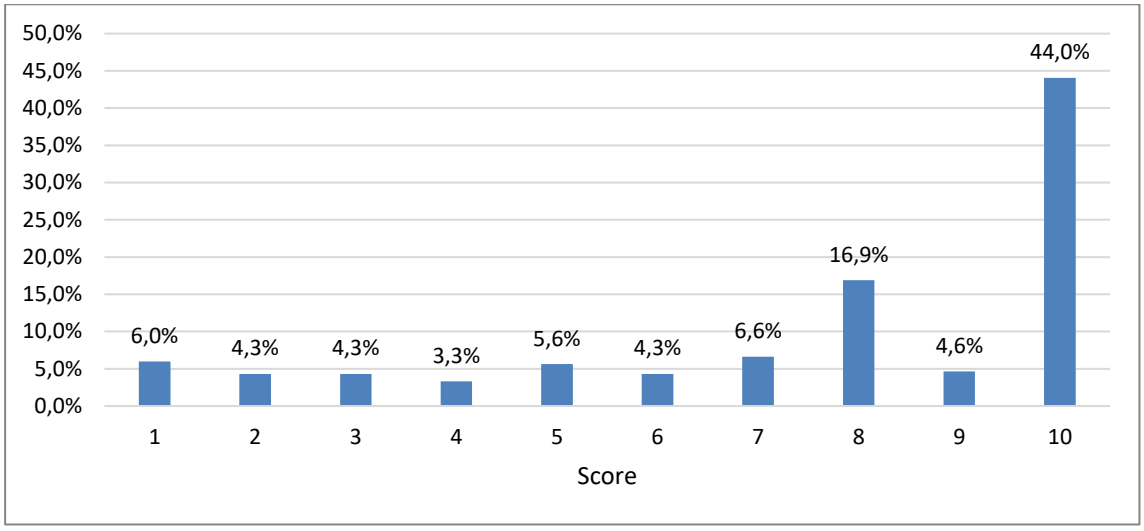
Forventningen var, at respondenterne ville bedømme kortmisbrug som mindre grænseoverskridende end identitetsmisbrug eller chikane, men denne antagelse holdt ikke stik. Figur 9.1 viser således ikke store forskelle ved de forskellige former for internetkriminalitet. Gennemsnitsscoren er 7,6, og samtlige kriminalitetstyper scorer mellem 6,6 og 8,2.

Figur 9.1 Gennemsnitlig score for, hvor grænseoverskridende de forskellige kriminalitetstyper opleves



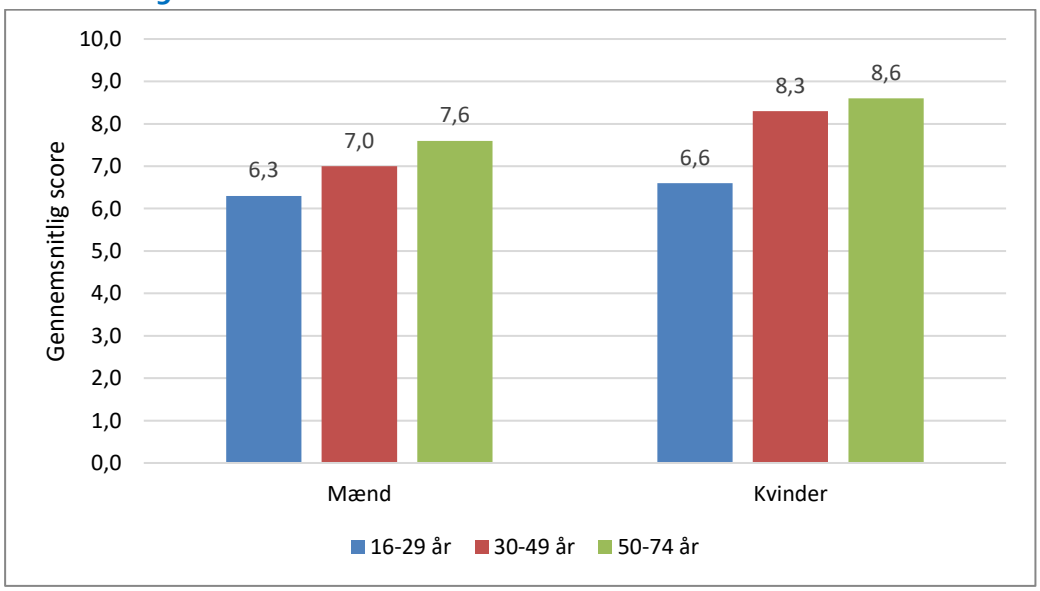
Ser vi på fordelingen af scoren, svarer 44 procent, at oplevelsen har været meget grænseoverskridende (bedømt med et 10-tal). 17 procent svarer med et 8-tal, og resten af bedømmelserne fordeler sig mere eller mindre ligeligt på de øvrige tal. Det betyder, at ca. to tredjedele af respondenterne betragter oplevelsen som stærkt grænseoverskridende (score fra 8 og opefter), mens den for én tredjedels vedkommende har føltes lidt mindre alvorlig (score fra 7 og nedefter).

Figur 9.2 Fordelingen af, hvor grænseoverskridende oplevelsen har været for ofrene (1-10)



Ser vi nærmere på baggrundsvariabler hos respondenterne, viser der sig ikke nævneværdige forskelle. Undtagelser er dog alder og køn. Jo højere alder, jo mere grænseoverskridende bedømmes oplevelsen. Kvinder har desuden en højere gennemsnitlig score end mænd (7,9 versus 7,2).

Figur 9.3 Gennemsnitlig score for, hvor grænseoverskridende oplevelsen har været efter alder og køn



Litteratur

- Boesen Pedersen, Anne-Julie, Britta Kyvsgaard & Flemming Balvig (2017) Udsathed for vold og andre former for kriminalitet 2005-2016. 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.
- Det Kriminalpræventive Råd (2016). Når forbrydelser bliver digitale: En antologi om IT-kriminalitet og adfærd på internettet.
- Digitaliseringsstyrelsen & DKCERT (2017). Danskernes informationssikkerhed 2016.
- DKCERT, Trendrapport, adskillige årgange.
- 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 (2016). Betalingskortmarkedet 2016.
- Kruize, Peter (2009). Identitetstyveri. Københavns Universitet: Det Juridiske Fakultet.
- Kruize, Peter (2013). Kriminalitet i en digitaliseret verden. Københavns Universitet: Det Juridiske Fakultet.
- Kruize, Peter (2014). Internetkriminalitet 2014. Undersøgelse om Identitetstyveri, bedrageri, afpresning og chikane i cyberspace. DKR & Københavns Universitet.
- 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.
- OECD (2009). Online Identity Theft.
- Politi (2017). National Strategisk Analyse 2017.

- Politi (2017). Metoderapport NSA 2017.
- 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.
- Straffelovsrådet (2017). Betænkning om freds- og ærekrænkelser, nr. 1563. Justitsministeriet.
- 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.

Besøgte hjemmesider

- borger.dk
- cert.dk
- dba.dk
- dkr.dk
- dr.dk
- dst.dk
- emaerket.dk
- fdih.dk
- finansdanmark.dk
- ft.dk
- fyens.dk
- guloggratis.dk
- justitsministeriet.dk
- lagen.nu
- lauritz.com
- lovdata.no
- nationalbanken.dk
- nets.eu/dk-da
- politi.dk
- politiken.dk
- retsinformation.dk
- um.dk
- videnskab.dk
- wetten.overheid.nl

Undersøgelsens metode

Bilag 1

Offerundersøgelser er det vigtigste datagrundlag for denne rapport. Der har været fire undersøgelser i henholdsvis 2009, 2013, 2014 og 2017. Spørgeskemaerne for de fire undersøgelser har ikke været identiske, men de er dog sammenlignelige. Denne påstand uddybes i dette bilag. Ellers beskrives her de almene begrænsninger af offerundersøgelser som dataindsamlingsmetode.

Filterspørgsmål i de tre offerundersøgelser

Sammenlignelighed mellem de fire 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 og 2017 kom der yderligere emner til undersøgelsen – forskudsbedrageri og afpresning – og der var et ønske om at opdele identitetstyveri i misbrug af identitetsoplysninger, misbrug af betalingskortoplysninger 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 respondenter. 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 2014/2017 er, at spørgsmålene i 2014/2017 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 2014/2017, 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, 2017, s. 11-12). 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 alene et mindre udsnit af den del af befolkningen, undersøgelsen omfatter, der udspørges. Det betyder, at tallene er forbundet med statistisk stikprøveusikkerhed.

- 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, din profil på Facebook eller delt mod din vilje krænkende billeder af dig), 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 person-oplysninger/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

15. Hvor grænseoverskridende synes du det har været, at din identitet er blevet misbrugt på en skala fra 1 til 10, hvor 1 står for "lige meget" og 10 for "meget invaderende"

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.

16. 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

17. 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

18. 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

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

20. 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

21. 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

22. Hvor grænseoverskridende synes du det har været, at dit betalingskort er blevet misbrugt på en skala fra 1 til 10, hvor 1 står for "lige meget" og 10 for "meget invaderende"

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.

23. 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

24. 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

25. 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

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

27. 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

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

29. Hvor grænseoverskridende synes du det har været, at du er blevet udsat for chikane på en skala fra 1 til 10, hvor 1 står for "lige meget" og 10 for "meget invaderende"

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.

30. 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

31. 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

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

33. 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

34. 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

35. Hvor grænseoverskridende synes du det har været, at du er blevet bedraget på en skala fra 1 til 10, hvor 1 står for "lige meget" og 10 for "meget invaderende"

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.

36. 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

37. 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

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

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

40. Hvor grænseoverskridende synes du det har været, at du er blevet bedraget på en skala fra 1 til 10, hvor 1 står for "lige meget" og 10 for "meget invaderende"

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.

41. 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

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

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

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

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

46. Hvor grænseoverskridende synes du det har været, at du er blevet bedraget på en skala fra 1 til 10, hvor 1 står for "lige meget" og 10 for "meget invaderende"

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.

47. 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

48. 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*)

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

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

51. Hvor grænseoverskridende synes du det har været, at du er blevet afpresset/truet på en skala fra 1 til 10, hvor 1 står for "lige meget" og 10 for "meget invaderende"