POLITI

Temaanalyse om unge og it-kriminalitet i Fyns politikreds

En kortlægning af kriminalitetstyper, ofre og gerningsmænd

Indholdsfortegnelse

Hovedfund

Med denne analyse ønsker vi at afdække, hvilke kriminalitetsformer børn og unge fra 0-24 år er udsat for og begår i det digitale rum. Analysen er udarbejdet på baggrund af 2.166 sager om it-relateret berigelseskriminalitet, 88 sager om seksualforbrydelser og 64 sager om trusler.

Hovedfund vedrørende it-relateret berigelseskriminalitet:

- Fra 2013-2015 er anmeldelserne steget med 59 %, og antallet af ofre er næsten fordoblet fra 2013-2017. Vi ser især flere sager om handelsbedrageri (39 %) og misbrug af betalingskortoplysninger (191 %), hvilket kan skyldes introduktionen af MobilePay i 2013.
- Antallet af sigtede personer er stabilt over årene, med i gennemsnit 34 sigtede pr. år. Omend tallene er små, understøtter resultatet formodningen om, at vi også på dette kriminalitetsområde ser en tendens til, at en stadig mindre gruppe af unge står for en forholdsmæssig stor andel af den samlede ungdomskriminalitet.
- Mere end halvdelen af ofrene (57 %) er bosat i Odense Kommune, men der er registreret ofre i alle kommuner i politikredsen. 65 % af ofrene er mellem 19-24 år, hvilket kan hænge sammen med alderen for, hvornår man erhverver sig et betalingskort, identitetsoplysninger mv., og dermed er sårbar overfor denne kriminalitet.
- 60 % af ofrene har været udsat for handelsbedrageri, hvor de har betalt for en vare, de aldrig har modtaget. Købet er oftest aftalt via Den Blå Avis, Facebook eller Gul & Gratis.
- 21 % af ofrene har været udsat for misbrug af betalingskortoplysninger, og 13 % har været udsat for misbrug af identitetsoplysninger med henblik på økonomisk gevinst. Analysen giver ikke et entydigt svar på, hvordan gerningsmanden tilvejebringer oplysningerne.
- Fyns Politi har rejst sigtelser mod 153 personer fra 0-24 år for it-relateret berigelseskriminalitet. Det Kriminalpræventive Råd påpeger, at disse gerningsmænd ofte er motiveret af de høje profitmulighed, sammenholdt med en lav risiko for at blive opdaget.

Hovedfund vedrørende it-relaterede seksualforbrydelser og trusler

- Antallet af seksualforbrydelser og trusler er meget lav, og vi kan derfor ikke drage konklusioner om udviklingen og tendenser. De få registrerede anmeldelser er bl.a. et udtryk for en lav anmeldelsestilbøjelighed på området.
- 36 ofre har været udsat for at få tilsendt/vist billeder/video af seksuel karakter, mens 16 ofre er blevet kontaktet med henblik på grooming. Gerningsmanden har primært taget kontakt via Snapchat og Messenger, mens Facebook og Skype også er anvendt i få sager.
- 28 ofre har været udsat for trusler på livet, og 14 har været udsat for trusler om vold. Truslerne er primært fremsat via Facebook og Messenger.

Formål

I National Strategisk Analyse 2017 og Offerundersøgelsen om internetkriminalitet fra 2017 understreges det, at it-kriminalitet er et område i vækst. Risikoen for at blive offer for internetrelateret kriminalitet er højest for de 16-29 årige, sammenlignet med andre aldersgrupper (Rigspolitiet 2017a, Kruize 2018).

En landsdækkende ungeprofilundersøgelse blandt unge i alderen 12-25 år finder, at 5 % af de adspurgte unge, har sendt et nøgenbillede/video af andre uden samtykke. 3 % har oplevet, at andre har sendt et nøgenbillede/video af dem uden samtykke, mens 5 % af de unge har begået hacking, cracking[1] eller DDoS-angreb[2]. Derudover har 3 % af de unge svindlet med deres forældres betalingskort og 1 % har svindlet med andres betalingskort (Det Kriminalpræventive Råd 2018).

Efter anmodning fra Odense Kommune har Fyns Politi udarbejdet denne analyse, der har til hensigt at undersøge, hvilke kriminalitetsformer børn og unge i Fyns politikreds er udsat for og begår i det digitale rum, samt hvordan udviklingen har været de seneste fem år. Formålet med analysen er at skabe et vidensgrundlag til brug for en tilpasset fælles forebyggende indsats, med henblik på at undgå, at børn og unge udvikler en digital risikoadfærd, der kan ødelægge deres fremtid. Analysen er begrænset til målgruppen af børn og unge i alderen 0-24 år, i overensstemmelse med kommunernes forebyggende arbejde.

Analysen anvender samme definition af it-kriminalitet, som fremgår af National Strategisk Analyse 2017, hvor it-kriminalitet forstås som traditionel kriminalitet (fx berigelseskriminalitet), der blot er flyttet over på internettet og som kriminalitet, hvor internettet bruges til at dele og videregive tekst, billeder, videoer eller lignende med kriminelt indhold. Internettet muliggør, at gerningsmanden kan nå ud til flere ofre, hurtigere end i de fysiske verden, og samtidig skabes der en distance til offeret, der kan betyde, at gerningsmanden ikke opfatter kriminaliteten ligeså alvorlig eller skadende for offeret, som kriminalitet begået ansigt til ansigt med offeret (Rigspolitiet 2017a).

I overensstemmelse med National Strategisk Analyse 2017 fokuserer denne analyse på at afdække udviklingen indenfor tre hovedområder: *berigelseskriminalitet, trusler* og *seksualforbrydelser*. (Se evt. National Strategisk Analyse, Rigspolitiet 2017a, side 160, for en detaljeret forklaring).

[1] At cracke vil sige at bryde datasikkerheden ved fx en virksomhed eller en institution.

[2] Et DDoS-angreb indebærer en distribueret servicenægtelse og overbelaster så at sige internetserveren, så en hjemmeside eller en blog lukkes ned.

Metode

Analysens datagrundlag er registrerede anmeldelser i POLSAS fra 1. januar 2013 til 31. maj 2018, hvor gerningsmand og/eller offer har bopælsadresse i Fyns politikreds, og er mellem 0-24 år. Således har vi udfundet de sager, hvor offer (i POLSAS registreret som A/F eller FOU) er mellem 0-24 år, *eller* hvor gerningsmanden (i POLSAS registreret som SIG eller U15) er mellem 0-24 år. Dette betyder, at der kan forekomme sager, hvor gerningsmanden eksempelvis er ældre end 24 år, men hvor offeret er i alderen 0-24 år. Omvendt kan der også være sager, hvor offeret er ældre end 24 år, men hvor gerningsmanden er 0-24 år.

For hvert af de tre kriminalitetsområder - *berigelse, trusler og seksualforbrydelser* - har vi søgt på en række tilhørende gerningskoder og specifikke søgeord i sagens resumefelt. Vi har taget udgangspunkt i de søgeord (se nedenstående), som er anvendt i National Strategisk Analyse 2017, men suppleret disse med yderligere søgeord, som vurderes relevante for Fyns Politi. De ekstra tilføjede søgeord er angivet med grønt.

Søgeord til berigelseskriminalitet

Gul & gratis, gul og gratis, dba, den blå avis, qxl, reshopper, re shopper, .dk, .com, .net, .uk, face book, facebook, mail, mails, linkedIn, linked in, app, appen, nigeriabrev, nigeria brev, romance scam, scam, Nigeria, kroner, kr. kr, penge, beløb, dollar, euro, abonnement, tab, snapchat, snap chat, skype, messenger, internet, nethandel, trendsale, nettet, ebay, online, paypal, instagram, phising.

Søgeord til seksualforbrydelser

.dk, .com, .net, .uk, face book, facebook, mail, mails, linkedin, youtube, you tube, Instagram, insta gram, Arto, twitter, scor.dk, snapchat, snap chat, skype, datingside, dating side, momio, moviestarplanet, ask.fm, messenger, whatsapp, whats app, tinder, datingsite, dating site, dating.dk, match.com, firstdate.com, single.dk, grooming, sextortion, sex tor-tion, app, appen, linkedIn.

Søgeord til trusler

.dk, .com, .net, .uk, mail, mails, youtube, you tube, Instagram, Arto, twitter, snap-chat, snap chat, skype, momio, moviestarplanet, ask.fm, messenger, whatsapp, whats app, tinder, sextortion, sex tortion, face book, facebook, linkedin, ransomware, ransom ware, DDOS, malwaremal ware, virus, spyware, spy ware, bitcoin, bit coin, windows, scam, ro-mance scam, romancescam,
app, appen, LinkedIn.

Kodning og analyse

Søgningen afstedkom i alt 88 sager om trusler, hvoraf 64 trusler var it-relaterede. Derudover afstedkom søgningen 110 sager om seksualforbrydelser, hvoraf 88 sager var relevante og 2.625

sager om berigelseskriminalitet, hvoraf 2.166 var relevante for denne analyse i forhold til definitionen af it-kriminalitet, som tidligere beskrevet.

Efter fremsøgning blev alle sager kodet i Excel og efterfølgende behandlet ved brug af Qlikview. Kodningen er foregået ved brug af resumefeltet. For at sikre en konsistens i kodningen har vi udarbejdet en kodemanual, som blev testet flere gange, således at eventuelle uenigheder og misforståelser blev drøftet og tilrettet. Som nævnt blev flere sager frasorteret, hvis de faldt udenfor definitionen af it-kriminalitet. I analysen har vi anvendt deskriptiv statistik.

Serieforbrydelser
Inden for berigelseskriminalitet er der flere tilfælde, hvor én gerningsmand er ansvarlig for større sagskomplekser. Eksempelvis fordi vedkommende har misbrugt samme kreditkort, kundekort, spilkonti eller lignende flere gange. Det er netop en af konsekvenserne ved den teknologiske udvikling - at gerningsmænd på grund af it har mulighed for at øge volumen af deres kriminalitet (Rigspolitiet 2017a). I denne analyse kalder vi disse forhold for serieforbrydelser.

I Fyns Politi er der sket en ændring i registreringspraksis på området, hvor Fyns Politi i højere grad end tidligere registrerer sådanne serieforbrydelser som flere unikke forhold/sager, frem for som ét enkelt sagskompleks. Dette kan skævvride billedet af udviklingen, så stigningstendensen fremstår større end reelt. For at tage højde herfor har vi gennemgået datasættet for serieforbrydelser, således at et sagskompleks med flere registrerede unikke sager, tilhørende samme gerningsmand, kun kan tælle for én sag i vores analyse, frem for eksempelvis 20 sager. Vi har kun korrigeret herfor i de tilfælde, hvor gerningsmanden var sigtet for 10 eller flere sager. Dette gjorde sig gældende for 35 unikke gerningsmænd. På den måde har vi forsøgt at tage højde for den ændrede registreringspraksis i Fyns politi, så vi kan give et mere reelt billede af udviklingen. Når vi korrigerer for serieforbrydelser falder antallet af anmeldelser om it-relateret berigelseskriminalitet fra 2.166 sager til 1.485 sager.

Det er vigtigt at understrege, at denne korrektion for serieforbrydelser alene anvendes, når vi analyserer *antallet af anmeldelser*. Når vi ser på *antallet af ofre og gerningsmænd* tæller alle unikke individer med i analysen, og alle de oprindelige informationer omkring fx alder og køn indgår derfor i analysen.

Metodiske forbehold
Metoden, som er anvendt i analysen, har en række usikkerheder, da der er tale om en søgning på ord, som kan optræde i mange forskellige sammenhænge. Der kan være andre søgeord, der er relevante, end de der er anvendt her. Eller der kan være relevante sager, som ikke indeholder en dækkende beskrivelse i sagens resuméfelt, og som derfor ikke opdages ved hjælp af denne søgemetode. Metoden kan derfor bruges til at undersøge udviklingstendensen indenfor området, men ikke til at angive et absolut anmeldelsestal på området (Rigspolitiet 2017b).

Mørketal

En helt central usikkerhed forbundet med vores analyse og datagrundlag er mørketal. En Offerundersøgelse fra 2017 peger på, at det kun er omkring en tredjedel af sagerne vedrørende internetrelateret kriminalitet, der bliver politianmeldt (Kruize 2018). Vi vurderer, at dette mørketal også gør sig gældende for de 0-24årige, hvilket naturligvis skaber en usikkerhed om vores resultater. Som supplement til vores politiregistreringer inddrager vi derfor andre relevante undersøgelser løbende i analysen.

Ordliste

- **Handelsbedrageri** defineres som bedrageri ved køb og salg af varer på internettet.
- **Misbrug af betalingskortoplysninger** er bedrageri, hvor gerningsmanden har tilegnet sig ofrets betalingskortoplysninger og efterfølgende brugt disse til at opnå en økonomisk gevinst fx oprettelse af abonnementer, køb af varer på nettet, kontooverførsler, MobilePay-overførsler mv. I analysen inddrages kun tilfælde, hvor oplysningerne er stjålet/franarret ved brug af it, *eller* hvor det efterfølgende misbrug er sket ved brug af it. I tilfælde hvor betalingskortoplysningerne er stjålet i den fysiske verden (fx i en butik, ved pinkodealuring eller lignende), og hvor oplysningerne efterfølgende er blevet anvendt fysisk (fx til at hæve penge i en automat eller købe en vare i en butik), er sagen frasorteret.
- **Misbrug af identitetsoplysninger med henblik på økonomisk gevinst** er bedrageri, hvor ofrets identitetsoplysninger (fx CPR nr., navn, e-postadresser, konti på sociale medier, telefon/telefonnumre og NemID) stjæles eller franarres af en gerningsmand, som efterfølgende misbruger disse til at opnå en økonomisk gevinst uden ofrets vidende eller accept.
- **Misbrug af identitetsoplysninger med henblik på chikane af offeret** er bedrageri, hvor ofrets identitetsoplysninger stjæles eller franarres af en gerningsmand, der misbruger disse for at chikanere offeret.
- **Afpresning ved ransomeware** er i denne analyse afgrænset til afpresning af privatpersoner. Ransomware er en sammentrækning af ordene ransom (løsesum) og software. Ransomware er en type malware, der er i stand til at spærre en device. Offeret får besked om at betale en løsesum for atter at få adgang til programmer og/eller data på mobiltelefon, tablet eller pc.
- **Svindel med udlejningslejligheder** er bedrageri, hvor gerningsmanden udlejer en lejlighed, som han ikke har råderet over eller som ikke eksisterer, med henblik på at opnå en økonomiske gevinst (fx depositum). Vi inddrager kun sager, hvor kontakten mellem gerningsmand og lejer er sket online.
- **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 (fx en lotterigevinst, en arv fra et ukendt familiemedlem, et godt forretningstilbud eller et større beløb som tak for, at man har hjulpet en person). Svindlen består i, at offeret aldrig modtager den lovede gevinst, men derimod blot mister de penge, vedkommende har overført.

Kilde: *Når forbrydelser bliver digitale* (DKR 2016) og *Internet Kriminalitet 2017* (Kruize 2018).

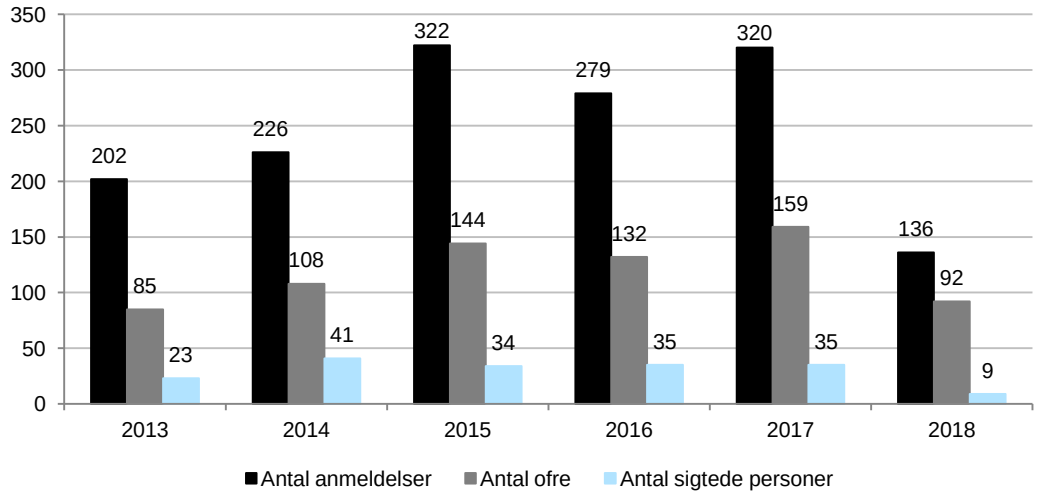
Udvikling indenfor it-kriminalitet

I dette afsnit vil vi undersøge, hvorvidt der er sket en stigning i it-kriminalitet i Fyns politikreds, hvor offer og/eller gerningsmand var mellem 0-24 år på gerningstidspunktet. For at kortlægge dette ser vi både på antallet af anmeldelser, ofre og gerningsmænd fra 2013 til 31. maj 2018.

Berigelseskriminalitet

Indledningsvist retter vi med figur 1 fokus på udviklingen indenfor it-relateret berigelseskriminalitet, som sagsmæssigt fylder mere i statistikkerne, end trusler og seksualforbrydelser.

Figur 1: Udvikling i anmeldelser, ofre og gerningsmænd til berigelseskriminalitet, fra 2013 til 31. maj 2018



Kilde: POLSAS data trukket d. 31.05.18

Figur 1 viser, at der har været en stigning i antallet af anmeldelser om it-relateret berigelseskriminalitet, hvor enten offer eller gerningsmand har været mellem 0-24 år på gerningstidspunktet. Således er udviklingen gået fra 202 sager i 2013 til 226 sager i 2014 og 322 sager i 2015. Dette svarer til en stigning på 59 %. Siden 2015 har antallet af anmeldelser været mere stabilt, og det foreløbige tal for maj 2018 tyder på, at vi ender på niveau med 2017. Bemærk at disse tal er korrigeret for serieforbrydelser (se metode for en uddybning).

Data viser, at stigningen primært kan tilskrives flere sager om handelsbedrageri, som er steget fra 135 sager i 2013 til 188 sager i 2015 (39 % stigning), samt flere sager om misbrug af betalingskortoplysninger, som er steget fra 32 sager i 2013 til 93 sager i 2015 (191 % stigning). En af forklaringerne på stigningen i netop disse år kan være introduktionen af app'en MobilePay. App'en blev indført i maj 2013, og er efterfølgende blevet udbredt massivt blandt danskerne samtidig med, at beløbsgrænsen for, hvor meget man kan sende og modtage, er blevet hævet (Danmarks Nationalbank 2017).

Mens MobilePay kun blev anvendt som betalingsmetode i 3 sager om handelsbedrageri i 2013, blev app'en anvendt i hele 59 sager om handelsbedrageri i 2015. På samme måde viser vores kodning, at gerningsmanden brugte MobilePay til at foretage ulovlige kontooverførsler (misbrug af betalingskortoplysninger) i 4 sager i 2013, mens tallet steg til 22 sager i 2015.

Retter vi fokus på antallet af ofre viser figur 1, at der i overensstemmelse med udviklingen i anmeldelserne også har været en stigning. Fra 2013 til 2017 er antallet af ofre i alderen 0-24 år således næsten fordoblet (47 %). Derimod viser figuren, at antallet af sigtede personer er forholdsvis stabilt over årene, med et udsving fra 23 sigtede i 2013, til 41 sigtede i 2014 og 34-35 sigtede i de efterfølgende år. Eftersom antallet af sigtede personer påvirkes af mange faktorer, herunder opdagelsesrisiko ved den pågældende kriminalitet, politiets mulighed for at efterforske og opklare sagerne osv., er det vanskeligt at give en præcis forklaring på, hvorfor vi ser et stabilt antal af sigtede personer over årene. Sammenholdt med, at vi i samme periode ser en stigning i såvel antallet af sager og ofre er det nærliggende at trække på Flemming Balvigs (2017) ungdomsundersøgelse, der viser, at en stadig mindre gruppe af børn og unge i Danmark begår relativt meget kriminalitet og står for en forholdsmæssig stor andel af den samlede ungdomskriminalitet. Opklaringsprocenten[3] i Fyns Politi er, i forhold til disse sager, nogenlunde stabil i undersøgelsesperioden, og det tyder således ikke på, at det stabile antal sigtede personer alene kan tilskrives ændringer i politiets indsats på området. Derimod underbygger det formodningen om, at tallene (om end de er meget små), kan være et udtryk for den mere generelle tendens omkring unges kriminelle adfærd, som Balvig beskriver den.

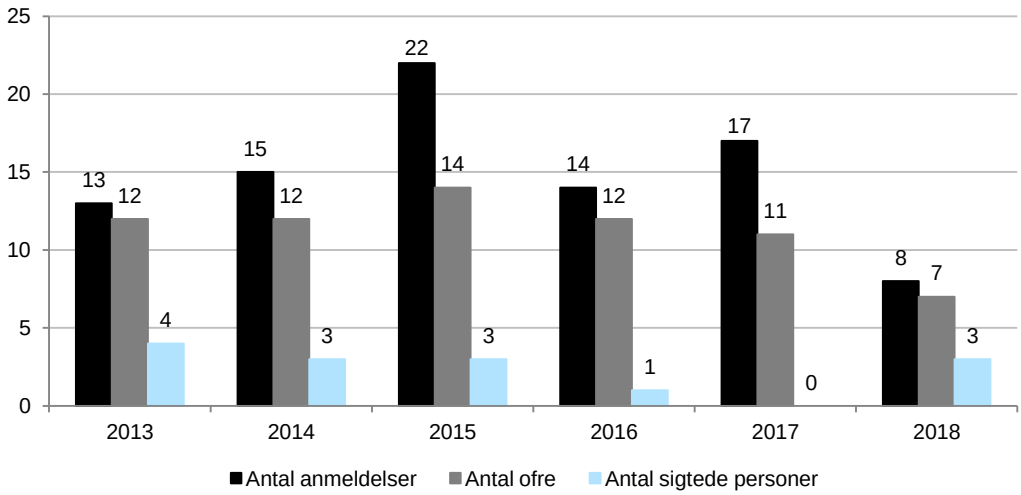
En analyse om unges kriminelle adfærd på nettet fra Det Kriminalpræventive Råd konkluderer desuden, at "når kriminaliteten bevæger sig online" betyder det ikke nødvendigvis, at flere unge bliver kriminelle. I mange tilfælde er det de samme unge, som er gerningsmænd til online og offline kriminalitet. Undersøgelsen viser, at disse unge er præget af en dårligere trivsel og en lavere selvkontrol (Det Kriminalpræventive Råd 2018).

[3] Opklaringsprocenten er et udtryk for, i hvor mange af sagerne det har været muligt at sigte en person.

Seksualforbrydelser og trusler

Figur 2 viser antallet af it-relaterede seksualforbrydelser, ofre og gerningsmænd i undersøgelsesperioden.

Figur 2: Udvikling i anmeldelser, ofre og gerningsmænd til seksualforbrydelser, fra 2013 til 31. maj 2018



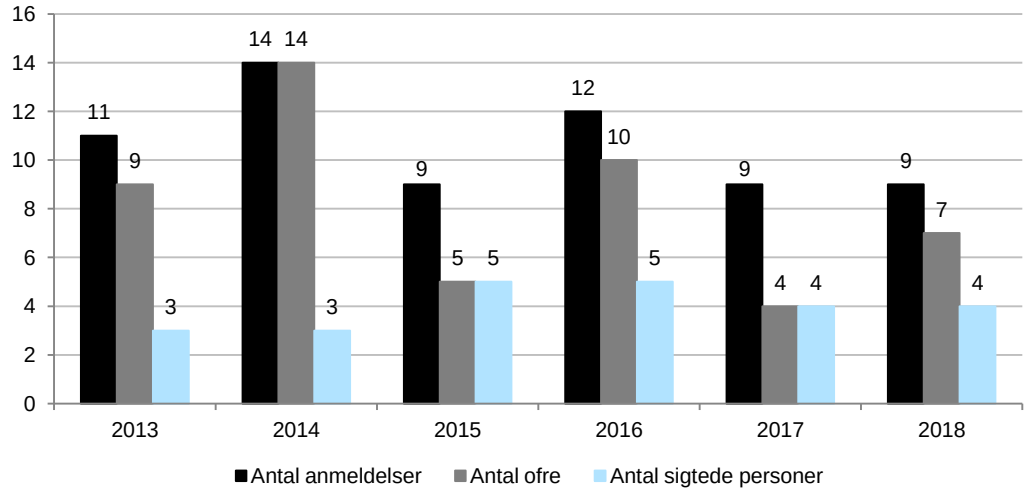
Kilde: POLSAS data trukket d. 31.05.18

Da der er tale om meget små tal i forhold til såvel antallet af sager, ofre og gerningsmænd, kan vi ikke drage egentlige konklusioner omkring udviklingen på området ud fra Fyns Politis data. De små tal er som tidligere nævnt mere et udtryk for en lav anmeldelsestilbøjelighed på området, end et udtryk for, at kriminaliteten ikke er udbredt. Dette understreges blandt andet af Umbrellasagen, hvor mere end 1.000 unge blev sigtet for at have delt sexvideoer af børnepornografisk karakter gennem Facebook-appen Messenger (Berlingske 2018). Vores gennemgang af sagerne efterlader et indtryk af, at seksualforbrydelserne oftere anmeldes, når forældre opdager forbrydelsen. Det kan indikere, at der er mange sager, hvor forældre eller pårørende ikke opdager forholdet, hvorfor det aldrig bliver anmeldt til politiet.

På trods af det begrænsede antal sager er seksualforbrydelser forbundet med store fysiske og psykologiske skadesvirkninger for ofrene. De alvorligste og længstvarende psykologiske eftervirkninger forekommer i de tilfælde, hvor forurettede er ung og bliver udsat for overgreb fra en tilknytningsperson, som hun/han forventer en tryghed og omsorg fra (Oldrup mfl. 2016).

Figur 3 viser antallet af it-relaterede trusler, herunder ofre og gerningsmænd i undersøgelsesperioden.

Figur 3: Udvikling i anmeldelser, ofre og gerningsmænd til trusler, fra 2013 til 31. maj 2018



Kilde: POLSAS data trukket d. 31.05.18

I lighed med seksualforbrydelser er der tale om meget få sager, ofre og gerningsmænd vedrørende it-relaterede trusler, og vi kan derfor heller ikke drage konklusioner omkring udviklingen inden for denne kriminalitetsform ud fra Fyns Politis data. På landsplan finder Rigspolitiet dog en signifikant stigning fra 2013 og frem (Rigspolitiet 2017a).

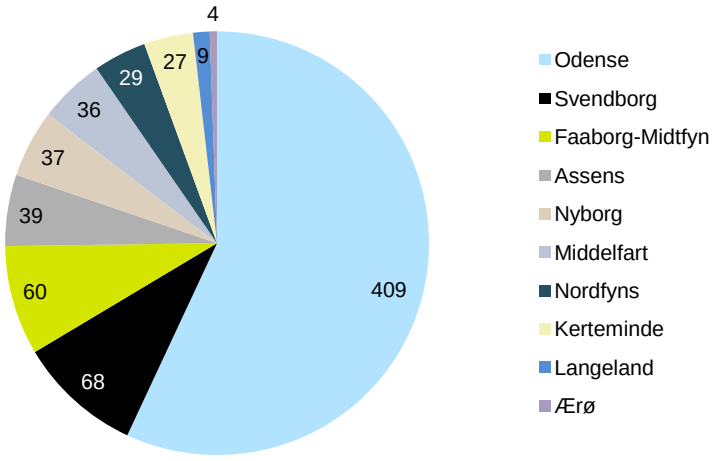
Hvem er ofrene og hvad bliver de udsat for?

I dette afsnit vil vi kortlægge, hvad der karakteriserer dé børn og unge, der har været udsat for berigelseskriminalitet, og herunder give en beskrivelse af hvilke former for it-kriminalitet, de har været udsat for.

Ofre for berigelseskriminalitet

Over hele perioden er der i alt registreret 716 unikke ofre for berigelseskriminalitet. Figur 4 viser fordelingen af ofrene efter bopælskommune.

Figur 4: Ofre fordelt efter bopælskommune, fra 2013 til 31. maj 2018



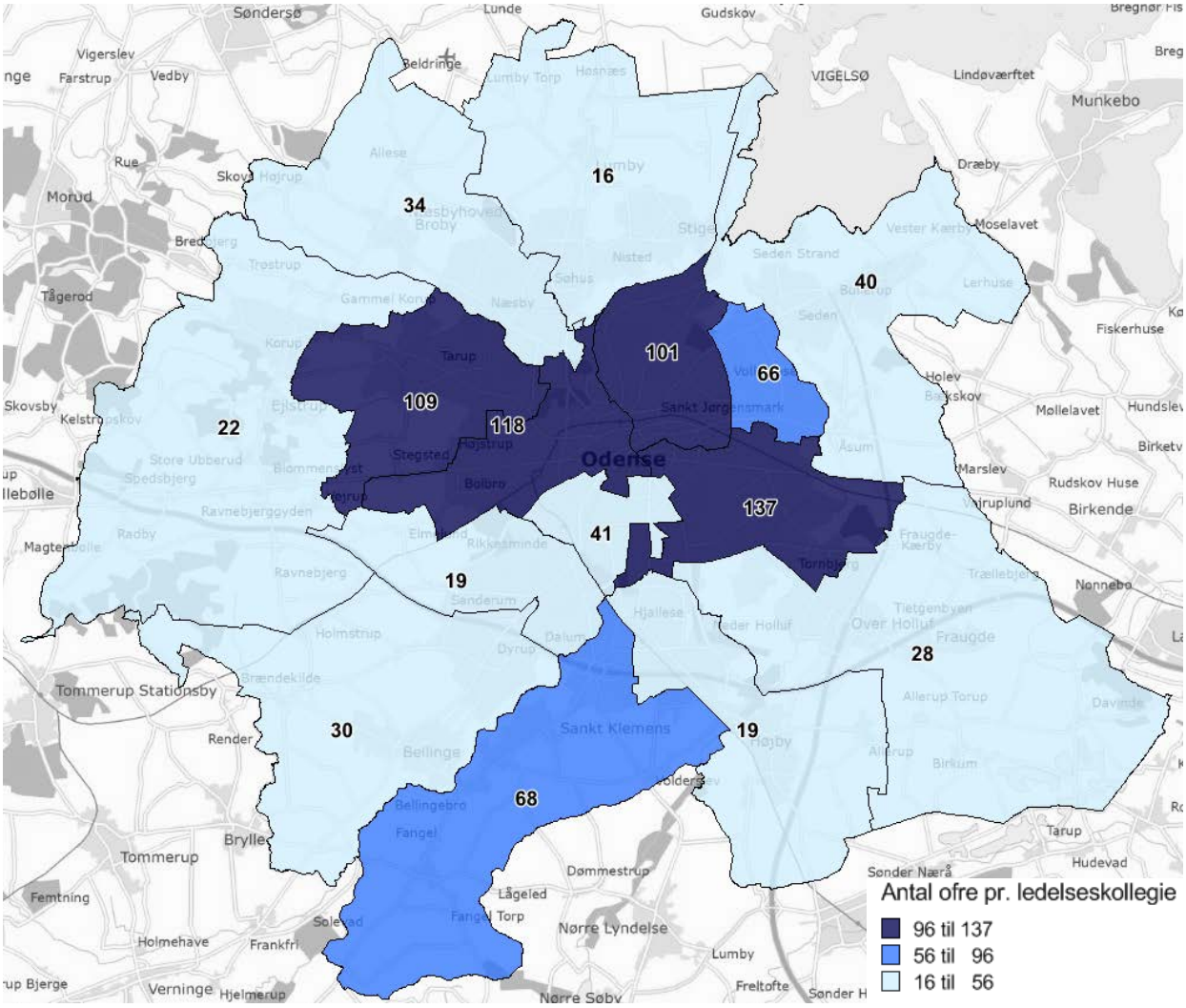
Kilde: POLSAS data trukket d. 31.05.18

Mere end halvdelen af de unge ofre for it-relateret berigelseskriminalitet, med bopælskommune i Fyns politikreds, bor i Odense Kommune (57 %). Dette er forventeligt, eftersom der generelt er bosat flere unge i alderen 0-24 år i Odense, sammenlignet med de øvrige kommuner i politikredsen[4]. Derudover viser figur 4, at der er børn og unge i alle kommuner i politikredsen, der har været ofre for berigelseskriminalitet på nettet. Dette understreger, at it-kriminaliteten rammer bredt, og i modsætning til traditionel kriminalitet ikke er geografisk forankret.

På grund af det høje antal ofre med bopæl i Odense Kommune har det været muligt at udarbejde et mere detaljeret kort, der viser fordelingen af ofrenes bopæl efter ledelseskollegier – som er en opdelingen af institutioner og skoler i Odense Kommune.

[4] Antal unge i alderen 0-24 år på kommune: Assens: 11.376, Faaborg-Midtfyns: 13.894, Kerteminde: 6.253, Langeland: 2.495, Middelfart: 10.531, Nordfyns: 7.971, Nyborg: 8.688, Odense: 65.458, Svendborg: 16.423, Ærø: 1.218. Kilde: Danmarks Statistik, Statistikbanken, tabel FOLK1A

Kort 1: Kort over ofrenes bopæl i Odense Kommune, fordelt efter ledelseskollegier, fra 2013 til 31. maj 2018

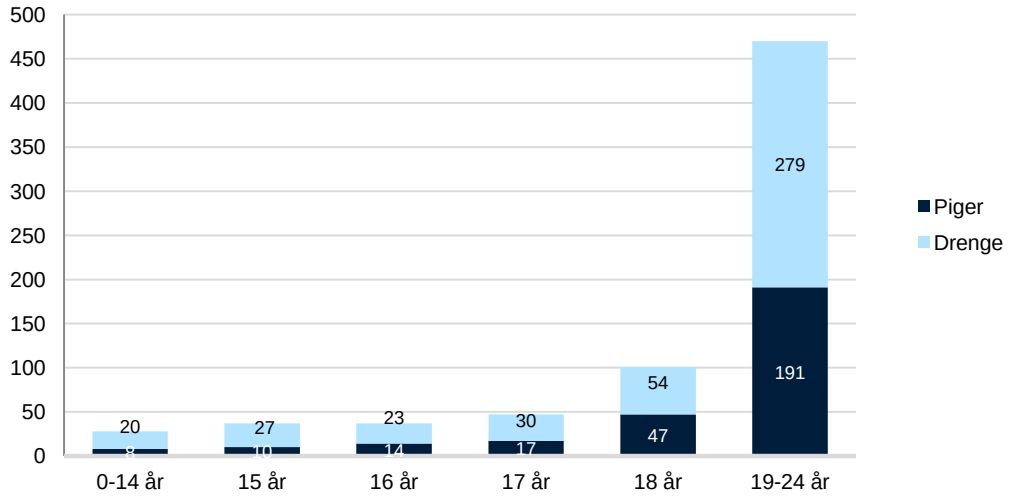


Kilde: POLSAS data trukket d. 31.05.18. Kort udarbejdet i MapInfo, hvor intervaller er opdelt med lige store intervaller.

Kortet viser, at ofrene geografisk set er bosat i hele kommunen, om end der ses en koncentration af ofre i bymidten, hvor befolkningstætheden ligeledes er højere. I de mørkeblå områder har der været bosat mellem 96-137 ofre i undersøgelsesperioden (se konkret antal på kortet).

Figur 5 viser fordelingen af ofre efter alder og køn. Det skal påpeges, at opdelingen i aldersgrupper er sket på forespørgsel fra Odense Kommune, da disse grupperinger generelt anvendes i det forebyggende arbejde. Bemærk, at aldersgruppen 0-14 år og 19-24 år naturligt vil være større end de grupper, der alene repræsenterer en specifik alder, fx 15 år. Dette skal holdes in mente, når figur 5 (og øvrige figurer over aldersfordelingen) læses.

Figur 5: Ofre fordelt efter alder og køn, fra 2013 til 31. maj 2018

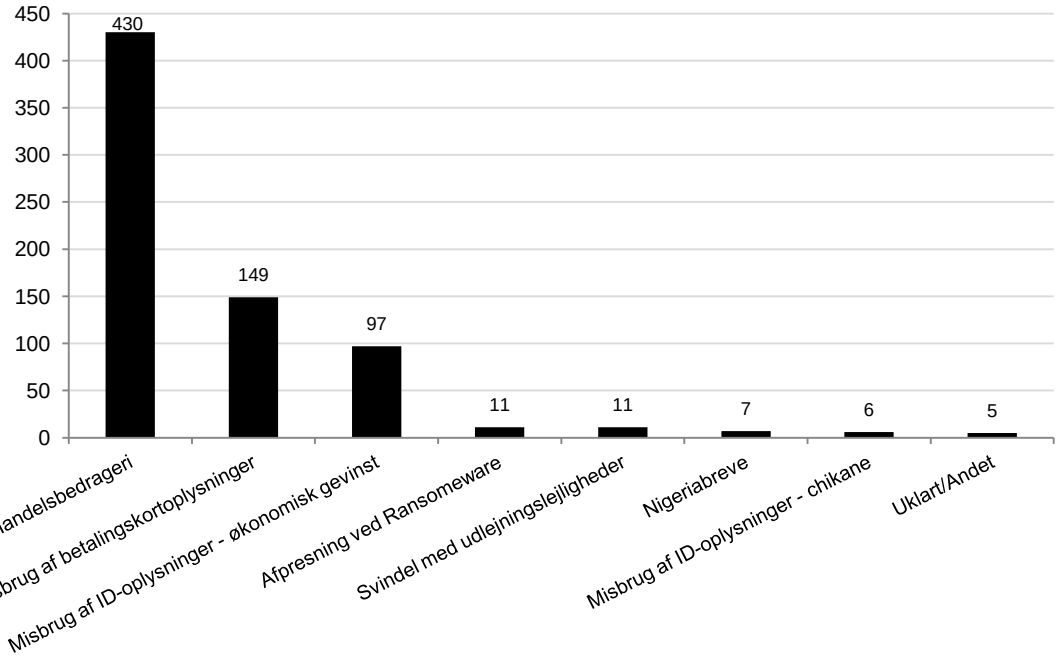


Kilde: POLSAS data trukket d. 31.05.18

Langt hovedparten af ofrene (65 %) er i alderen 19-24 år, og dernæst følger de 18 årige (14 %). Derudover viser figur 5, at der er en svag overvægt af drenge blandt ofrene til berigelseskriminalitet på nettet, uanset hvilken aldersgruppe, der er tale om. Sammenlagt udgør drengene 60 % af ofrene. Hovedparten af ofrene (91 %) har dansk statsborgerskab, mens de øvrige fordeler sig på 31 forskellige nationaliteter.

Figur 6 viser, hvilke former for it-relateret berigelseskriminalitet, som ofrene har været udsat for. For en uddybning af de enkelte kriminalitetsformer henvises til ordlisten i metodeafsnittet og til de kvalitative cases 1-3.

Figur 6: Ofre fordelt efter typer af it-relateret berigelseskriminalitet, fra 2013 til 31. maj 2018



Kilde: POLSAS data trukket d. 31.05.18

Figur 6 viser, at de 0-24 årige i Fyns politikreds hyppigst har været ofre for *handelsbedrageri*. Således har 430 personer, hvilket svarer til cirka 60 % af ofrene, været udsat herfor i undersøgelsesperioden. Dernæst følger kriminalitetstypen *misbrug af betalingskortoplysninger*, hvilket 149 børn og unge har været udsat for i perioden (21 %), og *misbrug af identitetsoplysninger med henblik på økonomisk gevinst*, hvilket 97 børn og unge har været ofre for (13 %).

Uanset hvilken aldersgruppe, vi ser på, er handelsbedrageri dén kriminalitetsform, som flest ofre har været udsat for. Der er dog en mindre variation i data, da ofrene i aldersgrupperne 0-14 år, 15 år, 16 år og 17 år primært er udsat for denne form for bedrageri, mens ofrene fra 18 år og op efter i højere grad er udsat for de andre former for bedrageri, herunder misbrug af betalingskortoplysninger og identitetsoplysninger[5]. Dette hænger formentligt sammen med alderen for, hvornår man erhverver sig et betalingskort og dokumentation for identitetsoplysninger. Eksempelvis kan det formodes, at forældre administrerer de unges identitetsoplysninger i alderen 0-14 år, men at de unge – når de bliver ældre - i højere grad vil får ansvaret for dette.

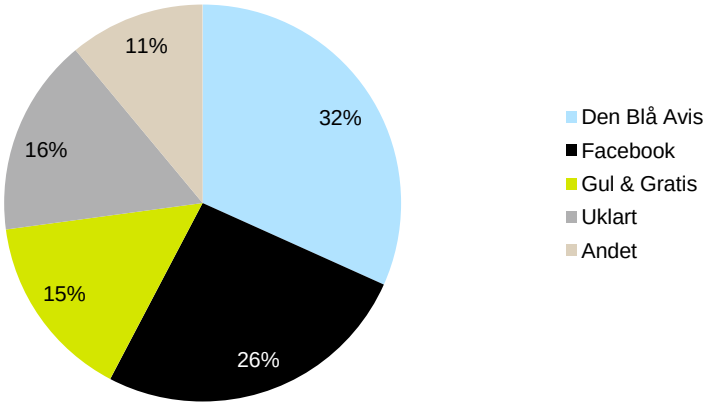
[5] Som nævnt er der blandt alle ofrene 60 %, der har været udsat for handelsbedrageri. Opdelt på de forskellige aldersgrupper er andelene: 79 % af de 0-14årige, 84 % af de 15årige, 73 % af de 16årige, 81 % af de 17årige, 48 % af de 18årige og 57 % af de 19-24årige.

I nedenstående vil vi uddybe karakteristika ved disse tre hyppigst forekomne kriminalitetsformer.

Handelsbedrageri

Handelsbedrageri er kendetegnet ved, at gerningsmanden opnår en form for økonomisk gevinst ved at svindle i forbindelse med en handel på internettet – se fx case 1. Figur 7 viser, på hvilke platforme handelsbedrageriet hyppigst er forekommet.

Figur 7: Ofre fordelt efter hvilken platform, de har oplevet handelsbedrageri. Opgjort i procent. Fra 2013 til 31. maj 2018



Kilde: POLSAS data trukket d. 31.05.18

32 % af ofrene er blevet snydt i forbindelse med en handel på Den Blå Avis, mens 26 % af ofrene er blevet snydt i forbindelse med en handel på Facebook. Derudover er 15 % af ofrene blevet snydt i forbindelse med en handel på Gul & Gratis. I de resterende tilfælde har det været uklart, hvor henne handlen er foregået - det er blot oplyst, at det er på internettet, og derudover er der en række tilfælde med enkeltstående eller få sager relateret til diverse internetsider. Tabel 1 viser, på hvilken måde ofret hyppigst er blevet bedraget (modus).

Tabel 1: Ofre fordelt efter modus for bedrageri. Opgjort i procent. Fra 2013 til 31. maj 2018

Modus	Andel af ofrene
Payment no delivery: Offeret har betalt for en vare, men aldrig modtaget denne.	92%
Delivery no payment: Offeret har sendt en vare, men aldrig modtaget betaling for denne.	5%
Payment wrong/fake delivery: Offeret har betalt for en vare, men modtaget en forkert eller falsk vare.	3%

Kilde: POLSAS data trukket d. 31.05.18

Hovedparten af ofrene (92 %) er blevet bedraget ved, at de har betalt for en vare, som de aldrig har modtaget. Dette betegner vi ”payment no delivery”. Lidt mere end halvdelen af disse ofre (55 %) har overført pengene til gerningsmanden via en kontooverførsel, mens knap en tredjedel (30 %) har overført pengene til gerningsmanden via MobilePay. Det omvendte forhold, hvor offeret

har en vare til salg, som gerningsmanden foregiver at ville købe, men som gerningsmanden aldrig betaler penge for, kalder vi ”delivery no payment”. Tabel 1 viser, at det kun er 5 % af ofrene for handelsbedrageri, der er blevet udsat herfor. Ingen af ofrene for handelsbedrageri har (så vidt det fremgår af resumefeltet) en relation til deres gerningsmand – der er derimod tale om en ukendt person.

Case 1: Handelsbedrageri - payment no delivery

Maria har fundet en billig Iphone 6S på Den Blå Avis, og den ser helt ny ud. Efter aftale overfører hun 3.000 kr. via MobilePay til Torben, som har lovet at sende telefonen hurtigst muligt. Efter tre uger har Maria stadig ikke modtaget telefonen, og hun kan ikke længere finde Torbens profil på Den Blå Avis. Maria beslutter sig for at anmelde sagen til politiet.

Misbrug af betalingskortoplysninger

Misbrug af betalingskortoplysninger omhandler tilfælde, hvor gerningsmanden på en eller anden måde har tilvejebragt offerets betalingskortoplysninger, og efterfølgende misbrugt disse. I kodningen har vi kun inddraget de sager, hvor betalingskortoplysninger er stjålet eller franarret ved brug af it, *eller* hvor det efterfølgende misbrug er sket ved brug af it. Bemærk, at vi har anlagt en bred definition på it, da apps som MobilePay også inddrages, fx i tilfælde hvor betalingskortoplysningerne er misbrugt til at foretage en MobilePay overførsel til gerningsmandens egen konto, eller hvor gerningsmanden har fået adgang til offerets MobilePay konto og ad denne vej har overført penge til sig selv.

Generelt er det vanskeligt at udlede af sagernes resuméfelt, hvordan de unge mister deres betalingskortoplysninger. Ud af de i alt 149 ofre for misbrug med betalingskortoplysninger har 31 ofre fået deres betalingskort/betalingskortoplysninger stjålet eller franarret i den fysiske verden, mens 23 ofre har været udsat for, at gerningsmanden har skaffet sig adgang til deres MobilePay konto. Eksempelvis kan telefonen have været stjålet, eller gerningsmanden kan have snydt sig adgang ved at lade som om, at han var en fremmed i pengenød. Derudover har Fyns Politi kendskab til ”falske” anmeldelser om misbrug af MobilePay eller sager hvor ofret i større eller mindre grad har givet sin accept til misbruget. For hele 74 ofre for betalingskortmisbrug har det ikke været muligt at kortlægge, hvordan betalingskortoplysningerne er blevet mistet.

Hovedparten af ofrene har ikke kendt deres gerningsmand forud for det kriminelle forhold. Det er kun 15 personer, der har haft en eller anden relation til deres gerningsmand, eksempelvis et familiemedlem eller en ekskæreste.

Case 2: Misbrug af betalingskortoplysninger

Allan står i Netto og skal til at betale, da han opdager, at hans kort er spærret. Han ringer til sin bank og finder ud af, at hans kortoplysninger er blevet misbrugt til forskellige køb på nettet for tusindvis af kroner, hvorfor banken har spærret hans kort. Allan har en formodning om, at hans kortoplysninger er blevet stjålet, da han købte billig hundemad på internettet.

Misbrug af identitetsoplysninger med henblik på økonomisk gevinst

Den sidste form for kriminalitet, der fylder i opgørelsen over it-relateret berigelseskriminalitet jf. figur 6, er misbrug af identitetsoplysninger med henblik på økonomisk gevinst. På samme måde som ved misbrug af betalingskortoplysninger er hensigten for gerningsmanden at tilegne sig en eller anden form for økonomisk gevinst (fx køb af varer, oprettelse af abonnement mv.), men her er det blot offerets identitetsoplysninger (fx CPR. nr., navn, mail, Nem ID), der misbruges.

I disse sager har det på baggrund af den gennemførte kodning ikke været muligt yderligere at konkretisere, hvordan de unge mister deres identitetsoplysninger. Således er dette uklart for 64 ud af de 97 ofre. Dette kan skyldes, at det ikke fremgår af resumefeltet, da det først "opklares" senere i sagsforløbet, men erfaringen fra Fyns Politi er også, at det generelt er svært for offeret at gennemskue, præcis hvornår eller hvordan, de har mistet oplysningerne. Rigspolitiet peger på, at identitetstyveri blandt andet kan ske ved, at ofret modtager et link på sin mobil, hvorefter vedkommende klikker på linket og derefter uploader sine bankoplysninger, et billede af NemID eller lignende, idet gerningsmanden udgiver sig for at være forurettedes bank (Rigspolitiet 2017a).

Case 3: Misbrug af identitetsoplysninger med henblik på økonomisk gevinst

Michael modtager en dag flere rykkere fra kreditorer og banker med posten. Han kender intet til regningerne og det viser sig, at en fremmed person har brugt hans personnummer til at oprette flere lån og mobilabonnementer på internettet. Michael har ikke givet sit personnummer til nogen og finder derfor aldrig ud af, hvordan han er blevet bedraget.

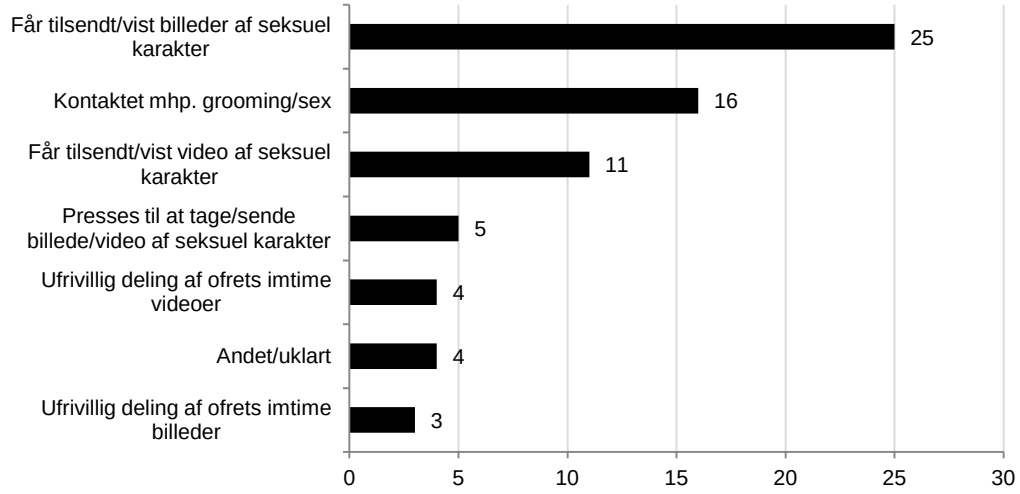
Ofre for seksualforbrydelser

Fra 2013 til 31. maj 2018 er der i alt registreret 67 unikke ofre for it-relaterede seksualforbrydelser i Fyns Politi. Det lave antal af politiregistrerede ofre, sammenholdt med de tidligere omtalte selvrapporterede offerundersøgelser (Det Kriminalpræventive Råd 2018), understreger den lave anmeldelsestilbøjelighed på området. De små tal betyder, at denne analyses fund ikke er repræsentative eller kan anvendes som en mere generel offerkarakteristik på området. Resultaterne er alene et udtryk for, hvilken type af ofre, som Fyns Politi har været i kontakt med.

Af de 67 ofre er 29 bosat i Odense Kommune, mens de resterende er bosat i syv øvrige fynske kommuner: Faaborg-Midtfyn, Svendborg, Nordfyn, Assens, Middelfart, Kerteminde og Langeland. 58 af ofrene er kvinder/piger, mens de resterende 9 er mænd/drenge. Aldersmæssigt er der en overvægt blandt de yngste, idet 50 af ofrene er i alderen 0-14 år, mens 5 af ofrene er 15 år. De resterende ofre fordeler sig med få personer på de øvrige aldersgrupper. Alle på nær ét offer har dansk nationalitet.

Figur 7 viser en opgørelse over hvilke former for it-relaterede seksualforbrydelser, som ofrene har været udsat for.

Figur 7: Ofre fordelt efter typer af it-relaterede seksualforbrydelser, fra 2013 til 31. maj 2018



Kilde: POLSAS data trukket d. 31.05.18

I undersøgelsesperioden har 25 ofre været udsat for, at få *tilsendt eller vist billeder af seksuel karakter*, mens 11 ofre har fået *tilsendt eller vist videoer af seksuel karakter*. Det er hovedsageligt via platformene Snapchat (18 ofre) eller Messenger (8 ofre), at gerningsmændene har sendt eller fremvist sådanne billeder eller videoer. Kontakten er oftest foregået ved, at gerningsmanden har sendt en personlig besked til offeret, da dette gør sig gældende for 31 af ofrene. Fire ofre blev udsat for, at gerningsmanden anvendte en falsk identitet til at sende/fremvise billeder eller video af seksuel karakter, mens kontakten til de sidste to ofre foregik via live streaming – det vil

sige en kontakt, der foregår i realtid, hvor gerningsmanden via internettet er i kontakt med offeret på gerningstidspunktet, fx på Skype.

Videre viser figur 7, at 16 ofre er blevet kontaktet med henblik på *grooming*. Grooming foregår både ved fysiske overgreb og overgreb via internettet, og er defineret ved, at en voksen opbygger et tillidsforhold til et barn med det formål senere at begå et seksuelt overgreb mod barnet (Rigspolitiet 2017a). Syv af ofrene er blevet kontaktet af gerningsmanden via personlige beskeder, to er blevet kontaktet via et chatforum og to er blevet kontaktet via live streaming. I tre tilfælde har gerningsmanden kontaktet offeret ved brug af en falsk identitet. Kontakten er primært etableret via Facebook (8 ofre), men der er også eksempler på at Messenger (3 ofre) og Skype (2 ofre) er anvendt.

Endelig viser figur 7, at fem ofre er blevet *presset til at tage og fremsende billeder eller video af seksuel karakter* til gerningsmanden. I fire tilfælde har gerningsmanden anvendt live streaming via Skype til at begå det kriminelle forhold. Fire ofre har *ufrivilligt fået delt intime videoer*, mens tre ofre *ufrivilligt har fået delt intime billeder*. Her er platformene Facebook (3 ofre) og Messenger (2 ofre) ligeledes anvendt, og gerningsmanden har etableret kontakten via et chatforum (3 ofre) eller en personlig besked (3 ofre).

Ofre for trusler

I undersøgelsesperioden er der i alt registreret 48 unikke ofre for it-relaterede trusler, og på samme måde som ved seksualforbrydelser er resultaterne i det følgende alene et udtryk for, hvad der karakteriser de ofre, som Fyns Politi har registreret.

Af de 48 ofre for er 19 bosat i Odense Kommune, 7 bosat i Middelfart Kommune og 7 bosat i Svendborg. De resterende 15 ofre fordeler sig i kommunerne Nordfyn, Faaborg-Midtfyn, Assens, Nyborg og Kerteminde. Ofrene tilhører primært de ældre aldersgrupper, idet 19 personer er i alderen 19-24 år og 10 personer er 18 år. Derudover er syv ofre i alderen 0-14 år, mens der er fem ofre i hver af de resterende aldersgrupper – 15 år, 16 år og 17 år. Hovedparten af ofrene er kvinder/piger (30 ofre), og har dansk nationalitet (45 ofre).

Af de i alt 48 ofre har 28 været udsat for trusler på livet, mens 14 har været udsat for trusler om vold. Ud fra resuméfeltet har det ikke været muligt at konkretisere, hvilken form for trusler de resterende syv ofre har været udsat for. Hovedparten af ofrene (31 ofre) har modtaget truslerne på Facebook, men Messenger har også været anvendt flere gange (ved 7 ofre).

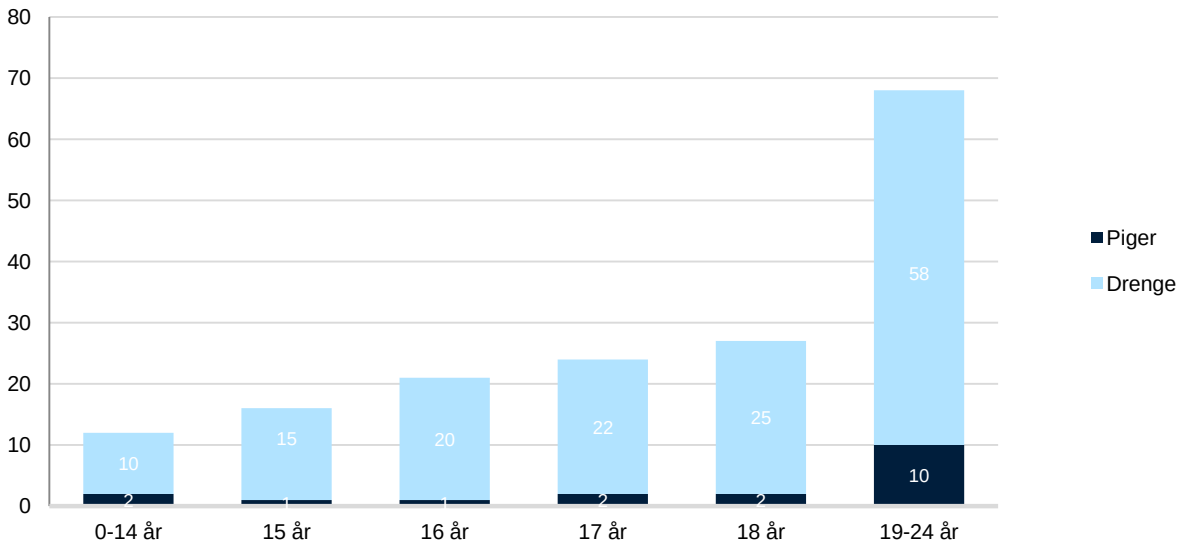
Hvem er gerningsmændene og hvad begår de?

I dette afsnit vil vi kortlægge, hvad der karakteriserer dé børn og unge, der begår it-kriminalitet, og give en beskrivelse af hvilke former for it-kriminalitet, de har begået. Det skal understreges, at dette afsnit alene er baseret på data vedrørende sigtede personer. Da det langt fra har været muligt at sigte en person i alle sager, er datagrundlaget for de følgende opgørelser forholdsvist lille, og vi kan ikke hævde, at materialet er repræsentativt for alle gerningsmænd på området.

Gerningsmænd til berigelseskriminalitet

Fyns Politi har sigtet 153 unikke gerningsmænd til it-relateret berigelseskriminalitet i undersøgelsesperioden, hvoraf hovedparten (62 %) er bosat i Odense Kommune – i overensstemmelse med ofrene. Figur 8 viser fordelingen på alder og køn.

Figur 8: Gerningsmænd fordelt efter alder og køn, fra 2013 til 31. maj 2018



Kilde: POLSAS data trukket d. 31.05.18

68 af de sigtede personer (44 %) er i alderen 19-24 år. Bemærk, som tidligere nævnt, at der naturligt vil være en stor andel i denne gruppe, da den rummer flere mulige udfald end de øvrige kategorier. Hovedparten af de sigtede er mænd (89 %), med dansk nationalitet (80 %).

En offerundersøgelse om unges kriminelle adfærd på nettet, baseret på selvrapportering fra 49.000 unge, finder, at de hyppigste gerningsmænd til it-kriminalitet er drenge, som går i 9. klasse - ca. 14-15 år (Det Kriminalpræventive Råd 2018). Dette er lidt yngre end de sigtede i Fyns Politis data. Forskellen kan hænge sammen med, at de yngre gerningsmænd enten er mere vanskelige at efterforske imod, eller at deres forbrydelser har en mindre alvorlig karakter og derfor

håndteres i det forebyggende arbejde. Som nævnt er denne analyse baseret på små tal, hvilket også kan påvirke resultaterne.

Blandt gerningsmændene til berigelseskriminalitet er 100 personer sigtet for misbrug af betalingskortoplysninger. Oplysningerne er primært anvendt til kortbetalinger på nettet (51 sigtede) eller til MobilePay overførsler (52 sigtede). Derudover er 41 personer sigtet for handelsbedrageri, mens 21 personer er sigtet misbrug af identitetsoplysninger med henblik på økonomisk gevinst. Denne fordeling kan afspejle, at misbrug af betalingskort er nemmere at efterforske, i forhold til handelsbedrageri eller misbrug af identitetsoplysninger. Det er desuden Fyns Politis erfaring, at gerningsmændene til bedrageri er meget opfindsomme, og hurtigt finder nye fremgangsmåder i takt med at sikkerhedshuller lukkes og nye tiltag indføres af myndighederne.

International forskning viser, at flere gerningsmænd til it-kriminalitet er af den opfattelse, at de ikke er rigtige kriminelle, fordi de bruger et tastatur til at begå kriminalitet og ikke er fysisk voldelige (Det Kriminalpræventive Råd 2016). Fyns Politi vurderer, at gerningsmændene til bedrageri både kan være personer med begrænsede it-færdigheder, der eksempelvis begår bedrageri ved at kopiere betalingskortoplysninger, og personer der begår bedrageri ved hacking af store virksomheders databeholdninger. En fælles motivationsfaktor for gerningsmændene er, at opdagelsesrisikoen og strafferammen vurderes som lav sammenlignet med den relativt set høje profitmulighed (Det Kriminalpræventive Råd 2016). Eksempelvis kan en gerningsmand modtage en pakke i en anonym pakkeboks, frem for at skulle oplyse sin egen adresse.

Gerningsmænd til seksualforbrydelser og trusler

I undersøgelsesperioden har Fyns Politi sigtet 13 unikke gerningsmænd til seksualforbrydelser, heraf er otte i alderen 19-24 år. De har alle dansk statsborgerskab og tolv af dem er mænd/drenge. Gerningsmændene fordeler sig i flere kommuner i politikredsen, og disse er sigtet for både ulovlig deling af intime videoer og billeder uden samtykke (6 sigtelser), kontakt med henblik på grooming (4 sigtelser) og at sende/vise intime eller seksuelle billeder af dem selv til ofre (5 sigtelser). Offerundersøgelsen konkluderer, at sexting (at sende nøgenbilleder/video af en selv) er en ganske udbredt del af mange unges hverdagsliv, hvor både piger og drenge sender nøgenbilleder til hinanden både med og uden samtykke (Det Kriminalpræventive Råd 2018), hvilket indikerer et stort mørketal på området.

I undersøgelsesperioden er der sigtet 25 personer for trusler, hvoraf 14 er sigtet for trusler på livet og 6 er sigtet for trusler om vold. I de resterende tilfælde har det ikke været muligt at konkretisere, hvad truslen har drejet sig om. Gerningsmændene har hovedsageligt fremsat deres trusler på Facebook (14 gerningsmænd) og derudover er Messenger, SMS, Skype og Snapchat brugt i få sager. 22 af de sigtede er mænd, med dansk statsborgerskab, og 14 af disse er mellem 19-24 år. Lidt mere end halvdelen (14 personer) har bopæl i Odense Kommune.

Referencer

Berlingske (2018). Overblik: Sådan straffes de første fem unge for deling af børneporno i Umbrella sagen. https://www.b.dk/nationalt/overblik-saadan-straffes-de-foerste-fem-unge-for-deling-af-boerneporno-i-umbrella (hentet 9. august 2018)

Balvig, F. (2017). Fra Barndommens Gade til Cyberspace. Det Kriminalpræventive Råd

Det Kriminalpræventive Råd (2018). Unges kriminelle adfærd på nettet. København

Det Kriminalpræventive Råd (2016). Når forbrydelser bliver digitale – En antologi om IT-kriminalitet og adfærd på internettet. København.

Danmarks Nationalbank (2017). Analyse - Danskerne er mestre i at betale elektronisk. 30. Marts 2017 – Nr. 6.

Kruize, P. (2018). Internet-kriminalitet 2017. Offerundersøgelse om identitetstyveri, bedrageri, afpresning og chikane i cybespace. Københavns Universitet. Det Kriminalpræventive Råd.

Oldrup, H., Christoffersen, M.N., Kristiansen, I.L. & Østergaard, S.V. (2016). Vold og seksuelle over-greb mod børn og unge i Danmark 2016. København: SFI – Det Nationale Forskningscenter for Velfærd.

Rigspolitiet (2017a). National Strategisk Analyse 2017. Dansk Politi, København.

Rigspolitiet (2017b). Metoderapport - National Strategisk Analyse 2017. Dansk Politi, København.