LCIK
LANDSDÆKKENDE CENTER FOR IT-RELATERET ØKONOMISK KRIMINALITET

POLITI

LCIK årsrapport 2020

En rapport om it-relateret økonomisk kriminalitet anmeldt i 2020

14. JUNI 2021

Indholdsfortegnelse

Forord

It-relateret økonomisk kriminalitet er et kriminalitetsområde i stor vækst. Det kan vi konstatere efter et 2020, hvor antallet af anmeldelser er steget med 11,1 %.

Politiets landsdækkende center for it-relateret økonomisk kriminalitet (LCIK) har været operationel i endnu et år, og det har givet anledning til at undersøge udviklingen og de tendenser, der har præget kriminalitetsområdet.

Årsrapporten tegner et overordnet billede af udviklingen inden for it-relateret økonomisk kriminalitet, som borgere og virksomheder udsættes for. Det er andet år, at LCIK offentliggør anmeldelsesdata for området og dermed første mulighed for at sammenligne kriminalitetsbilledet over tid.

Årsrapporten indeholder vores officielle tal, som er dem vi arbejder med, når vi prioriterer og tilpasser politiets driftsmæssige og forebyggende aktiviteter på området. Dermed henvender rapporten sig primært til politiet, men er derudover også relevant for en bredere målgruppe og alle, der har interesse i bekæmpelse af it-relateret økonomisk kriminalitet.

God læselyst.

Jesper Kracht

Centerchef i LCIK

Resumé

POLITI

Væsentlige resultater 1/2

Anmeldelser om it-relateret økonomisk kriminalitet

- LCIK modtog i 2020 29.905 anmeldelser om it-relateret økonomisk kriminalitet.
- Samhandel er stadig LCIK's største sagsområde, og anmeldelsestallet er steget siden 2019.

Udviklingen indenfor LCIK’s forskellige sagsområder

- Der er en stigning i antallet af anmeldelser om digital afpresning på 35,5 % fra 2019 til 2020.
- Samlet set blev der anmeldt færre sager vedrørende misbrug af kortoplysninger i 2020 end i 2019.
- Der blev anmeldt flere sager om misbrug af adgang til netbank m.m. i 2020 end i 2019.
- Der ses en betydelig stigning i antallet af anmeldelser, hvor personer er blevet snydt på fuphjemmesider, der lokker med forskellige låne- og investeringsmuligheder.

Væsentlige resultater 2/2

Om de private og professionelle anmeldere i sager om it-relateret økonomisk kriminalitet

- De private anmeldere anmelder hovedsageligt samhandelsbedrageri, misbrug af kortoplysninger, digital afpresning og kreditbedrageri.
- Private anmeldere bosat i Københavns politikreds anmelder i højere grad it-relateret økonomisk kriminalitet end borgere i andre dele af landet.
- De professionelle anmeldere anmelder hovedsageligt misbrug af adgang til netbank m.m., kreditbedrageri og misbrug af kortoplysninger.
- På trods af at professionelle anmeldere hyppigst anmelder misbrug af adgang til netbank m.m., så udsættes flest forskellige professionelle for kontaktbedrageri hovedsageligt i form af BEC/CEO fraud. Det vidner om, at det er få banker, der anmelder mange tilfælde af misbrug af adgang til netbank m.m.

Om de forurettede i sager om it-relateret økonomisk kriminalitet

- Flere mænd end kvinder anmelder it-relateret økonomisk kriminalitet.
- Knap halvdelen af de private forurettede udsættes for samhandelsbedrageri.
- Misbrug af adgang til netbank m.m. er den type af it-relateret økonomisk kriminalitet, hvor de forurettede er ældst.

Anmeldelser om it-relateret økonomisk kriminalitet i 2020

POLITI

LCIK modtog knap 30.000 anmeldelser i 2020

29.905

I 2020 modtog LCIK 29.905 anmeldelser om it-relateret økonomisk kriminalitet. Dette tal udgør den primære base gennem hele årsrapporten*

I 2020 modtog LCIK i alt **31.582** anmeldelser*

I 2020 modtog LCIK **1.677** anmeldelser uden for LCIK's sagsområde**

*Tallet er fratrukket de underforhold, der stammer fra anmeldelser givet gennem LCIK's API-løsning. Læs metodeafsnittet på side 83 for mere information om API-løsningen.

**Når LCIK modtager en anmeldelse, bliver den visiteret og kvalificeret. Nogle anmeldelser falder uden for LCIK's sagsområde 'it-relateret økonomisk kriminalitet'. Disse sager bliver udkorrigeret og sendt til rette politikreds. I 2020 blev 1.677 anmeldelser udkorrigeret.

LCIK modtog 11,1 % flere anmeldelser i 2020 i forhold til 2019

Antal anmeldelser i 2019 og 2020

Stigning i anmeldelserne på 2.982 i 2020

LCIK modtog i 2020 29.905 anmeldelser om it-relateret økonomisk kriminalitet. Det er 2.982 anmeldelser flere end i 2019, hvilket svarer til en stigning på 11,1 %.

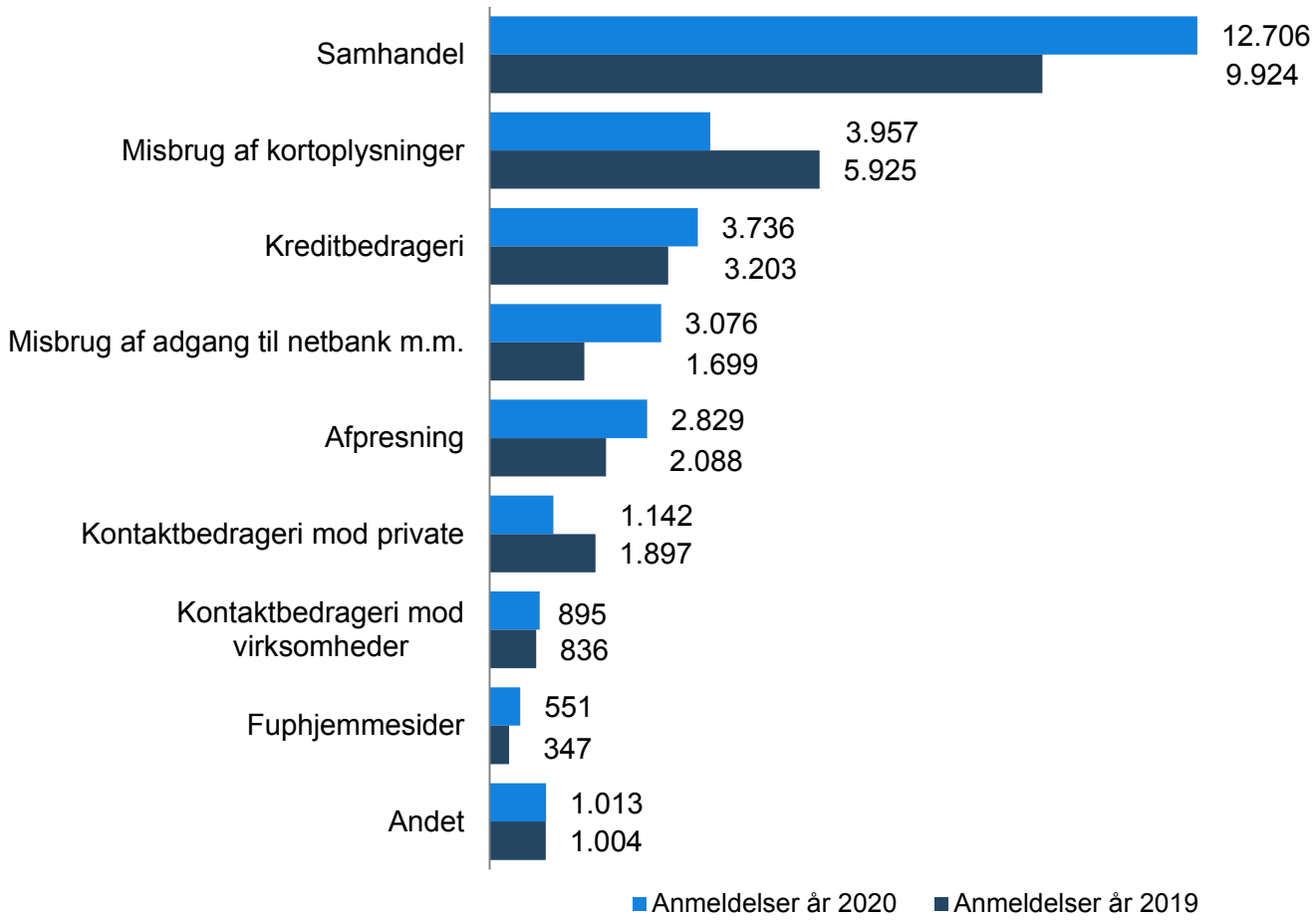
Forskel på behandlingen af data i 2019 og 2020

For at få et mere nøjagtigt overblik over anmeldelser om it-relateret økonomisk kriminalitet har LCIK valgt at benytte en ny opgørelsesmetode i årsrapporten for 2020 . Den nye opgørelsesmetode betyder, at der fratrækkes en række underforhold, som oprettes ved anmeldelser gennem LCIK's API-løsning. Der er tale om 2.099 underforhold, som er fratrukket det samlede anmeldelsestal. Læs mere om den nye opgørelsesmetode i metodeafsnittet på side 83.

Den nye opgørelsesmetode betyder at sammenligningsgrundlaget mellem 2019 og 2020 ikke er 1:1 sammenligneligt. Såfremt LCIK ikke havde benyttet den nye opgørelsesmetode i 2020, ville det samlede antal anmeldelser for 2020 være 32.004.

Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020

Over halvdelen af anmeldelserne i LCIK er sager om samhandel og misbrug af kortoplysninger



Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.
Base: (26.923) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2019.

Samhandel er stadig LCIK's største sagsområde

Samhandel er for andet år i træk det sagsområde, som LCIK modtager flest anmeldelser indenfor. Der har været en stigning på 2.782 anmeldelser om samhandel fra 2019.

Antallet af anmeldelser om misbrug af adgang til netbank m.m. er steget med 81%

Sagsområdet misbrug af adgang til netbank m.m. er steget med 81 % fra 2019 til 2020. Stigningen er sket på trods af en ny opgørelsesmetode, der i 2020 frasorterer underforhold, som er oprettet gennem anmeldelser via LCIK's API-løsning. Det er ikke tilfældet i 2019-tallene. Læs mere om den nye opgørelsesmetode i metodeafsnittet på side 83.

Fald i antallet af sager om misbrug af kortoplysninger og kontaktbedrageri mod private

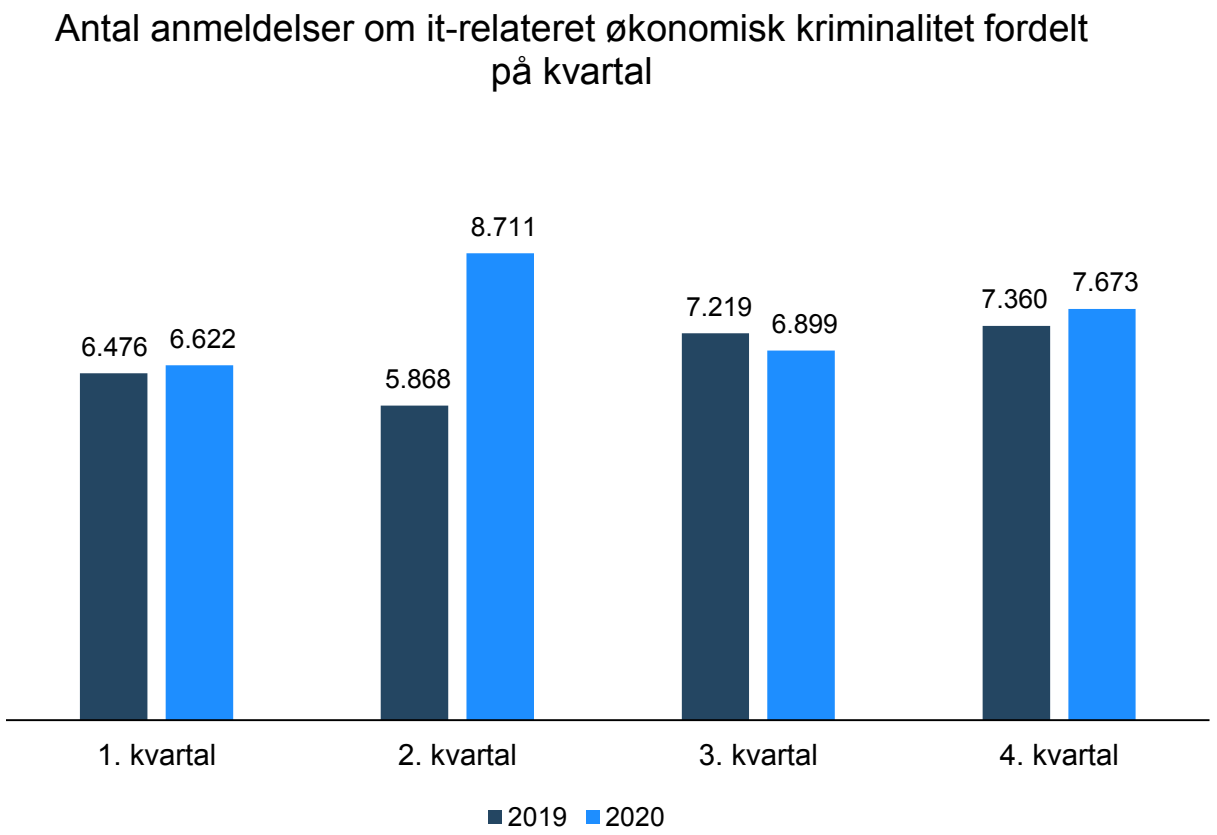
I 2020 var der et væsentligt fald i anmeldelser om misbrug af kortoplysninger sammenlignet med 2019.

Der kan også konstateres et væsentligt fald i antallet af anmeldelser om kontaktbedrageri mod private anmeldere.

Om kategorien 'Andet'

Kategorien 'Andet' dækker over de anmeldelser, som falder uden for LCIK's etablerede sagsområder eller anmeldelser, der endnu ikke er blevet tildelt et sagsområde af en sagsbehandler.

LCIK modtog i 2020 særligt mange anmeldelser i 2. kvartal



LCIK gennemsnitlige antal anmeldelser i kvartalet

LCIK modtog i gennemsnit 7.476 anmeldelser i kvartalet i 2020. I 2019 modtog LCIK i gennemsnit 6.731 anmeldelser i kvartalet.

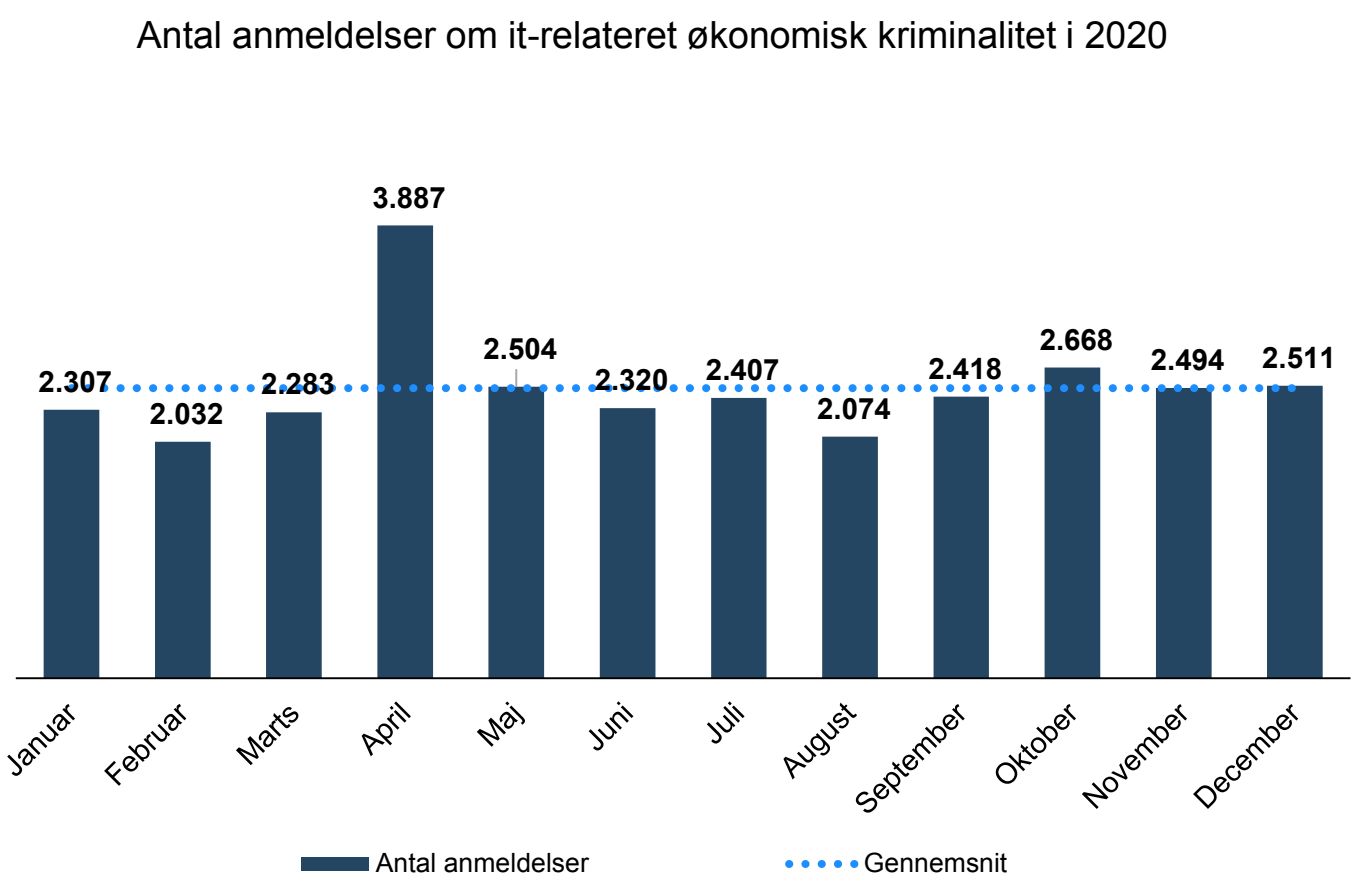
2. kvartal skiller sig ud på grund af et højt antal anmeldelser om masseafpresning

Kvartalsvis ligger anmeldelsestallene nogenlunde på niveau med det foregående år bortset fra 2. kvartal. I 2. kvartal 2020 modtog LCIK langt flere anmeldelser i forhold til 2019. Her er der tale om en stigning i antallet af anmeldelser på 48 %.

Stigningen i 2. kvartal er udtryk for et stort antal anmeldelser om masseafpresning i april 2020.

Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.

I 2020 modtog LCIK i gennemsnit 2.492 anmeldelser om måneden



Anmeldelser om måneden

LCIK modtog i gennemsnit 2.492 anmeldelser om it-relateret økonomisk kriminalitet hver måned i 2020. Gennemsnittet er visualiseret med en blåstiplet linje på grafen til venstre.

Stigningen i april skyldes en stor andel sager om digital afpresning

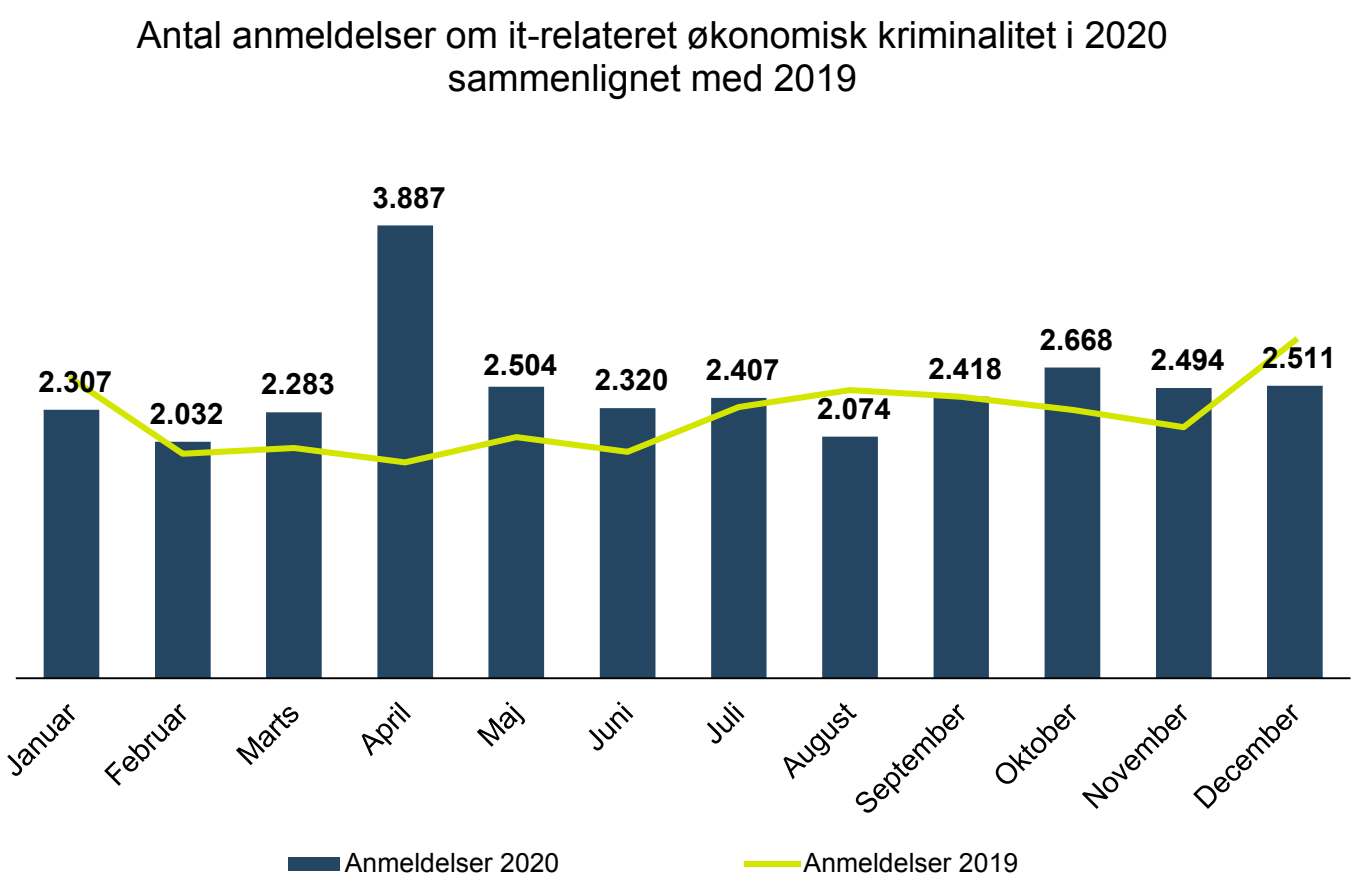
I 2020 modtog LCIK særligt mange anmeldelser i april, herunder et bemærkelsesværdigt stort antal sager om masseafpresning.

I alt modtog LCIK 1.752 anmeldelser om digital afpresning i april. Til sammenligning har LCIK i gennemsnit modtaget ca. 236 anmeldelser om digital afpresning om måneden i 2020.

Ud af de 1.752 anmeldelser om digital afpresning er der tale om 1.698 tilfælde af masseafpresning, hvor gerningsperson(er) har truet med at frigive pornografisk materiale knyttet til forurettede. I mange tilfælde er gerningspersonen gået efter at få betalt et beløb i bitcoins.

Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.

LCIK modtog de fleste måneder i 2020 flere anmeldelser end tilsvarende måneder i 2019



I ni af årets tolv måneder modtog LCIK flere anmeldelser end i tilsvarende måneder i 2019

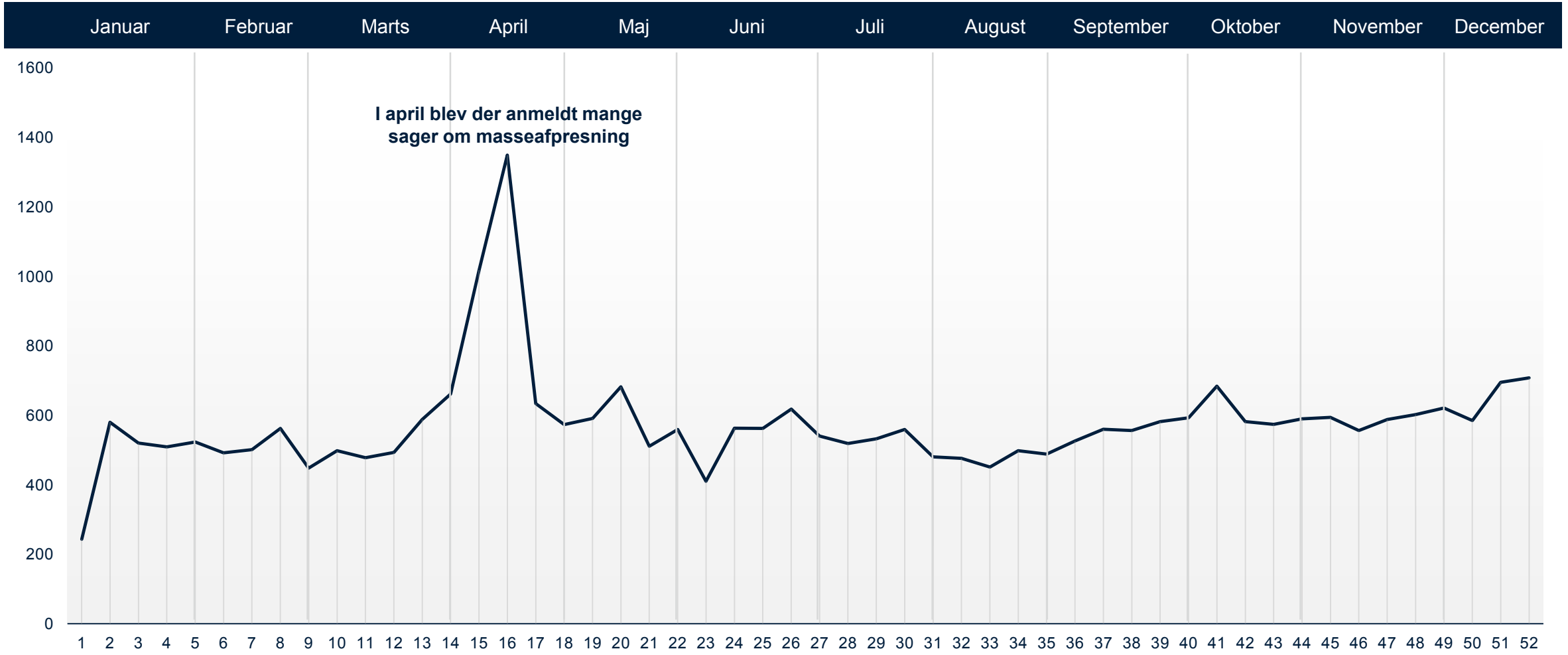
Undtagelserne er januar, august og december, hvor der i 2019 blev anmeldt flere sager om it-relateret økonomisk kriminalitet til LCIK end i 2020.

Stigningen i december 2019

Antallet af anmeldelser i december 2019 skal tages med det forbehold, at en privat aktør indgav mange anmeldelser gennem LCIK's API-løsning. Stigningen i antallet af anmeldelser i december 2019 skyldes, at MobilePay benyttede LCIK's API-løsning til deres anmeldelser, som opretter flere underforhold med LCIK-journalnumre. Fratrækkes disse underforhold modtog LCIK i alt 1.966 anmeldelser i december 2019. Såfremt anmeldelsestallene mellem årene blev opgjort på de samme præmisser ville anmeldelsestallet i 2020 være højere end i 2019.

Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.

Anmeldelser om it-relateret økonomisk kriminalitet i 2020 fordelt på uger



Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.

Antallet af anmeldelser fra private anmeldere steg med en femtedel fra 2019 til 2020

84,8 % er private anmeldere

24.644 af anmeldelserne er fra private anmeldere.

I 2019 modtog LCIK 20.497 anmeldelser fra private anmeldere svarende til 77,1 % af alle anmeldelser i 2019.

15,2 % er professionelle anmeldere

4.426 af anmeldelserne er fra professionelle anmeldere.

I 2019 modtog LCIK 6.082 anmeldelser fra professionelle anmeldere svarende til 22,9 %. af alle anmeldelser i 2019.

Anmeldere af it-relateret økonomisk kriminalitet opdeles i to grupper

I årsrapporten opdeles anmelderne i to grupper. Den ene gruppe kaldes 'private anmeldere' og dækker over privatpersoner. Den anden gruppe kaldes 'professionelle anmeldere', og dækker over virksomheder, organisationer og myndigheder.

Stigning i antallet af anmeldelser fra private anmeldere i 2020

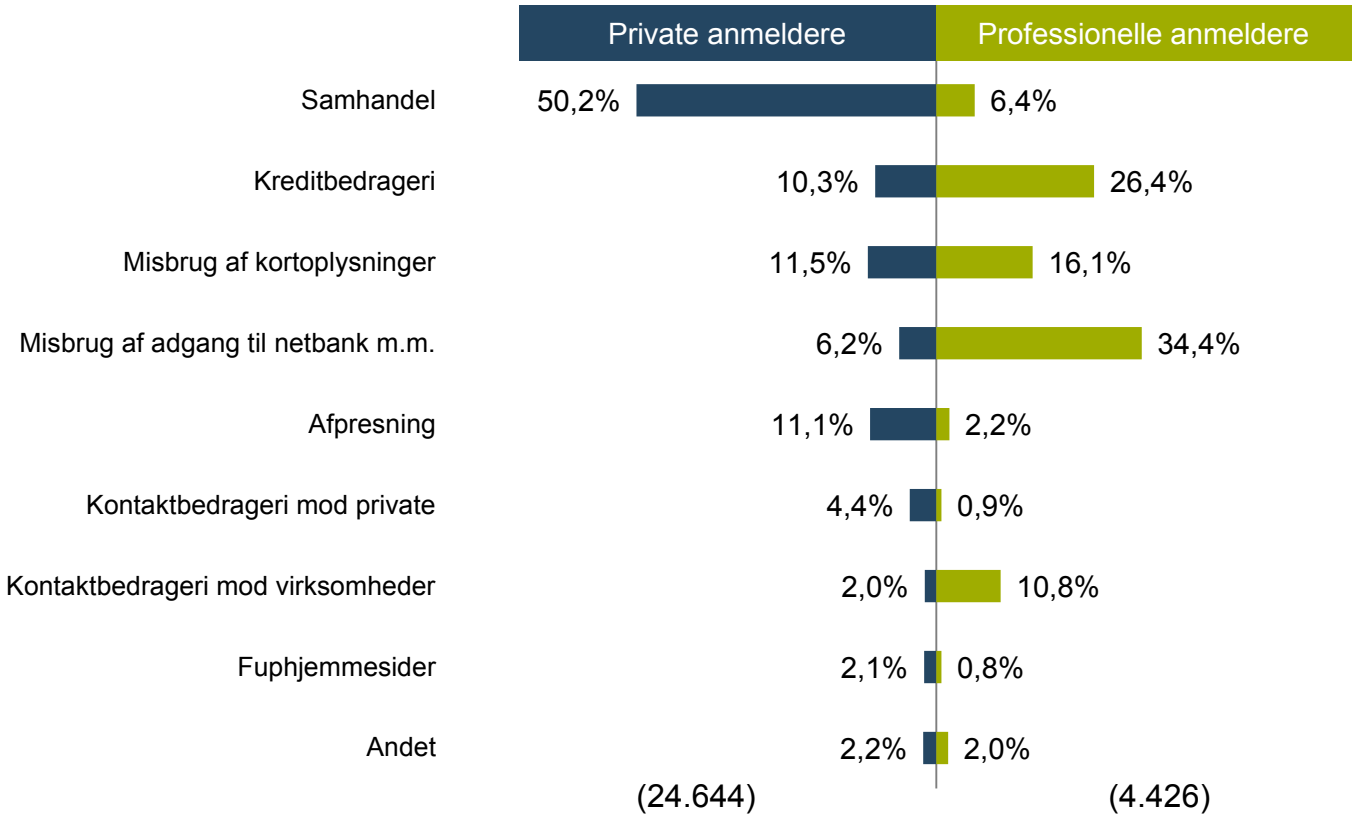
Antallet af anmeldelser fra private anmeldere steg fra 20.497 anmeldelser i 2019 til 24.644 anmeldelser i 2020. Det svarer til en stigning på 20,2 %.

Faldet i anmeldelser fra professionelle anmeldere skyldes en ny opgørelsesmetode

I årsrapporten 2020 har LCIK fratrukket en række underforhold fra anmeldelsestallet. Der er tale om de underforhold, der genereres gennem LCIK's API-løsning, som benyttes af nogle professionelle anmeldere. Såfremt underforholdene var inkluderet i årsrapporten i år, ville andelen af anmeldelser fra professionelle anmeldere være 20,9 pct. og dermed ligge tæt på sidste års niveau. Læs mere om den nye opgørelsesmetode i metodeafsnittet på side 83.

Base: (29.070) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i år 2020 med tilknyttede personoplysninger.

Private anmeldte mest samhandel - professionelle anmeldte misbrug af adgang til netbank m.m.



De private anmeldere anmeldte i høj grad samhandelsbedrageri

Derudover er misbrug af kortoplysninger, kreditbedrageri og digital afpresning også nogle af de sagsområder, som de private anmeldere hyppigst anmeldte i 2020.

Anmeldelser fra de professionelle anmeldere kom oftest fra banker og lånevirksomheder

De professionelle anmeldelser handlede især om misbrug af adgang til netbank m.m., kreditbedrageri og misbrug af kortoplysninger. Det er ikke overraskende, at netop disse sagsområder fylder meget, da de fleste professionelle anmeldelser kom fra banker og lånevirksomheder.

Base: (29.070) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i år 2020 med tilknyttede personoplysninger.

Anmeldelser om it-relateret økonomisk kriminalitet fordelt på politikredse

Nordjyllands Politi
2.274 anmeldelser.
Det svarer til **7,8 %** af alle anmeldelser

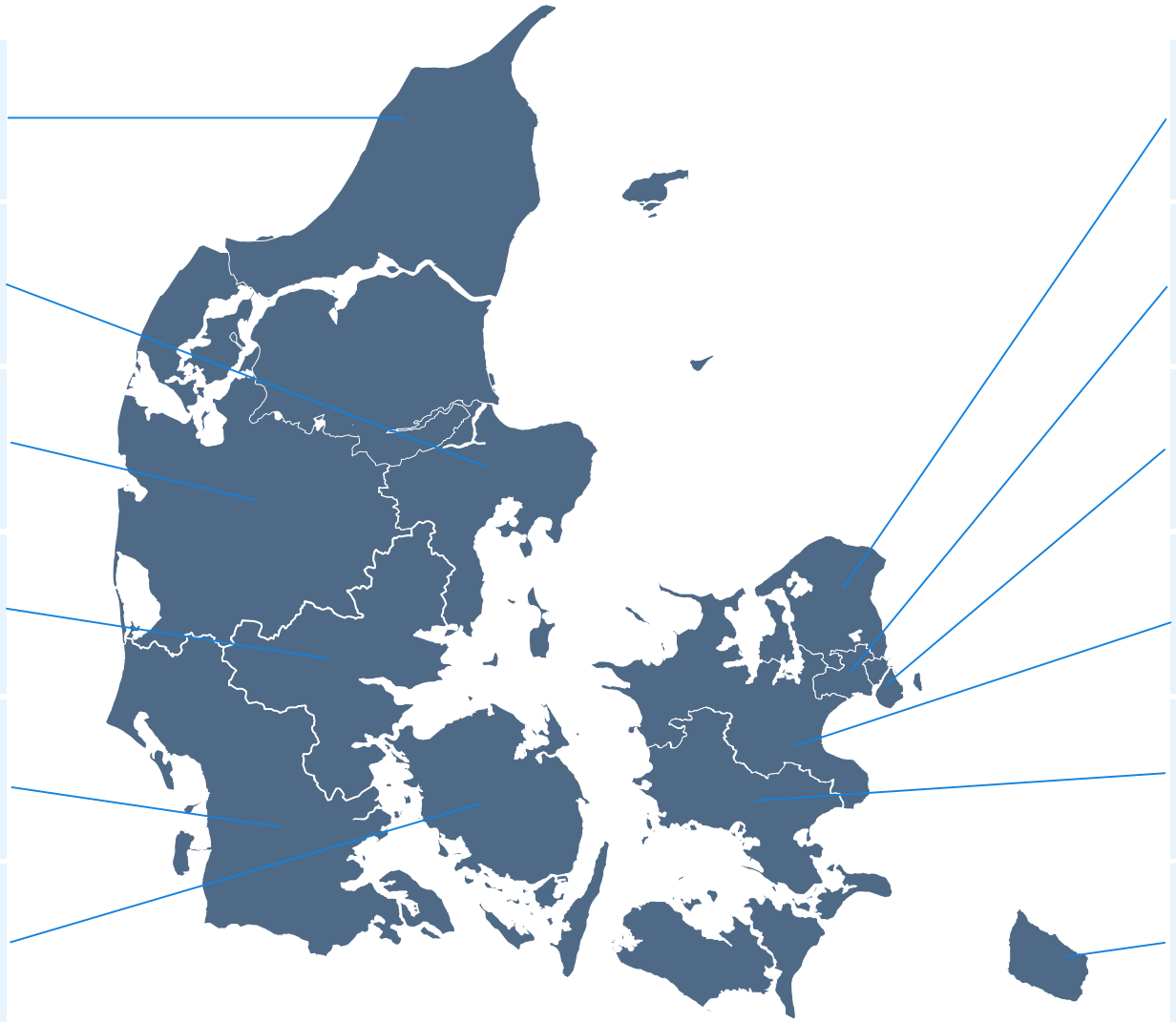
Østjyllands Politi
2.675 anmeldelser
Det svarer til **9,2 %** af alle anmeldelser

Midt- og Vestjyllands Politi
2.566 anmeldelser
Det svarer til **8,8 %** af alle anmeldelser

Sydøstjyllands Politi
2.110 anmeldelser
Det svarer til **7,3 %** af alle anmeldelser

Syd- og Sønderjyllands Politi
1.963 anmeldelser
Det svarer til **6,8 %** af alle anmeldelser

Fyns Politi
2.438 anmeldelser
Det svarer til **8,4 %** af alle anmeldelser



Nordsjællands Politi
3.001 anmeldelser
Det svarer til **10,3 %** af alle anmeldelser

Københavns Vestegns Politi
2.300 anmeldelser
Det svarer til **7,9 %** af alle anmeldelser

Københavns Politi
5.853 anmeldelser
Det svarer til **20,1 %** af alle anmeldelser

Midt- og Vestsjællands Politi
1.894 anmeldelser
Det svarer til **6,5 %** af alle anmeldelser

Sydsjælland og Lolland-Falsters Politi
1.584 anmeldelser
Det svarer til **5,4 %** af alle anmeldelser

Bornholms Politi
156 anmeldelser
Det svarer til **0,5 %** af alle anmeldelser

Base: (29.070) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i år 2020 med tilknyttede personoplysninger.
Note: Der er taget udgangspunkt i anmelder/forurettedes bopælsadresser for at opnå et kvalificeret bud på, hvor anmeldelsen ville være indgivet, såfremt LCIK ikke modtog den.
Note: Antallet af ” Samlet antal anmeldelser ” dækker over anmeldelser fra både private og professionelle anmeldere (se base).

POLITI

Anmeldelser fra private anmeldere i hver politikreds

Nordjyllands Politi
2.032 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **3,9**

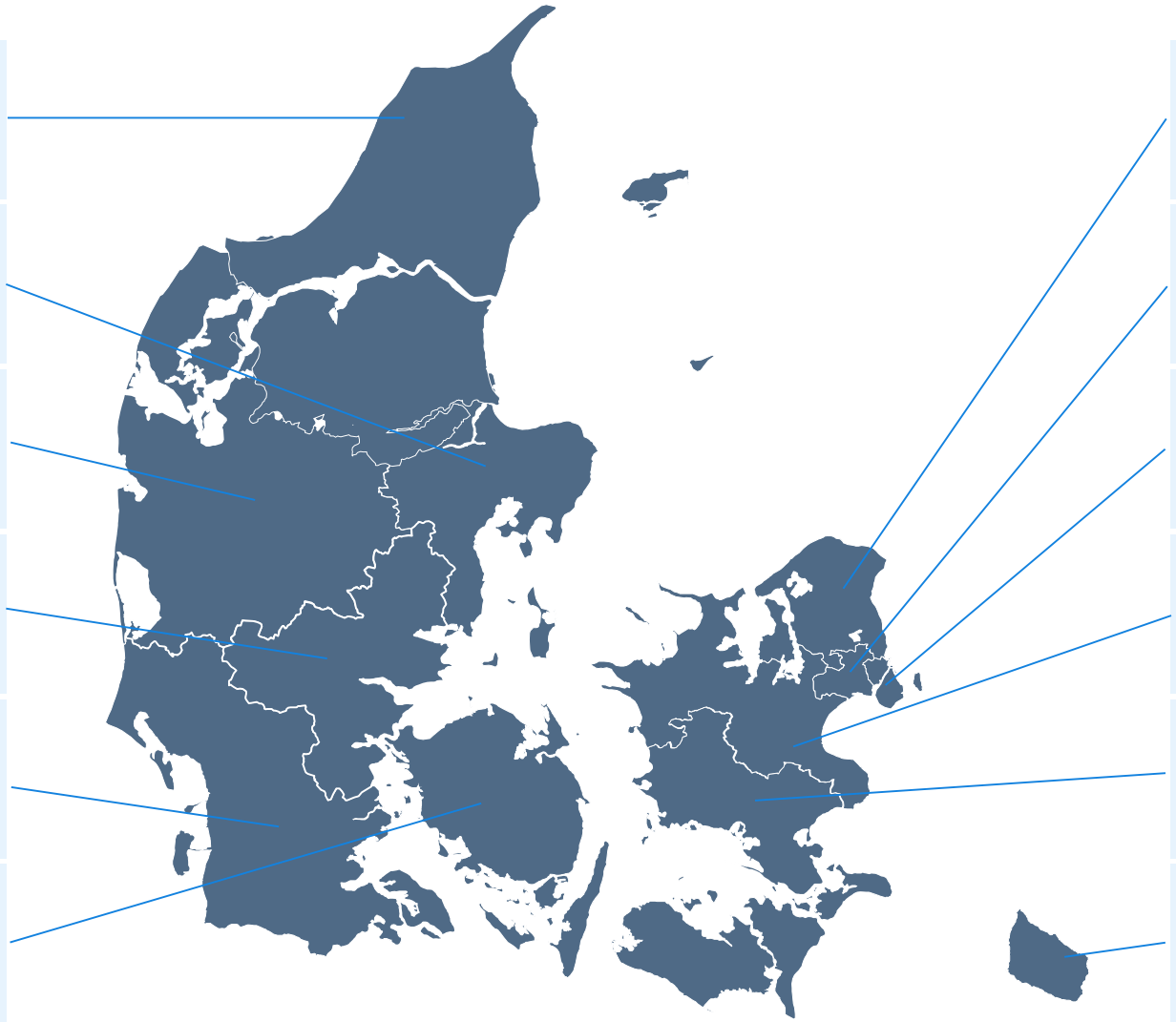
Østjyllands Politi
2.474 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **4,1**

Midt- og Vestjyllands Politi
2.186 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **3,7**

Sydøstjyllands Politi
1916 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **3,9**

Syd- og Sønderjyllands Politi
1.562 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **3,6**

Fyns Politi
2.278 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **4,6**



Nordsjællands Politi
2.636 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **4,4**

Københavns Vestegns Politi
1.724 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **4,1**

Københavns Politi
4.181 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **5,2**

Midt- og Vestsjællands Politi
1.770 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **3,8**

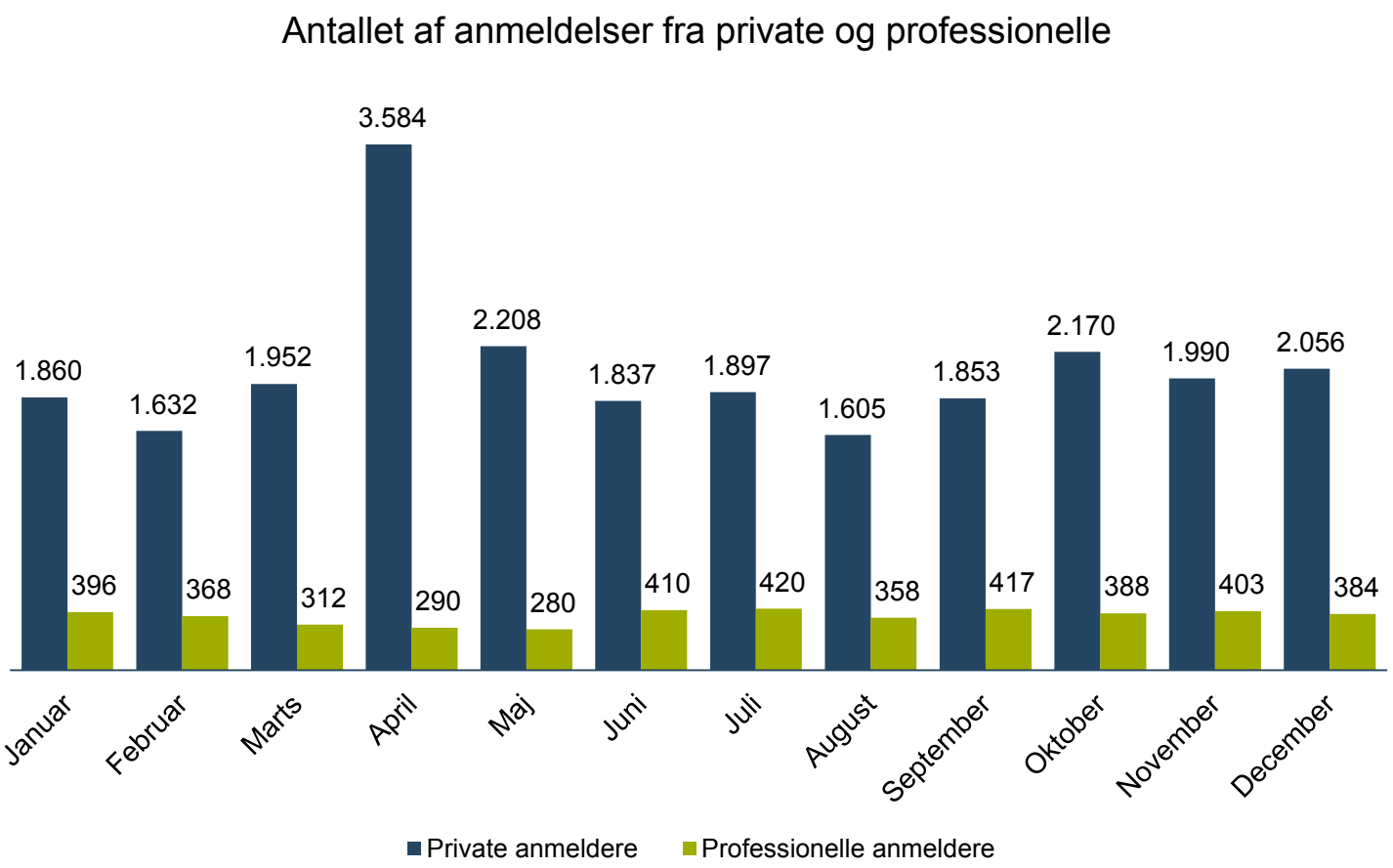
Sydsjælland og Lolland-Falsters Politi
1.499 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **4,0**

Bornholms Politi
150 private anmeldelser
Private anmeldelser
pr. 1.000 indbyggere: **3,8**

Base: (24.644) Antal anmeldelser om it-relateret økonomisk kriminalitet fra private anmeldere modtaget hos LCIK i 2020 med tilknyttede personoplysninger.
Note: Der er taget udgangspunkt i anmelder/forurettedes bopælsadresser for at opnå et kvalificeret bud på, hvor anmeldelsen ville være indgivet, såfremt LCIK ikke modtog den.

POLITI

Anmeldelser fra private og professionelle anmeldere fordelt på måneder



Anmeldelser fra private anmeldere om måneden

LCIK modtog i gennemsnit 2.052 anmeldelser fra private anmeldere om måneden i 2020*. I 2019 lå dette tal på 1.708 anmeldelser.

Anmeldelser fra professionelle anmeldere om måneden

LCIK modtog i gennemsnit 369 anmeldelser fra professionelle anmeldere om måneden*. I 2019 modtog LCIK 507 anmeldelser om måneden fra professionelle anmeldere. Det store gennemsnitlige fald blandt professionelle anmeldere skyldes en ny behandling af data sammenlignet med databehandlingen i LCIK's 1-års analyse 2019. For mere om den nye behandling af data henvises til s. 83.

Mange anmeldelser om masseafpresning i april

Der var særligt mange anmeldelser fra private anmeldere i april 2020, herunder et bemærkelsesværdigt stort antal anmeldelser om masseafpresning.

Base: Antal anmeldelser om it-relateret økonomisk kriminalitet fra borgere (24.644) og professionelle anmeldere (4.426) modtaget hos LCIK i år 2020.
Note: *gennemsnit er afrundet til nærmeste hele tal.

Samhandelsbedrageri

POLITI

Beskrivelse af samhandelsbedrageri

Generelt om samhandelsbedrageri

Samhandelsbedrageri er en handel mellem to eller flere parter, hvor den ene part - med forsæt - ikke overholder sin del af aftalen. Handlen er oftest mellem borgere, der fx handler via handelsplatforme eller sociale medier på nettet som fx DBA, Gul og Gratis eller Facebook. Samhandelsbedrageri kan også ske i en handel mellem en borger og en virksomhed, fx når en privatperson handler på en webshop, der viser sig at være falsk. Sidstnævnte eksempel kan også ramme virksomheder, der køber produkter/ydelser på andre virksomheders hjemmesider (B2B). Det er samhandelsbedrageri, uanset om det er sælger eller køber, der ikke overholder aftalen. I disse sager benytter gerningspersonerne ofte falske dokumenter, misbruger andres identitet eller anvender muldyr for at sløre pengesporet. I de fleste tilfælde er det sælgeren, der bedrager køberen.

LCIK arbejder med fire overordnede kategorier for typer af varer, der er genstand for samhandelsbedrageri.

Fysiske varer

Den udbudte/handlede vare er en fysisk genstand. I sager med fysiske varer, hvor sælgeren er gerningspersonen, vil udbyttet som udgangspunkt være penge (typisk ved kontooverførsel eller MobilePay).

Er køberen derimod gerningsperson, vil udbyttet i stedet være den handlede vare.

Det er ofte elektronik, design, tøj og børneartikler, der indgår som fysisk vare i sager om samhandelsbedrageri.

Boligudlejning

Den udbudte/handlede vare er en bolig til enten langvarig beboelse eller ferieophold.

Gerningspersonen agerer udlejer og tilbyder at udleje enten fiktive boliger eller faktiske boliger, som gerningspersonen ikke har råderet over. I flere tilfælde gennemføres fremvisninger, og der indgås lejekontrakter med flere forurettede, som derpå betaler depositum og forudbetalt husleje.

Billetter

Den udbudte/handlede vare er billetter - typisk til populære koncerter, festivaller, sportsarrangementer m.v.

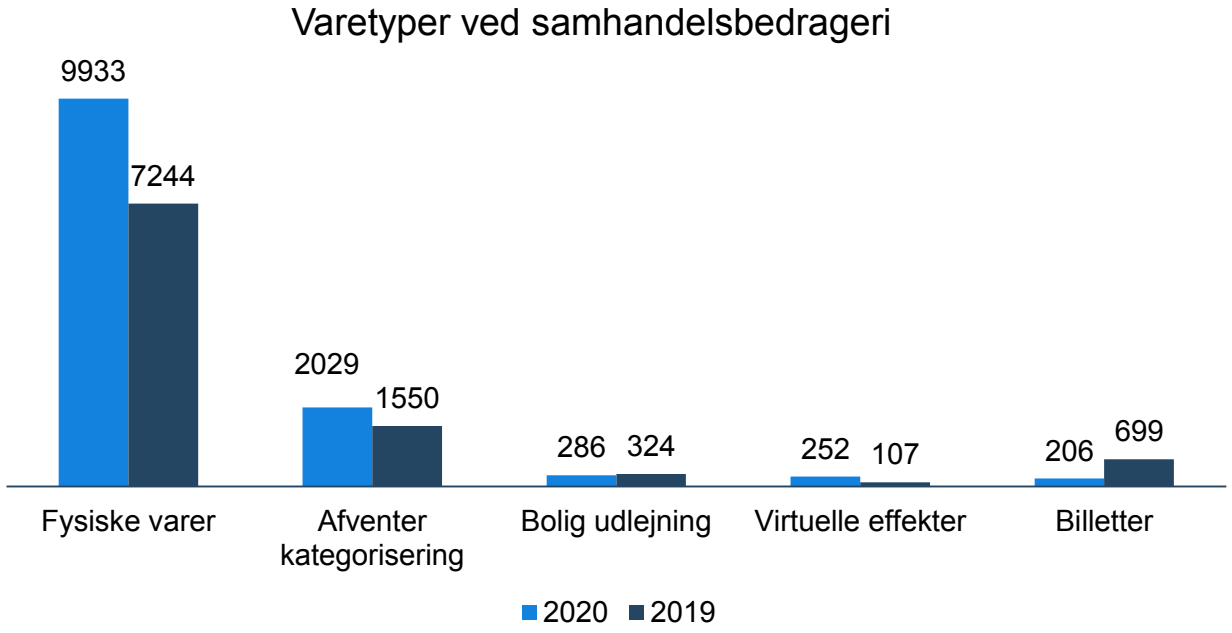
Samhandelsbedrageri vedrørende billetsvindel ses kun i tilfælde, hvor gerningspersonen agerer sælger af billetterne. Ved denne form for svindel opsøger gerningspersonen ofte den forurettede, efter at vedkommende har efterspurgt specifikke billetter på sociale platforme.

Virtuelle effekter

Den udbudte/handlede vare er en virtuel genstand. Handlerne foregår oftest i online spilverdener såsom CS:GO eller spilplatforme som fx Steam. Den handlede vare er oftest skins eller virtuel valuta.

Langt størstedelen af de anmeldte samhandelsbedragerier handler om svindel med fysiske varer

42,5% af anmeldelserne til LCIK handlede i 2020 om samhandel (12.706).



Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.

Samhandelsbedrageri foregår på forskellige platforme

Mange samhandelsbedragerier finder sted på sociale medier og digitale platforme, der forbinder køber og sælger. Især Facebook, herunder Facebook Messenger, og DBA går igen blandt anmeldelserne.

Fysiske varer

DBA, Facebook, Gul og Gratis, Webshops, Trendsales, Instagram, mail og sms.

Billetter

Facebook, DBA, Gul og Gratis, Tilbudibyen.dk, Onlineticketshop.com, fysisk.

Boligudlejning

Facebook, DBA, Boligportal.dk, Airbnb, Lejebolig.dk, Instagram og Boligsurf.dk.

Virtuelle effekter

Facebook, CS:GO, Empire.com, DBA, Steam, og G2a.com.

Offerundersøgelse peger på et stort mørketal

Anmeldelsestilbøjelighed og det økonomiske tab

Den nyeste offerundersøgelse fra Justitsministeriets Forskningskontor (2020) peger på, at en stor del af ofrene for bedrageri ved køb og salg af varer/ydelser på nettet ikke anmelder forholdet til politiet.

I offerundersøgelsen har man fundet, at knap 21 % af ofrene selv anmelder bedrageriet til politiet, mens politiet i 5 % af tilfældene får kendskab til bedrageriet på anden vis, fx gennem offerets bank eller kreditkortselskab. Det betyder, at ca. 74 % af ofrene ikke anmelder samhandelsbedrageri til politiet.

En af grundene til at mange private ikke anmelder samhandelsbedrageri, kan være, at de typisk selv hæfter for de økonomiske tab på trods af anmeldelsen. Ifølge Offerundersøgelsen har 85 % af ofrene for samhandelsbedrageri helt eller delvist hæftet for det økonomiske tab.

Såfremt undersøgelsens bud på et mørketal omkring 74 pct. er retvisende, udgør LCIK's 12.706 anmeldelser om samhandelsbedrageri kun 26 pct. af den faktiske forekomne samhandelskriminalitet. Ud fra disse nøgletal vil et bud på den faktiske forekomst af samhandelsbedrageri lyde på omkring 48.869 tilfælde på et år.

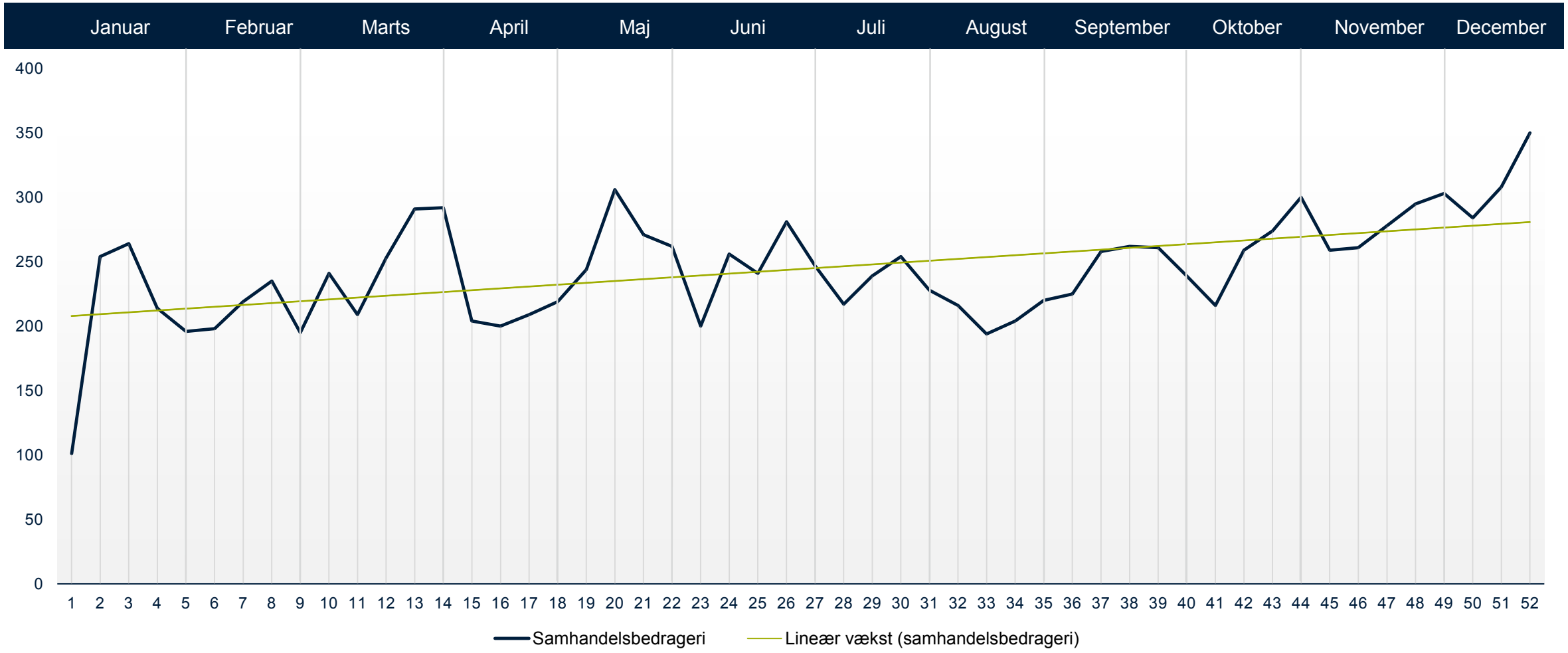
I undersøgelsen skønnes det, at mange samhandelsbedragerier ikke anmeldes, fordi det tabte beløb anses for at være af en beskeden størrelse. Her peger undersøgelsen ligeledes på, at de ofre, der ikke selv har anmeldt, i 32 % af tilfældene har lidt tab for under 499 kroner, og 87 % har lidt tab på under 2.999 kroner.

Det skal understreges, at offerundersøgelsen bygger på relativt få observationer på dette område, hvorfor resultaterne skal tolkes varsomt.

Kilde: Justitsministeriets Forskningskontor (2020). Udsathed for vold og andre former for kriminalitet, *Offerundersøgelserne 2005-2019*.

Anmeldelsestidspunkt for alle samhandelsbedragerier fordelt på uger

Der har været en lineær vækst i antallet af anmeldelser om samhandelsbedrageri



Base: (12.706) Antal samhandelsanmeldelser modtaget hos LCIK i 2020.

Opsummering af samhandelsbedrageri

Generelt om samhandelsbedrageri

Igen i 2020 udgjorde samhandelsbedrageri det største sagsområde inden for it-relateret økonomisk kriminalitet målt på antallet af anmeldelser. Hele 42,5 % af alle LCIK's anmeldelser i 2020 handlede om samhandelsbedrageri. Det er en stigning siden 2019, hvor andelen af samhandelsbedrageri udgjorde 36,9 % af det samlede anmeldelsesbillede.

Der har været en tendens til, at antallet af samhandelsanmeldelser er vokset svagt henover hele året.

Samhandel anmeldes hovedsageligt af privatpersoner. Hele 50,2 % af de private anmeldelser i 2020 drejede sig om samhandel.

Offerundersøgelse peger på mørketal

Justitsministeriets offerundersøgelse peger på, at mørketallet blandt samhandelsbedragerier er stort (ca. 74 %)

Det store mørketal indikerer, at LCIK i fremtiden potentielt skal håndtere flere anmeldelser om samhandel, såfremt anmeldelsespraksis ændrer sig, og flere personer begynder at anmelde samhandelsbedrageri. Det skal dog understreges, at mørketallet er udregnet på baggrund af en lille stikprøve, og at resultatet derfor skal tolkes varsomt.

Størstedelen af anmeldelserne om samhandel handlede om fysiske varer

Bedragerierne fandt primært sted på digitale handelsplatforme og sociale medier som DBA, Gul og Gratis og Trendsales og sociale medier som Facebook, herunder Facebook Messenger, og Instagram.

I nogle tilfælde blev de forurettede også kontaktet over enten mail eller sms.

Færre anmeldelser om billetter grundet COVID-19

Antallet af anmeldelser om billetter faldt med 70,5 % fra 2019-2020. I 2019 var svindel med billetter især et problem op til sommeren og under festivalsæsonen hen over sommeren. Grundet COVID-19 og nedlukningen af samfundet, blev en række begivenheder aflyst, og det ses tydeligt i antallet af anmeldelser vedrørende billetter.

Det ses dog, at de kriminelle tilpasser sig og kaster sig over nye varekategorier. I 2020 så LCIK bl.a., hvordan kriminelle foregav at sælge hundehvalpe, som har været en populær ”vare” under pandemien. Varen er let at svindle med, da den ofte kræver depositum og evt. forskud betalt af køber.

Fald i antallet af sager om boligudlejning

I 2020 modtog LCIK 286 anmeldelser om svindel med boligudlejning. Det svarer til et fald på 11,7 % i forhold til anmeldelsestallet i 2019.

Svindel med boligudlejning foregår hele året rundt, men med øget aktivitet i sommermånederne op til studiestart (juni, juli og august). Disse svindelnumre foregår både på online samhandelsplatforme og sociale medier som eksempelvis Facebook. Samhandelsplatformene dækker både over platforme som blandt andet DBA og Airbnb, Boligportal.dk og Lejebolig.dk, som er mere specialiserede i boligudlejning.

Over en fordobling i antallet af sager om virtuelle effekter

Antallet af anmeldelser om virtuelle effekter er mere end fordoblet siden 2019. I 2020 fik LCIK 252 anmeldelser, mens tallet i 2019 var 107. Denne stigning skal ses i lyset af, at svindel med virtuelle effekter er et mindre fænomen i forhold til de andre typer af samhandelsbedrageri.

Svindlen foregår ofte på sociale medier som eksempelvis Facebook eller spilplatforme som fx Steam og Facebook. I 2020 var der flere anmeldelser relateret til skin-gambling-sitet CSGOEmpire.com*.

Kilde: Justitsministeriets Forskningskontor. (2020). Udsathed for vold og andre former for kriminalitet, *Offerundersøgelserne 2005-2019.*
Note: CSGOEmpire.com er et betting-site, hvor man kan gamble, sælge og købe skins (virtuelle effekter red.) til spillet CS:GO.

Misbrug af kortoplysninger

POLITI

Beskrivelse af misbrug af kortoplysninger

Generelt om misbrug af kortoplysninger

Misbrug af kortoplysninger dækker over sager, hvor en gerningsperson betaler for et køb på internettet med en anden persons kortoplysninger. Misbrug af kortoplysninger finder ofte sted på webshops og gennem betalingstjenester og spilsites.

Denne type bedrageri opdages typisk ved, at en person med et betalingskort (kortholder) ser på sit kontoudtog og opdager, at der er foretaget køb eller betalinger, som vedkommende ikke kender til. Herefter gør kortholder sin bank opmærksom på situationen og gør samtidig indsigelse. Nets foretager chargeback, som er en tilbageoverførsel af de penge, der er brugt til uberettigede køb. Banken opfordrer ofte kortholder til efterfølgende at anmelde forholdet til politiet.

Hvis der er foretaget et chargeback for det beløb, indsigelsen handler om, modtager politiet ofte en anmeldelse fra den webshop, hvor den uberettigede handel er foregået. I denne situation har kortholderen fået misbrugt sine kortoplysninger, men det er webshoppen, der lider det økonomiske tab, da den har leveret en vare eller ydelse uden at modtage betaling.

I sager om misbrug af kortoplysninger får gerningspersonen ofte adgang til kortoplysningerne ved afluring eller fordi oplysningerne har været til salg på internettet. Især anskaffelsen af kortoplysninger på illegale sider på internettet synes at være et problem.

I andre tilfælde har kortholder ubevidst udleveret sine oplysninger via phishing sider, hvor kortholder tror, at han/hun betaler for en vare/ydelse (fx porto for et vundet gavekort). I virkeligheden udsættes kortholder for ”live-phishing”, og gerningspersonen bruger oplysningerne til at foretage et andet køb. Er kortholderen ikke opmærksom på det beløb der godkendes ved 2-faktor godkendelse, kan gerningspersonen slippe afsted med køb for store beløb.

Misbrug af kortoplysninger på webshop

Denne type svindel forekommer, når kortoplysninger uberettiget er blevet brugt til at købe en vare eller ydelse på en webshop. Varen sendes ofte til et muldyr eller til en postboks.

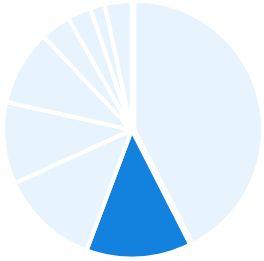
Misbrug af kortoplysninger gennem betalingstjenester

Der findes i dag flere betalingsløsninger, hvor brugere kobler deres kortoplysninger sammen med betalingsløsningen. Da man både kan foretage overførsler og køb i butikker gennem betalingstjenesterne, er de blevet et yndet middel for misbrug af kortoplysninger.

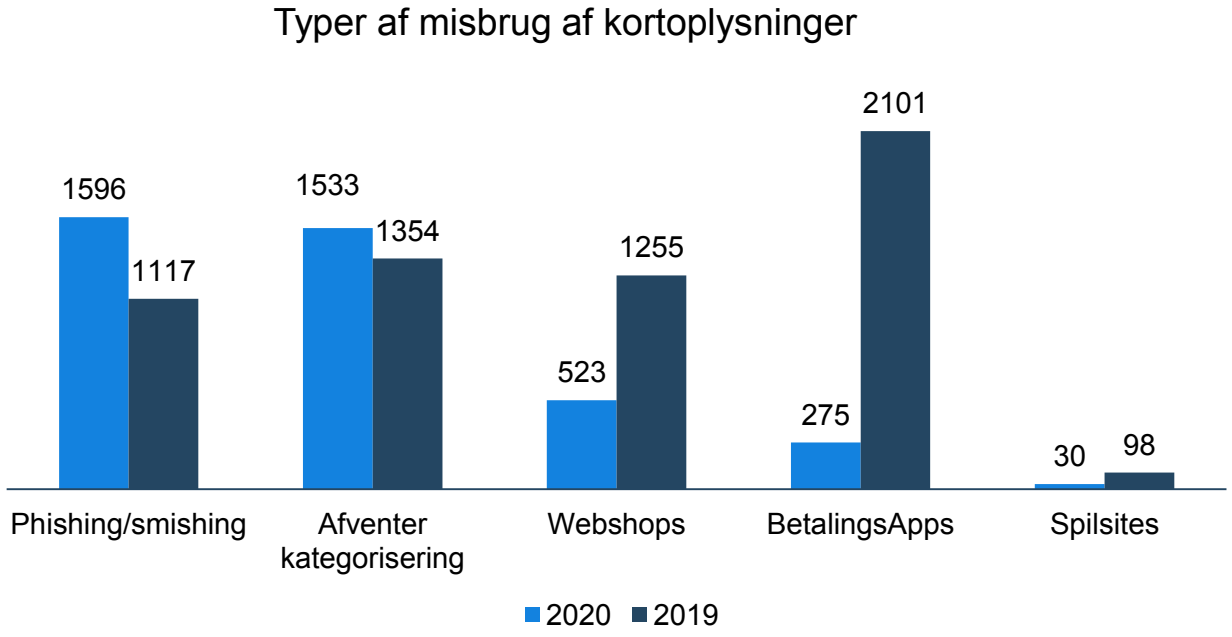
Misbrug af kortoplysninger gennem spilsites

I nogle tilfælde benytter gerningspersoner de stjålne kortoplysninger til at betale for odds hos spillefirmaer. Gevinster udbetales herefter til gerningspersonen og pengene er herefter ”hvide”. Den forurettede opdager typisk bedrageriet ved, at der på vedkommendes kontoudtog er trukket penge fra en spiludbyder, hvor den forurettede ikke har konto.

Der har været et fald i antallet af anmeldelser, hvor kortoplysninger er blevet misbrugt gennem betalingsapps



13,2 % af anmeldelserne til LCIK i 2020 handlede om misbrug af kortoplysninger (3.957).



Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.

Generelt fald i antallet af anmeldelser, men en stigning i sager om phising/smishing

Misbrug af kortoplysninger er et sagsområde, der har haft nedgang i antallet af anmeldelser fra 2019-2020. Samtidig er antallet af anmeldelser specifikt om phising/smishing af kortoplysninger steget.

Fald i antallet af sager om misbrug af kortoplysninger

Faldet i antallet af anmeldelser om misbrug af kortoplysninger ses især i store fald i antallet af sager om kortmisbrug gennem webshops og betalingsapps. Antallet af anmeldelser vedrørende misbrug af kortoplysninger gennem webshops er faldet med 58,3 pct. og antallet af anmeldelser om misbrug af kortoplysninger gennem betalingsapps er faldet med 86,9 pct. i forhold til år 2019. Det store fald skyldes formentligt den øgede sikkerhed på området, som f.eks. indførslen af 3D Secure.

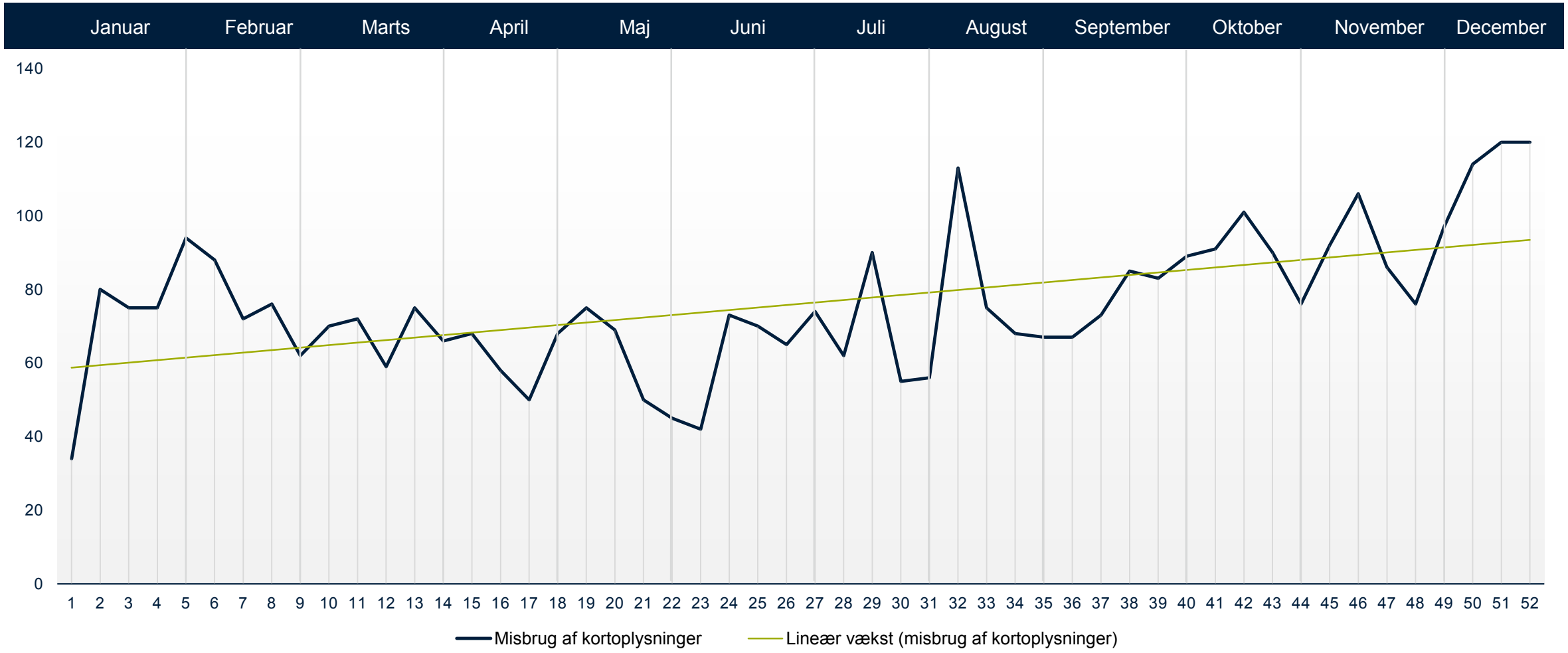
Stigning i anmeldelser om phising/smishing af kortoplysninger

På trods af det overordnede fald har én bestemt type af misbrug af kortoplysninger vundet fremgang. I 2020 steg antallet af sager vedrørende phising/smishing af kortoplysninger med hele 42,9 % i forhold til 2019.

Antallet af anmeldelser vedrørende phising/smishing af misbrugte kortoplysninger skal tolkes varsomt, da der i flere tilfælde af misbrug af kortoplysninger på webshops også er tale om phising/smishing af kortoplysningerne. Det er op til den enkelte sagsbehandler at vurdere, hvordan anmeldelsen registreres, hvorfor sagsområdet er særligt følsomt over for ændringer i registreringspraksis.

Anmeldelsestidspunkt for alle misbrug af kortoplysninger fordelt på uger

Der har været en lineær vækst i antallet af anmeldelser om misbrug af kortoplysninger



Base: (3.957) Antal anmeldelser om misbrug af kortoplysninger modtaget hos LCIK i 2020.

Opsummering af misbrug af kortoplysninger

Generelt om misbrug af kortoplysninger

Misbrug af kortoplysninger er det næststørste sagsområde i LCIK målt på antallet af anmeldelser. 13,2 % af alle LCIK's anmeldelser i 2020 handlede om misbrug af kortoplysninger.

På trods af, at sagområdet er det næststørste i LCIK, er antallet af anmeldelser om misbrug af kortoplysninger faldet ca. en tredjedel siden 2019. Faldet skyldes blandt andet den nye opgørelsesmetode i årsrapporten 2020, hvor alle underforhold som er genereret af anmeldelser gennem LCIK's API-løsning, er udeladt.

Antallet af anmeldelser om misbrug af kortoplysninger er faldet fra februar og frem til juni måned. Herefter er antallet af anmeldelser steget resten af året.

Justitsministeriets offerundersøgelse

Ifølge den seneste offerundersøgelse har godt to tredjedele af de ofre, der i 2019 angav, at de inden for det seneste år havde været udsat for kriminalitet begået på internettet, været udsat for misbrug af betalingskortoplysninger. Det svarer til, at 3 % af befolkningen i alderen 16-74 år var udsat for misbrug af betalingskortoplysninger i 2019.

Ikke alle ofre for misbrug af betalingskortoplysninger anmelder forholdet til politiet. I over halvdelen af tilfældene er forholdet ikke anmeldt til politiet af ofrene. Blot 16 % af ofrene anmeldte forholdet til politiet, mens politiet i 27 % af tilfældene fik kendskab om forholdet på anden vis, fx gennem den forurettedes bank eller kreditkortselskab.

Umiddelbart ser det ud til, at ældre aldersgrupper er mere udsat for misbrug af deres betalingskortoplysninger. Undersøgelsens ældste aldersgruppe (40-74 år) er statistisk signifikant mere udsat end undersøgelsens yngste aldersgruppe (16-24 år).

Ofrene for misbrug af kortoplysninger angiver hyppigst, at deres tab beløber sig til et sted imellem 500 – 2.999 kr. 49 pct. af ofrene har angivet et tab i denne størrelsesorden. I de fleste tilfælde angiver ofrene at deres bank eller kreditkortselskab har dækket for tabet.

Misbrug af kortoplysninger gennem betalingsapps

Antallet af anmeldelser, hvor kortoplysninger er blevet misbrugt via betalingsapps, er faldet markant. I 2020 var antallet af anmeldelser 275, hvilket svarer til et fald på 86,9 % i forhold til 2019. Dette kan bl.a. skyldes MobilePays indførsel af to-faktor godkendelse.

Webshops

Der er også et markant fald i antallet af anmeldelser, hvor kortoplysninger er blevet misbrugt gennem webshops. Faldet kan skyldes en udbredelse af to-faktor sikkerhedsgodkendelse ved handel på webshops.

Phising/smishing af kortoplysninger

I 2020 er phising/smishing af kortoplysninger den største grund til, at kortoplysninger misbruges. Der var i 2020 1.596 anmeldelser om phising/smishing af kortoplysninger, hvilket svarer til en stigning på 42,9 % i forhold til 2019. Det formodes, at nedlukningen af samfundet grundet COVID-19, har medført øget handelsaktivitet online, hvor betalingskortoplysninger er blevet benyttet, og at det har givet kriminelle mulighed for at tilegne sig flere kortoplysninger end normalt. Antallet af anmeldelser vedrørende phising/smishing af kortoplysninger kan dog være behæftet med usikkerhed på grund af LCIK's registreringspraksis (se side 27).

Spilsites

Misbrug af betalingskort gennem/på spilsites er stadig et relativt lille fænomen. I 2020 var der 30 anmeldelser om misbrug af kortoplysninger via spilsites. I 2019 var det tilsvarende tal 98 anmeldelser.

Kilde: Justitsministeriets Forskningskontor. (2020). Udsathed for vold og andre former for kriminalitet, *Offerundersøgelserne 2005-2019.*

Kreditbedrageri

POLITI

Beskrivelse af kreditbedrageri

Om kreditbedrageri

Kreditbedrageri bliver typisk opdaget ved, at en borger modtager opkrævninger for finansielle ydelser, som vedkommende ikke kender til. I andre tilfælde kan det være borgere på overførselsindkomst (fx førtidspension eller dagpenge), der opdager, at de ikke længere modtager deres ydelser på deres NemKonto.

Gerningspersonen har i disse tilfælde haft adgang til borgerens personlige oplysninger og NemID, og har brugt oplysningerne til at optage lån og kredit i vedkommendes navn eller ændre NemKontoen, så ydelserne tilfalder en konto, som gerningspersonen har valgt.

Gerningspersoner får typisk adgang til NemID og personoplysninger (cpr-nummer etc.) gennem opkald hvor gerningspersonen udgiver sig for at være fra bank, myndigheder eller lignende også kaldet" Vishing" eller ved på anden måde at franarre oplysningerne fra den forurettede person.

Kreditbedrageri foregår som oftest ved, at gerningspersonerne benytter enten falske eller stjålne identiteter. Der er også tilfælde, hvor gerningspersonerne bruger falske dokumenter til at optage kredit.

Kreditbedragerier med falsk eller stjålen identitet

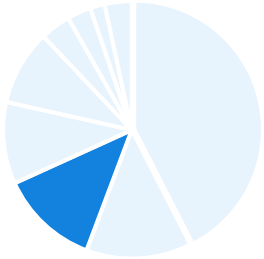
En gerningsperson har fået adgang til en borgers personoplysninger, som gør det muligt at misbruge vedkommendes identitet. Identiteten bliver misbrugt til at oprette lån eller leasingaftaler, hvorved låne- og leasingvirksomheder bliver bedraget til at overdrage penge eller en bil. Efterfølgende oplever virksomheden, at der ikke bliver betalt ydelse på kreditaftalen, og virksomheden forsøger at inddrive gælden hos den person, hvis identitet er misbrugt.

Flere virksomheder tilbyder i dag kunderne at købe varer på afbetaling, hvoraf nogle virksomheder specialiserer sig i udelukkende at tilbyde afbetalingsaftaler (kreditaftale) for varer købt hos andre virksomheder. Fx kan man i dag købe en ny iPhone hos virksomhed A, mens virksomhed B tilbyder at hjælpe forbrugeren med at finansiere telefonen. Disse afbetalingsløsninger bliver sommetider udnyttet af gerningspersoner, der misbruger andres personoplysninger til at oprette en afbetalingsaftale.

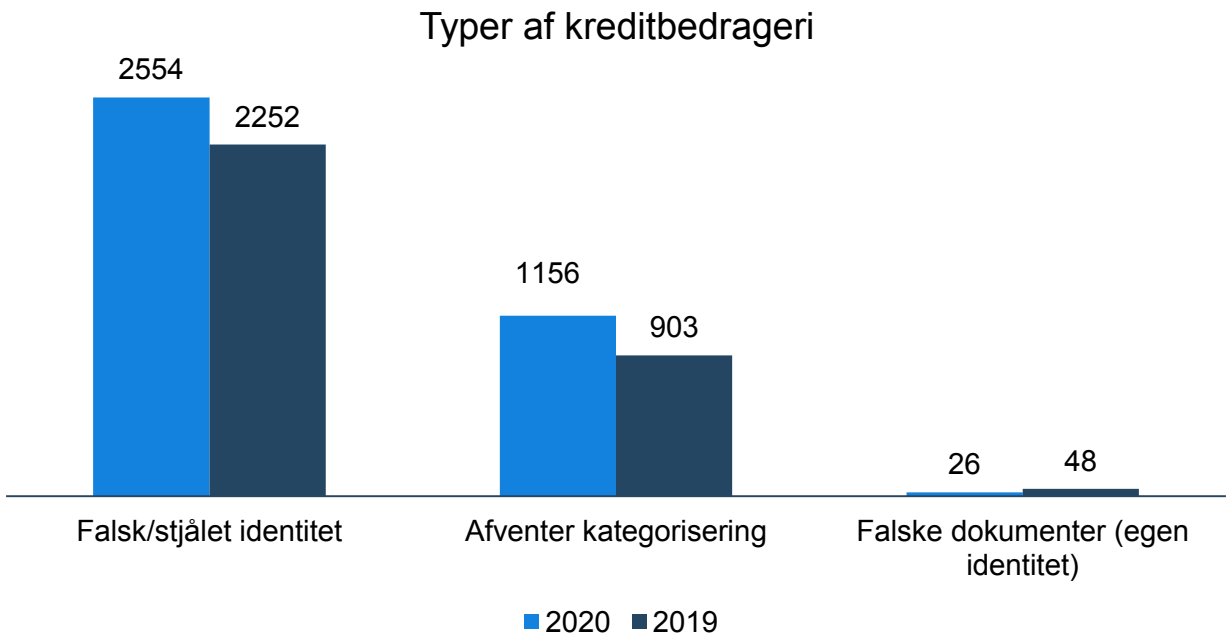
Kreditbedragerier med falske dokumenter

I nogle tilfælde benytter gerningspersoner falske dokumenter til at optage lån eller oprette en betalingsaftale (leasing af bil etc.). De falske dokumenter kan eksempelvis være lønsedler med falske tal eller falske lønindberetninger.

De fleste kreditbedragerier bliver stadig begået med falsk eller stjålet identitet



12,5% af anmeldelserne til LCIK i 2020 handlede om kreditbedrageri (3.736).



Antallet af anmeldelser om kreditbedrageri er steget i 2020

Sammenlignet med 2019 er antallet af anmeldelser om kreditbedrageri steget med 16,6 %.

Kreditbedrageri med falsk eller stjålen identitet

De fleste kreditbedragerier blev både i 2019 og 2020 begået af gerningspersoner, der enten benyttede falske eller stjålne identiteter til at optage kredit i en anden persons navn. Fra 2019 til 2020 ses en stigning på 13,4 %.

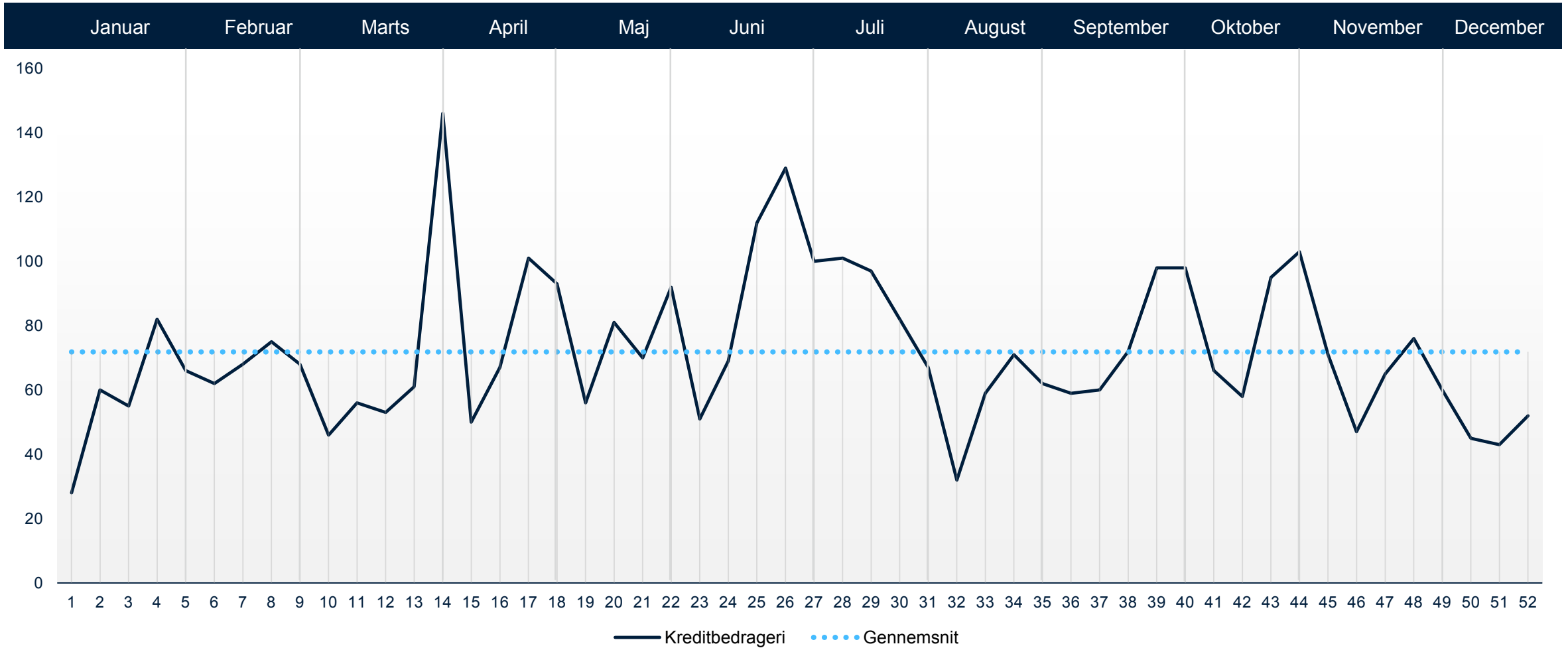
Få anmeldelser om kreditbedrageri med falske dokumenter

Anmeldelser om kreditbedrageri, hvor gerningspersoner manipulerer med eller benyttet falske dokumenter er mere sjældne. LCIK modtog i 2020 26 anmeldelser om denne type.

Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.

Anmeldelsestidspunkt for alle kreditbedragerier fordelt på uger

Der har været flere perioder med ”bølger” af kreditbedrageri henover året



Base: (3.736) Antal anmeldelser om kreditbedrageri modtaget hos LCIK i 2020.

Opsummering af kreditbedrageri

Om kreditbedrageri

LCIK modtog i 2020 3.736 anmeldelser om kreditbedrageri, hvilket gør det til LCIK's tredjestørste sagsområde. Der er tale om en stigning i antallet af anmeldelser om kreditbedrageri på 16,6 %. i forhold til 2019.

Anmeldelserne er anmeldt i "bølger" henover året med særligt mange anmeldelser i sommerperioden (juni og juli). Anmeldelser i bølger kan være et udtryk for, at selskaberne, som anmelder kreditbedrageri, samler en række anmeldelser til bunke før de vælger at anmelde til LCIK.

LCIK kan igen i 2020 konstatere, at de fleste anmeldte kreditbedragerier bliver begået med enten en falsk eller en stjålen identitet. I 2020 modtog LCIK i alt 2.554 anmeldelser om kreditbedrageri med falsk/stjålet identitet, hvilket er 13,4 % flere end i 2019.

Kreditbedrageri med falske dokumenter, hvor gerningspersonen har benyttet egen identitet, er stadig et relativt sjældent fænomen, idet LCIK kun modtog 26 anmeldelser om sådanne tilfælde.

Det er efterforskernes erfaring, at anmeldelser om kreditbedrageri ofte omhandler flere ulovlige forhold. Disse forhold oprettes i politikredsene under den videre efterforskning af sagen. Hvis forholdene var blevet oprettet i LCIK under den indledende efterforskning, ville antallet af kreditbedragerier formentligt være væsentligt højere.

Justitsministeriets offerundersøgelse

Mere end to tredjedele af kreditbedragerier i 2020 er gennemført med falske/stjålne identiteter. Anmeldelsestallene tyder derfor på, at der i 2020 har været udfordringer med personer, der har fået misbrugt deres personoplysninger af kriminelle, som fx har oprettet lån og bestilt varer i deres navn.

Netop problematikken med misbrug af personoplysninger er berørt i den nyeste udgave af offerundersøgelsen fra Justitsministeriets forskningskontor (2020).

Offerundersøgelsen definerer misbrug af personoplysninger på følgende måde: En person har anvendt ofrets personoplysninger (fx navn, cpr-nummer eller mailkonto) eller identitetsbeviser (fx kørekort eller sygesikringsbevis) med henblik på at opnå en økonomisk gevinst fx ved at bestille varer/ydelser eller oprette abonnementer i ofrets navn.

9 % af ofrene for kriminalitet begået på internettet har været udsat for misbrug af personoplysninger over internettet inden for det seneste år. Det svarer til, at 0,4 % af befolkningen i alderen 16-74 år var udsat for denne form for kriminalitet begået på internettet i 2019.

Knap en tredjedel af ofrene for misbrug af personoplysninger ved ikke, hvordan gerningspersonen har fået adgang til deres oplysninger. Året forinden var der tale om knap halvdelen. Størstedelen af de ofre, der ved hvordan gerningspersonen har fået deres oplysninger, angiver, at gerningspersonen brød ind i deres private computer, fx ved hacking eller malware*.

Omkring en femtedel af ofrene for misbrug af personoplysninger opdagede ikke selv, at deres oplysninger blev misbrugt, men blev gjort opmærksom på det af fx venner, familie eller bank. Sidste år udgjorde denne andel knap halvdelen af ofrene.

Kilde: Justitsministeriets forskningskontor. (2020). Udsathed for vold og andre former for kriminalitet, *Offerundersøgelserne 2005-2019*.
*Det er LCIK's erfaring, at ofrene har en anden opfattelse af, hvad der defineres som hacking, end den definition som fagpersoner og politiet bruger

Misbrug af adgang til netbank m.m.

POLITI

Beskrivelse af misbrug af adgang til netbank m.m.

Om misbrug af adgang til netbank m.m.

Ud over indbrud i netbank forsøger it-kriminelle også at få adgang til platforme, der indeholder en form for virtuel, økonomisk værdi, som de kan omsætte til kontanter eller aktiver. Det kan fx være platforme i form af streamingtjenester, spilplatforme og lignende. LCIK arbejder med tre overordnede kategorier for digitale tjenester, herunder; netbank, anden betalingstjeneste, spil og andre webtjenester..

Misbrug af adgang til netbank

Indbrud i netbank bliver ofte begået efter forudgående kontakt, hvor gerningspersonen typisk ringer til ældre borgere og udgiver sig for at være bankansat, fra en offentlig myndighed eller lignende. Gerningspersonen fortæller, at der er ved at blive gennemført en uretmæssig transaktion, og på den måde lykkes det at overtale den forurettede til at udlevere personoplysninger, NemID og SMS verificeringskoder. Oplysningerne bliver ofte misbrugt allerede under samtalen, som typisk er af længere varighed.

LCIK har erfaret, at kriminalitetsformen ofte omfatter et større netværk af muldyr, der kan medvirke til hvidvask af de penge, som er blevet overført fra den forurettedes konti. I mange tilfælde ses det, at gerningspersonerne laver overførsler i portioner svarende til det beløb, mange bankkunder dagligt kan hæve i pengeautomater. Der er stor forskel på, hvor stort et økonomisk tab den forurettede lider, og der er tale om beløb fra 1.000 kr. til nær 1.000.000 kr. Bankerne godtgør imidlertid ofte de forurettedes tab.

Misbrug af adgang til anden betalingstjeneste

Bonuskortordninger og andre former for konti med opsparede bonuspoint er også i gerningspersonernes interesse. Der er konstateret flere tilfælde af kompromitterede logins til konti med bonusordninger for fx flyrejsende. Pointene bliver herefter brugt af gerningspersonen til at købe varer, rejser og tjenesteydelser.

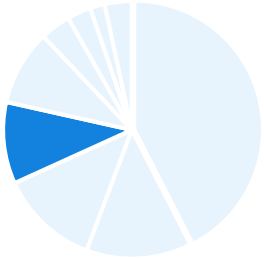
Denne slags misbrug giver typisk tab for under 10.000 kr. for den forurettede.

Misbrug af spil og andre webtjenester

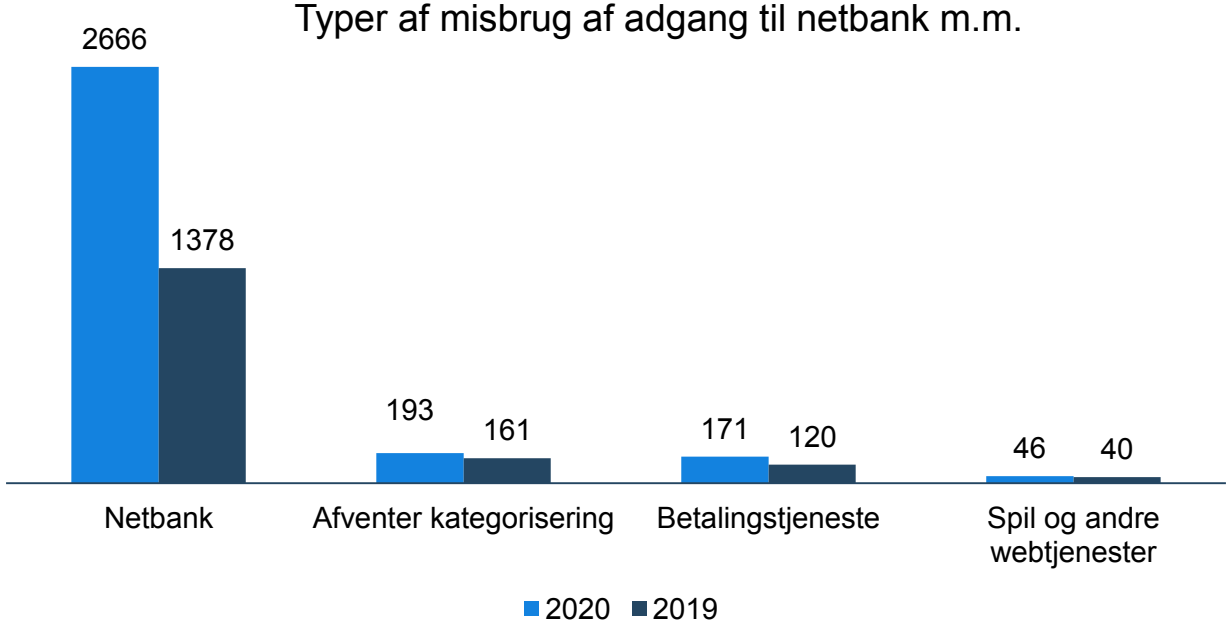
Gerningspersonen skaffer sig adgang til eksisterende brugerkonti på spilplatforme, streamingtjenester og lignende, hvorefter gerningspersonen foretager køb og/eller overfører virtuelle effekter såsom skins, skjolde, våben m.v. Der er også set politianmeldelser, hvor gerningspersonen købte film, streamede sportsevents m.v., hvorved den forurettede led økonomisk tab svarende til værdien af det købte.

Denne slags misbrug giver typisk tab for under 10.000 kr. for den forurettede.

Antallet af anmeldelser om misbrug af adgang til netbank m.m. er steget med 81 %



10,3 % af anmeldelserne til LCIK i 2020 handlede om misbrug af adgang til netbank m.m. (3.076).



Stor stigning i antallet af sager om misbrug af adgang til netbank m.m.

I 2020 modtog LCIK 3.076 anmeldelser om misbrug af netbank m.m., hvilket er en stigning på 81 % i forhold til 2019. Der er tale om en stor stigning, og til denne rapport har LCIK endda benyttet en ny opgørelsesmetode, der mindsker antallet af anmeldelser om misbrug af adgang til netbank m.m.*. Læs mere om den nye opgørelsesmetode i metodeafsnittet på side 83.

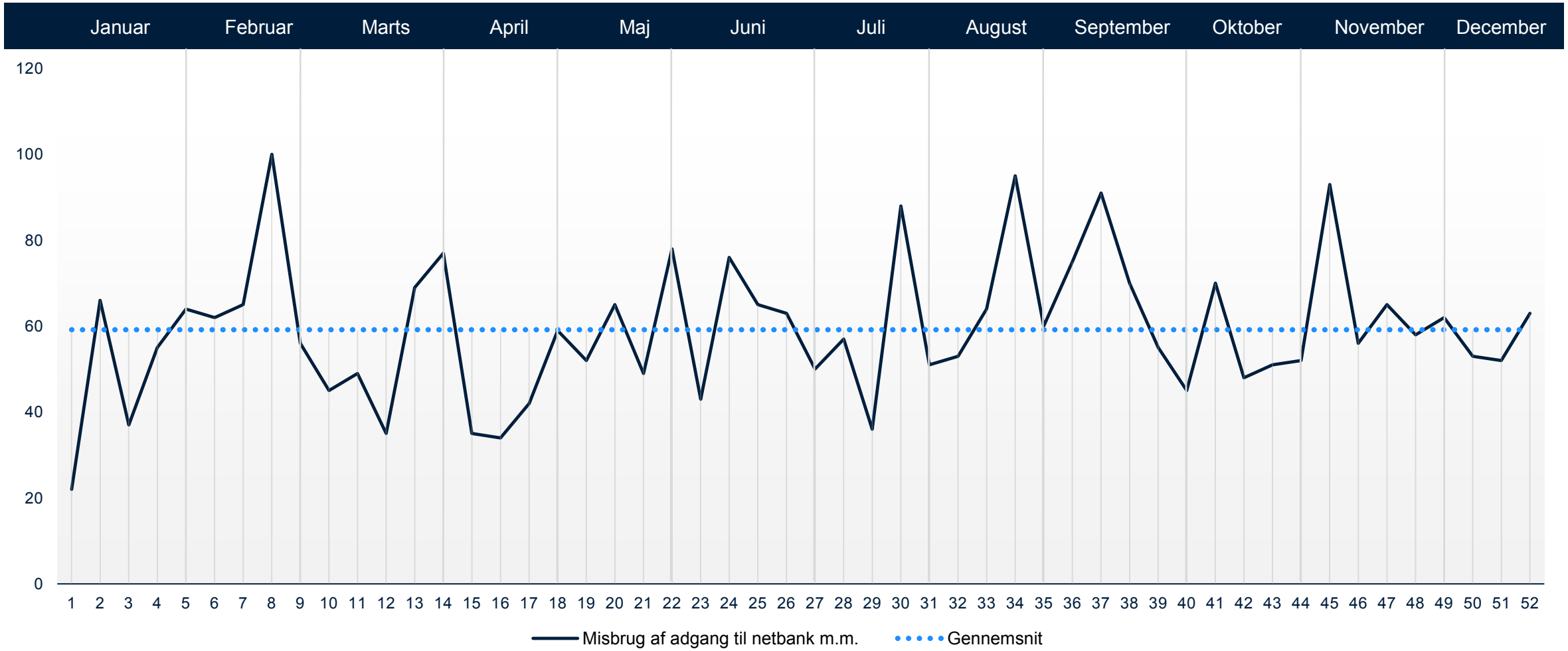
Misbrug af betalingstjenester, spil og andre webtjenester

Målt på anmeldelsestal er misbrug af adgang til betalingstjenester, spil og andre webtjenester stadig et mindre fænomen. På trods af dette var der i 2020 en stigning i antallet af anmeldelser om misbrug af adgang til betalingstjenester på 42,5 %.

Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.

Anmeldelsestidspunkt for misbrug af adgang til netbank m.m. fordelt på uger

Der var udsving i mængden af anmeldelser i løbet af 2020



Base: (3.076) Antal anmeldelser om misbrug af adgang til netbank m.m. modtaget hos LCIK i 2020.

Opsummering af misbrug af adgang til netbank m.m.

Generelt om misbrug af adgang til netbank m.m.

I 2020 modtog LCIK flere anmeldelser om misbrug af adgang til netbank m.m sammenlignet med 2019. Centeret modtog 3.076 anmeldelser om misbrug af adgang til netbank m.m., hvilket svarer til 10,3 % af det samlede antal anmeldelser om it-relateret økonomisk kriminalitet i 2020. Målt i forhold til 2019, er der tale om en stigning på 81 % i antallet af anmeldelser om misbrug af adgang til netbank m.m.

Anmeldelserne blev modtaget i bølger hen over året, hvor der i nogle uger var langt over gennemsnittet. LCIK modtog i gennemsnit 256 anmeldelser om misbrug af adgang til netbank m.m. om måneden. Anmeldelsesmønsteret i bølger kan skyldes, at de professionelle anmeldere, som anmelder misbrug af adgang til netbank m.m., samler en række anmeldelser sammen, før de beslutter at anmelde til LCIK.

Langt de fleste anmeldelser handlede om tilfælde, hvor gerningspersoner har misbrugt adgangen til forurettedes netbank. Tendensen var stigende hen over året. I 2020 modtog LCIK 171 anmeldelser om misbrug af adgang til betalingstjenester. 46 anmeldelser drejede sig om spil og andre webtjenester.

Digital afpresning

POLITI

Beskrivelse af digital afpresning

Om digital afpresning

Afpresningssager inden for it-relateret økonomisk kriminalitet dækker over sager, hvor e-mails med trusler bliver sendt til forurettede. Teksten er ofte på engelsk, men forekommer også på dårligt dansk, der bærer tydeligt præg af at have været igennem en oversættelsesmaskine. Der er dog også eksempler på afpresning via e-mails, hvor både tekst og formuleringer fremstår ganske troværdigt.

Der kan være mange forskellige temaer for digital afpresning. LCIK har bl.a. set et stort antal anmeldelser om afpresning, hvor afsenderen tilkendegiver at have hacket forurettedes computer og derigennem have overvåget forurettedes aktiviteter på internettet over en længere periode. Gerningspersonen påstår at være i besiddelse af browserhistorik, kompromitterende fotos af seksuel karakter og angiver i nogle tilfælde en kode til eksempelvis en e-mailkonto. Koden til e-mailkontoen kan gerningspersonen have erhvervet ved køb på internettet. Gerningspersonen forsøger typisk at presse de forurettede til at overføre mindre beløb i kryptovaluta (Bitcoins m.v.) for ikke at dele afpresningsmaterialet med forurettedes kontakter. Eksemplet illustrerer en typisk masseafpresningssag fra 2020, hvor e-mailen sendes til flere forurettede.

En anden form for afpresning foregår ved ransomware. Ransomware (afpresningssoftware) er betegnelsen for en type malware (skadelig software), som begrænser eller fuldstændig blokerer adgangen til den computer, server eller it-infrastruktur, der inficeres. Formålet er at få forurettede til at betale en løsesum for at få adgang til filerne igen.

Masseafpresning

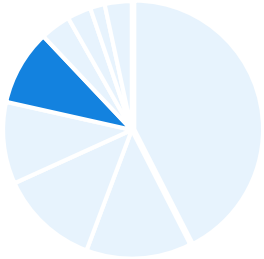
I masseafpresningssager sender gerningspersoner afpresningsmails til mange, tilfældige personer i håb om, at nogle af dem betaler en løsesum. Gerningspersonerne benytter ofte generelle vendinger og har i nogle tilfælde adgang til forældede informationer om forurettede. Det kan give indtryk af, at de har adgang til mere information om forurettede, end det reelt er tilfældet. Teksterne kan bære præg af dårlige formuleringer, især hvis de fremsendes på dansk eller andet nordisk sprog. I de anmeldelser, som LCIK har modtaget i forbindelse med førnævnte eksempel, har ingen forurettede efterkommet gerningspersonens krav.

Afpresning med ransomware

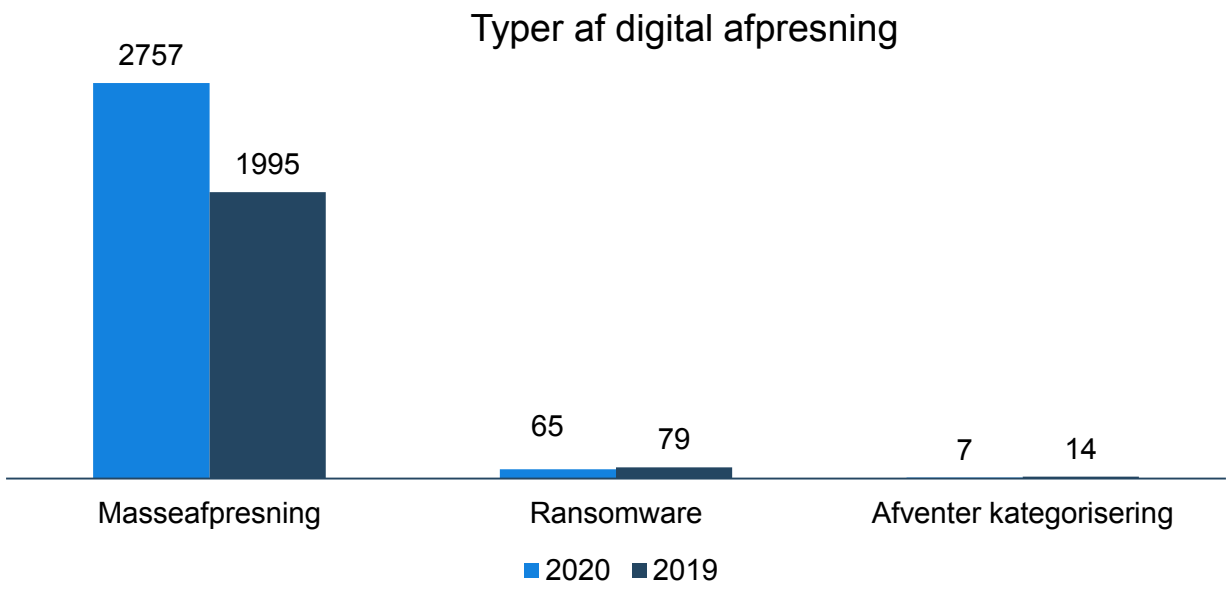
Ransomware rettes mod borgere såvel som virksomheder med en overvægt af sidstnævnte. LCIK har blandt andet set eksempler på ransomware, hvor én eller flere medarbejdere i en virksomhed modtog e-mails med skjulte links til download af filer fra antageligt VPS (virtuel privat server) eller TOR servere, der i løbet af minutter eller timer lod gerningspersonen kryptere filer på servere og cloud-løsninger. Virksomheden blev herved gjort helt eller delvist inoperativ.

I 2020 så LCIK både simple angreb mod borgere og mindre virksomheder og avancerede angreb begået af cyberkriminelle med indgående it-kendskab. Det var kendetegnende for 2020, at gerningspersonerne krævede betaling i kryptovaluta (Bitcoins m.fl.)

De fleste anmeldelser om digital afpresning er masseafpresning



9,5 % af anmeldelserne til LCIK i 2020 handlede om digital afpresning (2.829)



Flere anmeldelser om digital afpresning i 2020

Sammenlignet med 2019 er antallet af anmeldelser om digital afpresning i 2020 steget med 35,5 %. Stigningen viser sig bl.a. i en bølge af afpresningsmails i april.

Sager om masseafpresning driver udviklingen indenfor sagsområdet

I både 2019 og 2020 havde langt de fleste af anmeldelserne karakter af masseafpresning, hvor gerningspersoner sender den samme afpresningsmail i generelle vendinger til mange modtagere på én gang.

Anmeldelser om masseafpresning steg i 2020 med 38,2 %. i forhold til 2019 og resulterer i en generel stigning i sager om digital afpresning.

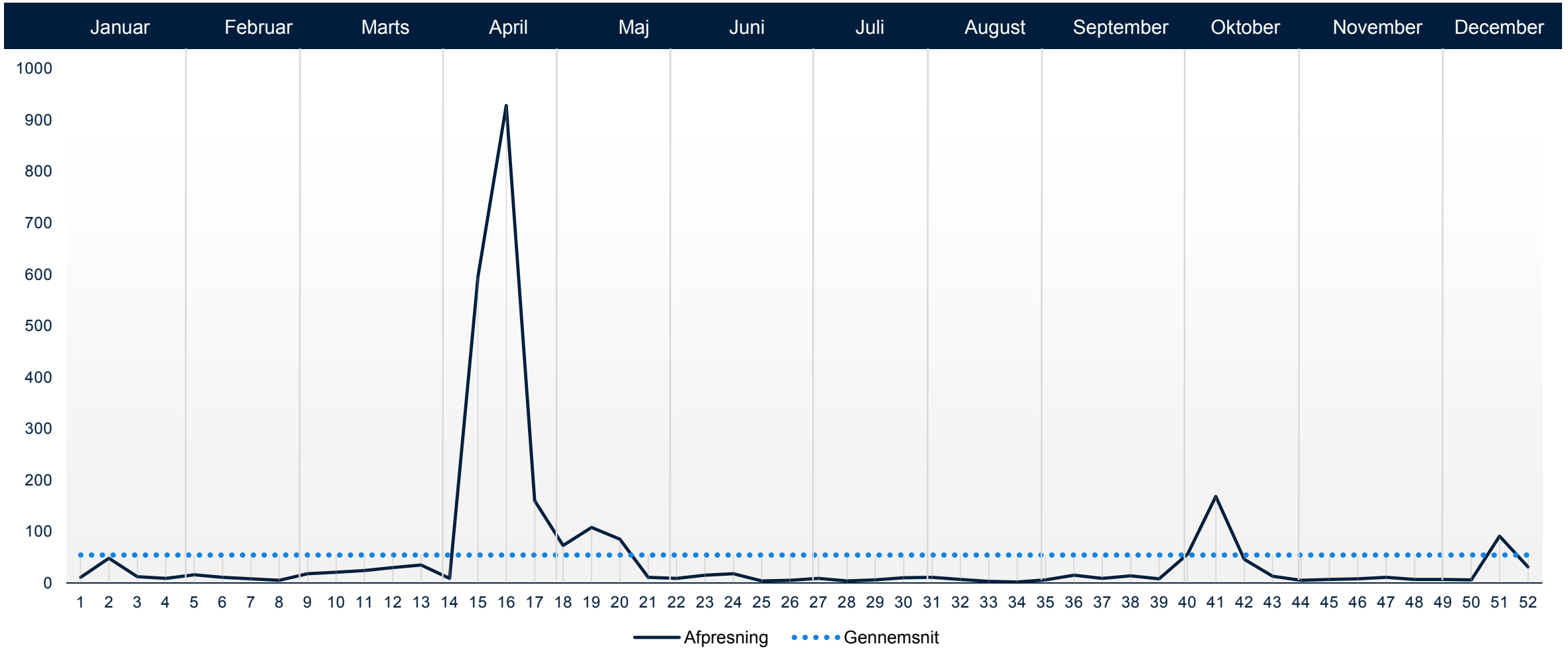
Få anmeldelser om afpresning med ransomware

LCIK modtog i 2020 lidt færre anmeldelser om afpresning med ransomware end i 2019.

Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.

Anmeldelsestidspunkt for digitale afpresningssager fordelt på uger

LCIK modtog et bemærkelsesværdig stort antal sager om masseafpresning i april 2020



Base: (2.829) Antal anmeldelser om digital afpresning modtaget hos LCIK i 2020.

Opsummering af digital afpresning

Om digital afpresning

LCIK modtog i 2020 flere anmeldelser om afpresning over internettet end i 2019. Der er tale om en stigning i anmeldelsestallet på lidt over en tredjedel. Langt størstedelen af anmeldelserne handler om masseafpresningsmails, hvor gerningspersoner sender afpresningsmails i generelle vendinger til mange modtagere. LCIK modtog i 2020 2.757 anmeldelser om masseafpresning. Det svarer til 97,5 % af alle modtagne anmeldelser om afpresning, og udgør en stigning på 38,2 % i forhold til antallet af anmeldelser om masseafpresning i 2019.

På trods af stigningen i antallet af anmeldte tilfælde af masseafpresning har LCIK i 2020 ikke set tilfælde, hvor den forurettede havde betalt gerningspersonen.

Anmeldelser om afpresning med udgangspunkt i installeret ransomware på forurettedes enhed(er) fyldte også i 2020 relativt lidt med kun 65 anmeldelser. Det svarer til 3,8 % af samtlige modtagne anmeldelser inden for afpresning.

Set ud fra anmeldelsestal er ransomware tilsyneladende kun forekommet i begrænset omfang i løbet af 2020. Ransomware kan dog have store datamæssige og økonomiske konsekvenser for de forurettede i form af mistede data, personoplysninger, private billeder og videoer. Virksomheder kan miste kundedatabaser, bogføringsdata m.m.

Selvom masseafpresning forekommer året rundt, så giver anmeldelsestallene i fra 2020 en klar indikation af, at kriminalitetsformen rammer i bølger hen over året. I april måned oplevede LCIK et massivt antal anmeldelser relateret til en masseafpresningskampagne, hvor gerningsperson(er) truede med at frigive pornografisk materiale knyttet til den forurettede. I mange tilfælde beder gerningspersoner om at få udbetalt et beløb i bitcoins.

Andre undersøgelser

I en undersøgelse foretaget af Digitaliseringsstyrelsen og DK-CERT i 2018 blev 728 personer i alderen 18-74 år spurgt om ransomware. 6 % havde i 2017 været ramt af ransomware på deres computer. Det er en smule lavere end i 2016, hvor ransomware ramte 8 % af respondenterne. Tallene for 2014 og 2015 var henholdsvis 8 og 7 %.

Da de små svarprocenter bygger på få personer, har der i en kategori som ”ransomware” ikke været svar nok til at give et statistisk grundlag for en konklusion. Tallene skal derfor læses med forbehold.

Kriminolog Peter Kruize påpeger, at det er overraskende, at ransomware ikke fylder mere. I 2017 blev verden ramt af et omfattende ransomware-angreb kaldet ”Wannacry”. 230.000 computere i 99 lande blev ramt. Angrebet var primært rettede mod virksomheders computere, og kun få computere blev ramt i Danmark.

I Europols seneste trusselsvurering på cyberområdet (iOCTA 2020: 7) beskrives ransomware som en topprioritet blandt politistyrker i EU landene. Det skyldes den store udbredelse og den store skade, som kriminaliteten kan forårsage. I Danmark er der set flere større ransomware angreb i de senere år. Blandt andet blev Mærsk ramt og i 2019 blev høreapparatfirmaet Demant ramt og mistede et trecifret millionbeløb (DKCERT, 2020).

Kilder: Peter Kruize. (2017). Internetkriminalitet 2017 - *offerundersøgelse om Identitetstyveri, bedrageri, afpresning og chikane i cyberspace.*
Digitaliseringsstyrelsen & DKCERT (2017). *Danskernes informationssikkerhed 2016*.

Kontaktbedrageri mod private

POLITI

Beskrivelse af kontaktbedrageri mod private

Om kontaktbedrageri mod private

Kontaktbedrageri mod privatpersoner foregår ofte ved, at en gerningsperson tager kontakt til en person med henblik på at begå bedrageri og franarre vedkommende penge eller værdier. Selvom det kan være forskelligt, hvilke forklaringer gerningspersonerne bruger til deres bedrageri, bærer flere af bedragerierne præg af *social engineering**.

Kontakten kan både forekomme telefonisk (vishing) eller over e-mail. Gerningspersonerne kan benytte sig af spoofing til at forfalske opkalds-id, så det for modtageren ser ud til, at telefonnummeret er et andet, end det der ringes fra. Der findes ligeledes spoofing i e-mails, hvor afsenderadressen fremstår forfalsket.

Bedragerierne kan udspille sig på flere forskellige måder. LCIK arbejder med f fire overordnede kategorier for kontaktbedrageri.

Microsoftscams

Microsoftscams involverer ikke nødvendigvis en gerningsperson, der udgiver sig for at være fra Microsoft. Det er en betegnelse for denne type svindel.

I 2020 så LCIK en variant, hvor gerningspersoner lokker den forurettede til at udlevere personlige oplysninger, som foto af kørekort, pas, kortoplysninger, NemID og sms-verificeringskoder. I flere tilfælde får gerningspersonen adgang til den forurettedes computer via fjernstyrring under dække af, at det er nødvendigt, for at de kan hjælpe den forurettede med påståede softwareproblemer.

Konsekvenserne er bl.a., at gerningspersonen har oplysninger nok til at begå indbrud i forurettedes netbank, foretage kortbetalinger, kontooverførsler eller misbruge forurettedes identitet på anden vis.

Nigeriabreve

Nigeriabreve involverer ikke nødvendigvis en gerningsperson, der udgiver sig for at være fra Nigeria. Det er en betegnelse for denne type svindel.

Tidligere så politiet anmeldelser om e-mails, hvor der blev lovet store lottogevinster.

I 2020 er den slags anmeldelser afløst af løfter om større pengebeløb knyttet til en arv fra en udenlandsk advokat. Den forurettede kan få andel i arven, hvis vedkommende indvilliger i at agere fjern slægtning. Forud for udbetaling af arven bliver der stillet krav om betaling af arveafgift m.v. af det lovede pengebeløb, som aldrig modtages.

Datingsvindel

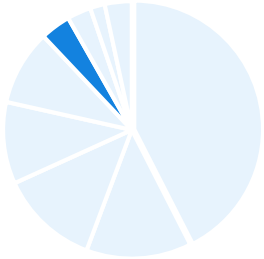
Datingsvindel tager udgangspunkt i, at en person danner relation til en person med falsk identitet via sociale medier fx Tinder, happn, Instagram eller Facebook. Gerningspersonen med den falske identitet udnytter forurettedes følelsesmæssige involvering og lokker penge ud af vedkommende ved konto-til-kontooverførsler eller via Western Union, Ria, Money Gram m.fl. Datingsvindel er karakteriseret ved en relation, som bygges op over en længere periode, og hvor gerningspersonen opnår en stor grad af tillid hos forurettede. Det ender typisk med, at den forurettede overfører flere tusinde kroner til gerningspersonen.

Bekendt i knibe

I 2020 var der også tilfælde, hvor den forurettede blev kontaktet via e-mail af en person, der udgav sig for at være en bekendt af forurettede eller dennes nære relationer. Historien var typisk, at der var opstået en nødsituation i udlandet, og den forurettede blev lokket til at foretage konto til kontooverførsler eller pengeoverførsler via Western Union, Ria, Money Gram m.fl.

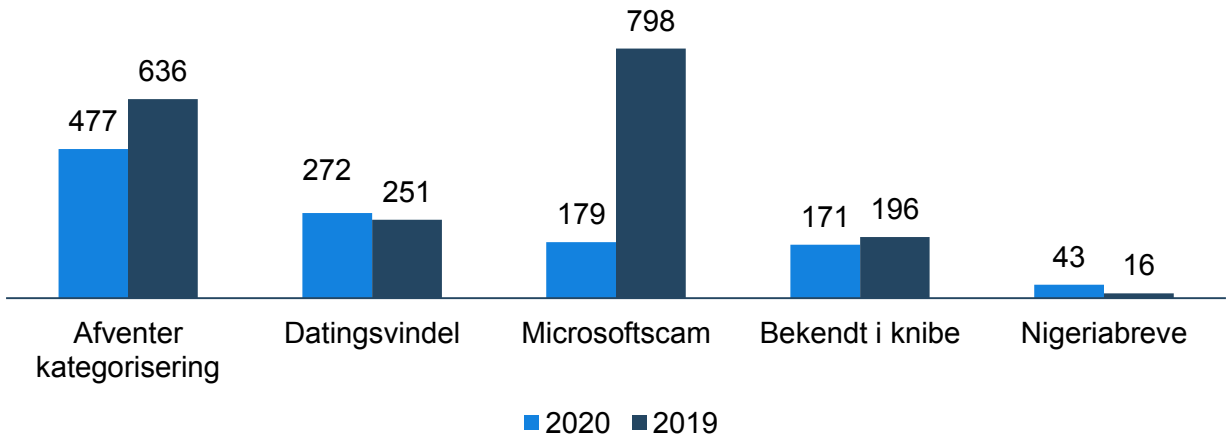
*Note: Social engineering er udbredt begreb inden for cybercrime, der dækker over manipulation af én eller flere personer.

Der har været et markant fald i antallet af kontaktbedragerier i form af microsoftscams



3,8 % af anmeldelser til LCIK i 2020 handlede om kontaktbedrageri mod private (1.142).

Typer af kontaktbedrageri mod private



Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.

Færre anmeldelser om kontaktbedragerier mod private

Fra 2019 til 2020 oplevede LCIK et fald på 39,8 % i antallet af anmeldelser om kontaktbedrageri mod private.

Væsentligt færre anmeldelser om microsoftscams

Det overordnede fald i antallet af kontaktbedragerier er især båret af et fald i antallet af anmeldelser om microsoftscams, som LCIK så færre tilfælde af i 2020. Sammenholdt med sidste år er anmeldelsestallet for kontaktbedragerier i form af microsoftscams faldet med 77,6 %.

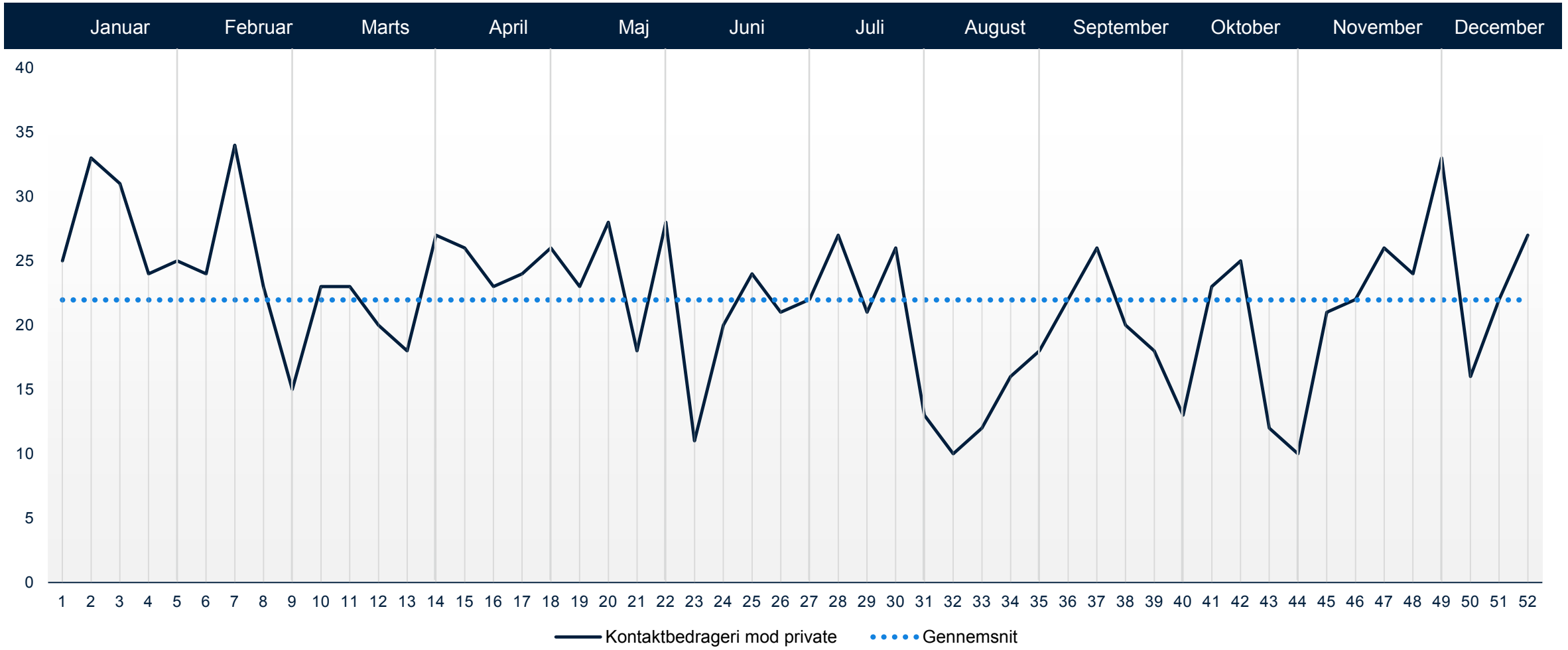
Faldet kan hænge sammen med, at mange kontaktbedragerier i form af microsoftscams ender med et indbrud i den forurettedes netbank, hvilket betyder, at de kategoriseres som misbrug af adgang til netbank m.m.

Andre former for kontaktbedrageri

Antallet af anmeldelser om kontaktbedragerier i form af datingsvindel og bekendt i knibe ligger nogenlunde på niveau med 2019. På trods af en procentuel stor stigning i antallet af anmeldelser om nigeriabreve, er denne form for kontaktbedrageri stadig et mindre fænomen blandt anmeldelserne.

Anmeldelsestidspunkt for kontaktbedrageri mod private fordelt på uger

Der har været udsving i mængden af anmeldelser i løbet af 2020



Base: (1.142) Antal anmeldelser om kontaktbedrageri mod private modtaget hos LCIK i 2020.

Opsummering af kontaktbedrageri mod private

Generelt om kontaktbedrageri mod private

LCIK modtog i 2020 færre anmeldelser kontaktbedrageri mod private.

I løbet af året modtog LCIK 1.142 anmeldelser om kontaktbedrageri mod private, hvilket svarer til et fald på knap 40 % fra 2019.

Samlet set udgjorde sagsområdet 3,8 % af alle anmeldelser om it-relateret økonomisk kriminalitet, som LCIK modtog i 2020.

Det er efterforskernes erfaring, at kontaktbedrageri kan have store økonomiske konsekvenser for den forurettede. Ifølge justitsministeriets seneste offerundersøgelse (2020) er det gennemsnitlige økonomiske tab for personer udsat for kontaktbedrageri 8.299 kr. Det er betydeligt højere end i 2019, hvor undersøgelsens resultater viste et gennemsnitlige tab på ca. 5.000 kr.

Justitsministeriets offerundersøgelse

Ifølge offerundersøgelsen har 8 % af ofrene for kriminalitet begået på internettet i 2019 angivet at have været udsat for kontaktbedrageri over internettet inden for det seneste år. Det svarer til, at 0,3 % af befolkningen i alderen 16-74 år blev udsat for kontaktbedrageri i 2019. Da datagrundlaget er spinkelt, skal resultaterne tolkes varsomt.

Datingsvindel

Anmeldelserne peger på, at datingsvindel – også kaldet romance scam – er den mest hyppige form for kontaktbedrageri i 2020. LCIK modtog i 2020 272 anmeldelser om datingsvindel, hvilket er 8,4 % flere end i 2019.

Bekendt i knibe

Kontaktbedragerier, hvor gerningspersonen udgiver sig for at være en bekendt i knibe udgjorde i 2020 15 %. af anmeldelserne om kontaktbedrageri. Dette modus er altså på niveau med microsoftscams.

Microsoftscams

I 2020 modtog LCIK færre anmeldelser om kontaktbedrageri i form af microsoftscams sammenlignet med 2019. LCIK modtog 179 anmeldelser om microsoftscams, hvilket udgør 15,7 % af alle anmeldte kontaktbedragerier. Antallet af sager om kontaktbedrageri mod private er 78 %. lavere end i 2019.

Nigeriabreve

Kontaktbedrageri mod private i form af nigeriabreve fylder stadig relativt lidt i anmeldelsesbilledet i 2020, hvor LCIK modtog 43 anmeldelser. I 2019 modtog LCIK 16 anmeldelser om nigeriabreve.

Kilde: Justitsministeriets Forskningskontor. (2020). Udsathed for vold og andre former for kriminalitet, *Offerundersøgelserne 2005-2019.*

Kontaktbedrageri mod virksomheder

POLITI

Beskrivelse af kontaktbedragerier mod virksomheder

Om kontaktbedrageri mod virksomheder

En stor del kontaktbedrageri mod virksomheder, myndigheder, foreninger eller andre organisationer er i form af BEC/CEO fraud.

BEC er en forkortelse for den engelske term Business E-mail Compromise. I international sammenhæng kaldes BEC fraud også for EAC fraud (E-mail Account Compromise). BEC fraud sker typisk ved, at en gerningsperson hacker sig adgang til en e-mail korrespondance mellem to eller flere aktører, og på den måde får mulighed for at ændre oplysninger i e-mail korrespondancen, fx kontonummeret på en aftalt pengetransaktion til et kontonummer.

CEO fraud kaldes i Danmark også for direktørsvindel. Ved CEO fraud anvendes ofte spoofing eller typosquatting. Ved spoofing, kan gerningspersonen sende en e-mail, der ser ud til at komme fra en virksomhedsdirektør eller en foreningsformand. Under dække af at være direktøren beder gerningspersonen over e-mail en økonomimedarbejder om at overføre et troværdigt beløb. Ved typosquatting sørger gerningspersonen for, før angrebet, at registrere et domænenavn (en e-mailadresse), der ligger tæt op ad direktørens, således at medarbejderen ikke bemærker, at den genkendelige e-mailadresse afviger. På denne måde udgiver gerningspersonen sig ligeledes for at være direktøren, hvorefter gerningspersonen beder om at få overført et beløb fra medarbejderen.

Kontaktbedrageri mod virksomheder i form af BEC/CEO fraud

I 2020 var der sager, hvor en virksomhed/forening modtog e-mails og i få tilfælde opfølgende telefonopkald fra gerningspersonen, der udgav sig for at være fx direktøren. Af de fremsendte e-mails fremgik det almindeligvis, at der hurtigst muligt skulle overføres større eller mindre beløb til en udenlandsk konto. Før selve betalingsanmodningen spurgte gerningspersonen i flere tilfælde, hvor mange penge der stod på virksomhedens konto.

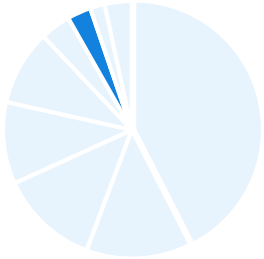
I 2020 var der stor forskel på kvaliteten af BEC/CEO fraud. I de mest simple tilfælde oprettede gerningspersonen fx en gmail med direktørens, virksomhedens eller foreningsformandens navn. I mere sofistikerede tilfælde kompromitterede gerningspersonerne reelt adgangen til virksomhedens eller samarbejdspartnerens mailsystem, anvendte spoofing eller typosquatting.

Kontaktbedrageri mod virksomheder i form af fakturasvindel

Fakturasvindel minder på mange måder om BEC/CEO fraud, idet gerningspersonen prøver at vildlede den økonomiansvarlige i en organisation til at betale en falsk faktura. Det sker typisk ved, at firmaet modtager en faktura fra gerningspersonen på e-mail, hvor modtagerkontoen er ændret til en konto kontrolleret af gerningspersonen.

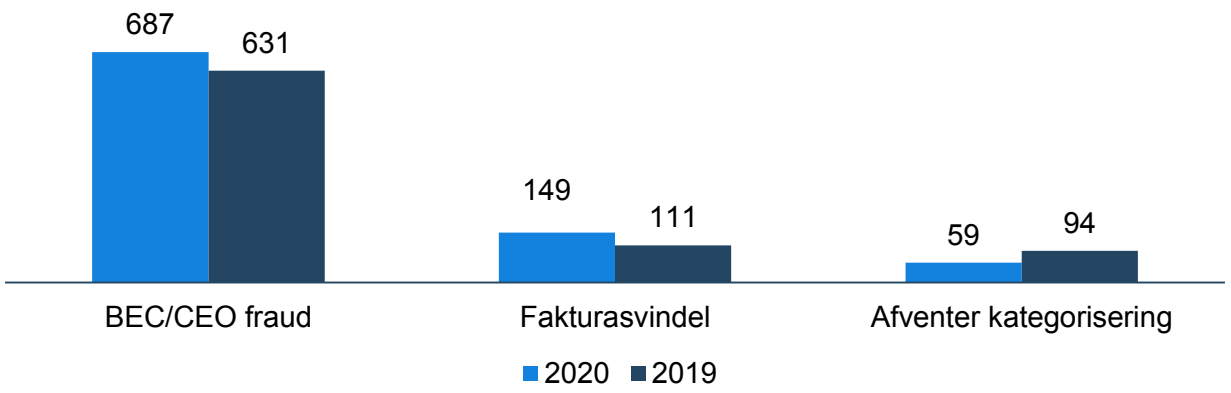
I mindre omfang er der også set kontaktbedrageri, der tager udgangspunkt i falske fakturaer. Disse sager er ofte kendetegnet ved, at forurettede modtager fakturaer på varer eller ydelser, de ikke har modtaget. I disse sager er der - foruden bedrageri - ofte tale om dokumentfalsk i form af falske eller forfalskede fakturaer. Der er således tale om tilfælde af både fremsendelse af ægte fakturaer, som gerningspersonen har tilegnet sig, og falske fakturaer, hvor gerningspersonen opfandt sit eget firma.

Antallet af anmeldelser om kontaktbedrageri mod virksomheder steg fra 2019 til 2020



3 % af anmeldelserne til LCIK i 2020 handlede om kontaktbedrageri mod virksomheder (895).

Typer af kontaktbedrageri mod virksomheder



Flere anmeldelser om kontaktbedrageri mod virksomheder

Der blev i 2020 anmeldt flere kontaktbedragerier mod virksomheder end i 2019. De fleste af disse kontaktbedragerier var i form af BEC (business e-mail compromise) og CEO fraud. Antallet af anmeldelser om kontaktbedrageri mod virksomheder er steget med 7,1 % fra 2019 til 2020.

Flere tilfælde af BEC/CEO fraud

Både i 2019 og 2020 var de fleste anmeldte kontaktbedragerier i form af BEC/CEO fraud. Fra 2019 til 2020 ses en stigning i antallet af anmeldte BEC/CEO-fraud tilfælde på 8,9 %.

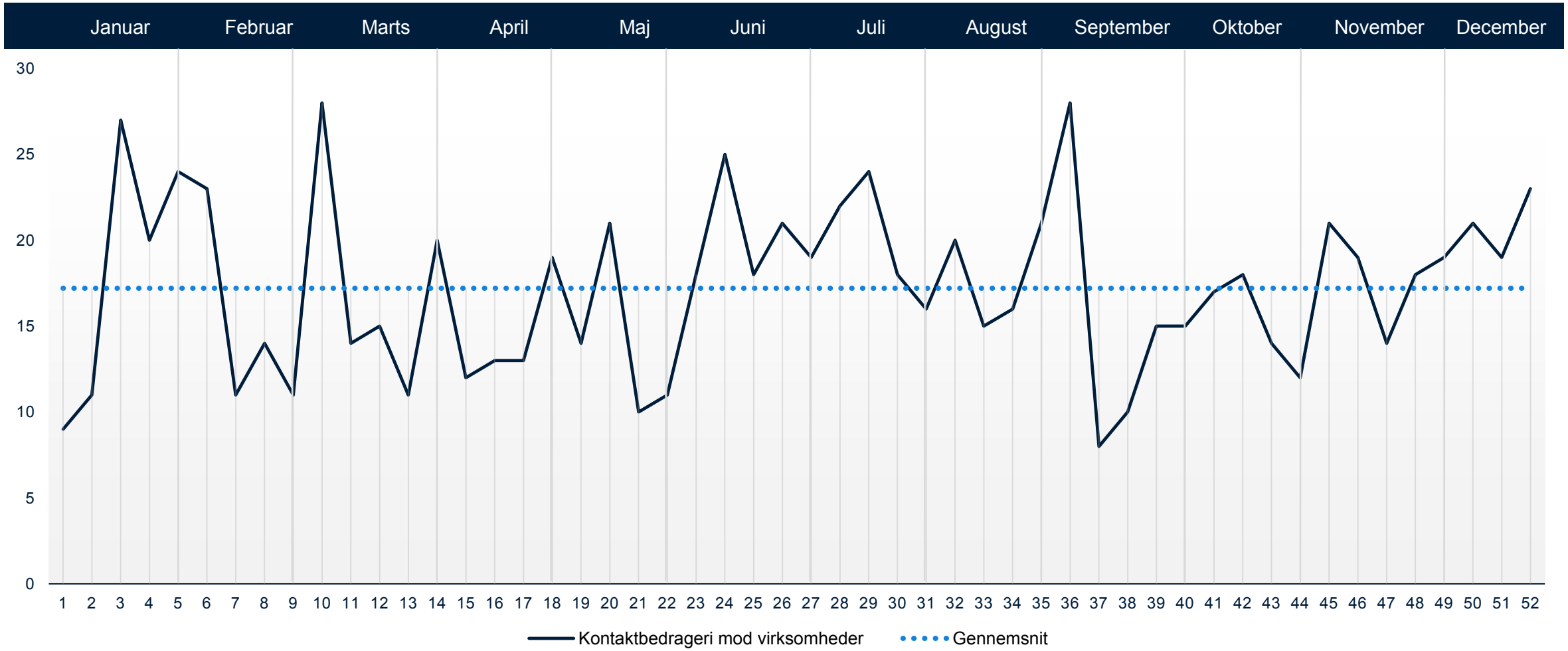
Flere anmeldelser om fakturasvindel

I 2020 var der 149 anmeldelser om kontaktbedrageri i form af fakturasvindel. Det er 38 anmeldelser flere end i 2019.

Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.

Anmeldelsestidspunkt for kontaktbedrageri mod virksomheder fordelt på uger

Der har været udsving i mængden af anmeldelser i løbet af 2020



Base: (895) Antal anmeldelser vedrørende kontaktbedrageri mod virksomheder modtaget hos LCIK i 2020.

Opsummering af kontaktbedrageri mod virksomheder

Generelt om kontaktbedrageri mod virksomheder

LCIK modtog 895 anmeldelser om kontaktbedrageri mod virksomheder i 2020. Det svarer til 3 % af det samlede antal anmeldelser, som LCIK modtog i 2020. Derudover svarer det til en stigning på 7 % i forhold til 2019, hvor LCIK modtog 836 anmeldelser om kontaktbedrageri mod virksomheder.

I 2020 modtog LCIK i gennemsnit ca. 75 anmeldelser om kontaktbedrageri mod virksomheder om måneden.

Det primære kriminelle modus for kontaktbedrageri mod virksomheder er BEC/CEO fraud, der tegner sig for 76,8 % af anmeldelserne i 2020. Det svarer til 687 anmeldelser. Ligesom ved kontaktbedrageri mod private kommer anmeldelserne i bølger henover året. Tallene peger altså på, at virksomheder – såfremt disse anmelder BEC/CEO fraud relativt hurtigt – især udsættes for denne form for bedrageri i sommermånederne, hvor mange ansatte afvikler ferie og derfor ikke har daglig kontakt til hinanden. Netop denne situation skaber gunstige vilkår for udførslen af BEC/CEO fraud.

Fakturasvindel er et væsentligt mindre anmeldt fænomen end BEC/CEO Fraud. Fakturasvindel er anmeldt 149 gange i 2020, hvilket svarer til en stigning på 34 % i forhold til 2019.

Fuphjemmesider

POLITI

Beskrivelse af fuphjemmesider

Om fuphjemmesider

It-kriminelle benytter fuphjemmesider til at begå bedrageri. Fuphjemmesider kan være falske webshops, hvor webshoppen aldrig sender de varer, som kunderne har købt, og hvor der typisk er tale om samhandelsbedrageri.

I 2020 har der også været fuphjemmesider, der med et godt tilbud lokkede kunder til at købe en vare på fuphjemmesiden. Ved købet accepterer kunden ubevidst en abonnementsaftale, der kontinuerligt trækker beløb fra kundens konto. Dette kaldes også for abonnementsfælder.

Sidst men ikke mindst bliver fuphjemmesider også benyttet som redskab til at lokke forurettede personer ind i falske låne- og investeringsmuligheder.

I mange tilfælde har fuphjemmesiderne annoncer på legitime hjemmesider, hvor de forurettede får øje på dem. Dette kan fx være i form af bannerreklamer på diverse fora og annonceringer på sociale medier.

LCIK beskæftiger sig kun med fuphjemmesider i det omfang, at der eksisterer et bedrageriforhold. Sager om selve fuphjemmesiden eller brud på markedsføringsloven er uden for LCIK's sagsområder.

Fuphjemmesider i form af falske låne- og investeringsmuligheder

Fuphjemmesider i form af falske låne- og investeringsmuligheder var i 2020 præget af en overvægt til sidstnævnte og typisk i forbindelse med fiktive handler med kryptovaluta (Bitcoins m.v). De forurettede reagerede ofte på annoncer på legitime websites (nyhedsmedier, sociale medier m.v.) og på fuphjemmesider, der til forveksling lignede danske legitime nyhedsmedier.

I årets løb var der flere anmeldelser fra forurettede, der reagerede på indhold hvor billeder af kendte danske mediepersonligheder blev brugt i falske nyhedshistorier og annoncer om investeringer i kryptovaluta.

Sagens gang

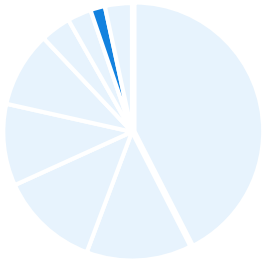
Indledningsvist er der ofte tale om en startinvestering på et mindre beløb (omkring 250 EUR) for den forurettede, som ofte overføres via kortbetaling. I forbindelse med oprettelsen som "investor" hos det såkaldte investeringsselskab får forurettede adgang til en fuphjemmeside, hvor investeringens udvikling kan følges. Efter oprettelsen bliver forurettede typisk ringet op af en gerningsperson, der udgiver sig for at være en børsmægler.

Den falske børsmægler gennemgår fuphjemmesidens funktioner, og med løfte om endnu større gevinster overtales forurettede til at foretage yderligere investeringer - oftest som kontooverførsler til udlandet. I nogle tilfælde er der daglig telefon- og e-mail kontakt mellem børsmægleren (gerningsperson) og forurettede. Denne kontakt har i nogle tilfælde løbet over et år.

I enkelte tilfælde får gerningspersonerne overtalt forurettede til at optage forbrugslån med henblik på investering, og nogle gange overtager gerningspersonen også forurettedes computer og netbank via TeamViever og Any Desk, hvorefter gerningspersonen med forurettedes personlige oplysninger kan foretage kontooverførsler.

Når den forurettede ønsker at hæve sit indestående, kan det ikke lade sig gøre, og forurettede opdager bedrageriet. I flere tilfælde er de forurettede herefter blevet kontaktet af gerningspersonerne, som påstår, at de vil assistere med at få pengene igen via "recovery". Dette er oftest endt ud i, at de forurettede er blevet svindlet på ny ved at betale for "gebyrer mv."

Stigning i antallet af anmeldelser om fuphjemmesider



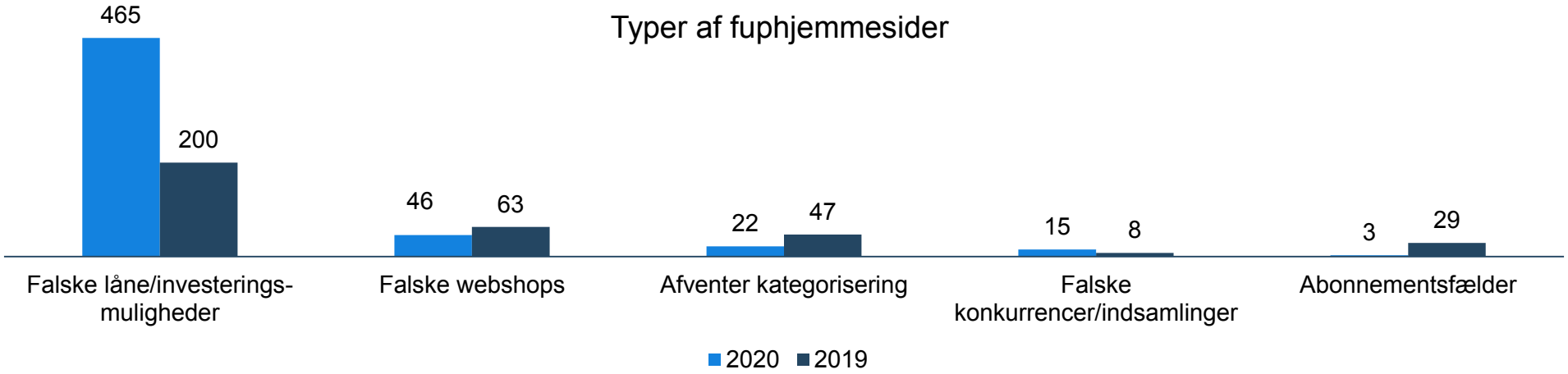
1,8% af anmeldelserne til LCIK i 2020 handlede om fuphjemmesider (551).

Sagsområdet er steget med 58,8 %

Der blev i 2020 anmeldt 551 tilfælde af bedrageri gennem fuphjemmesider. Det svarer til en stigning i anmeldelsestallet på 58,8 % i forhold til 2019. De fleste af anmeldelser om fuphjemmesider vedrører hjemmesider, der har til formål at franarre brugernes penge ved at lokke med falske låne- eller investeringsmuligheder.

Anmeldelser om falske låne/investeringsmuligheder er steget markant i 2020

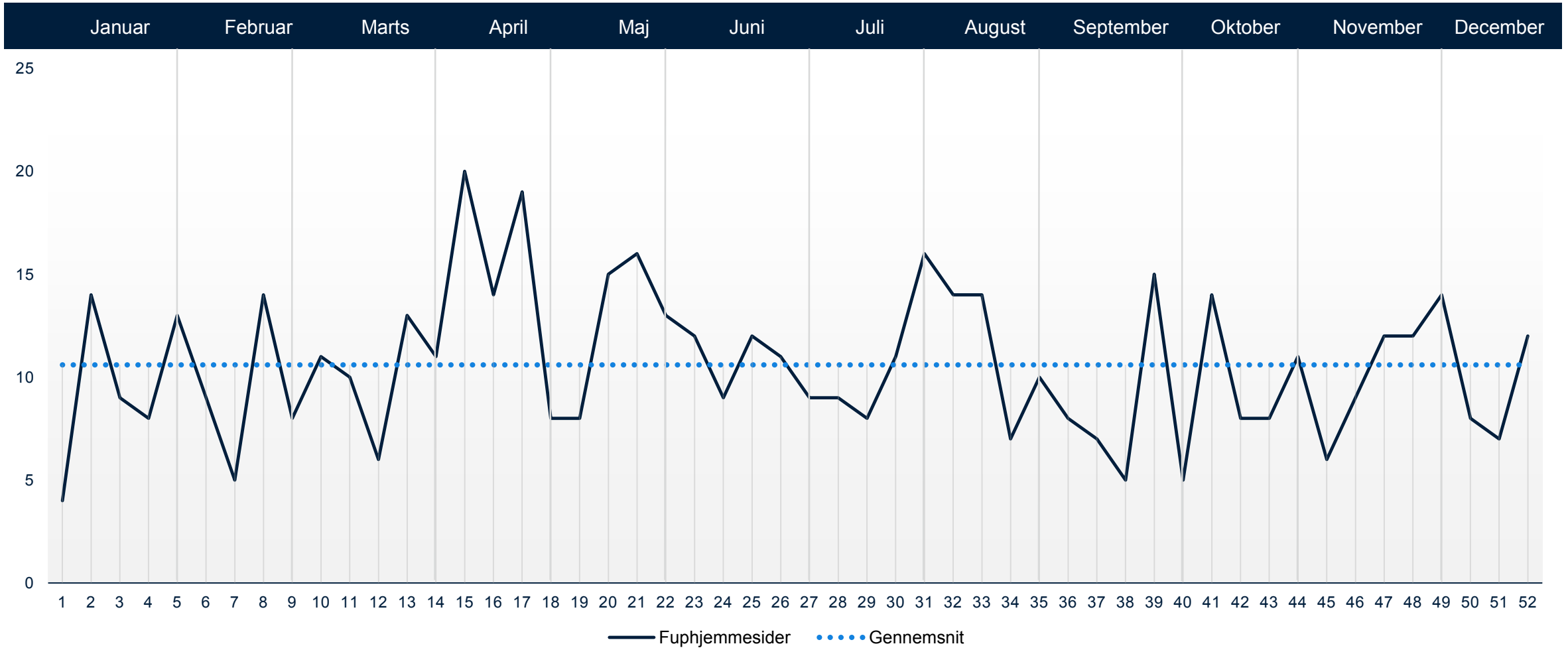
I 2020 har der været en stigning på 132,5 % i antallet af anmeldte fuphjemmesider, der tilbyder falske låne- eller investeringsmuligheder. Stigningen kan blandt andet skyldes den store investeringsinteresse blandt private investorer under coronaepedimien* og at flere pengeinstitutter har indført negative renter for indestående af en vis størrelse.



Base: (29.905) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos LCIK i 2020.
*Kilde: Finans (2020): *Danskerne handler danske aktier som aldrig før*. URL: https://finans.dk/privatokonomi/ECE12772369/danskerne-handler-danske-aktier-som-aldrig-foer/?ctxref=forside

Anmeldelsestidspunkt for bedragerier på fuphjemmesider fordelt på uger

Der har været udsving i mængden af anmeldelser i løbet af 2020



Base: (551) Antal anmeldelser om bedrageri på fuphjemmesider modtaget hos LCIK i 2020.

Opsummering af fuphjemmesider

Generelt om fuphjemmesider

I 2020 modtog LCIK 551 anmeldelser om fuphjemmesider. Det svarer til en stigning i antallet af anmeldelser på 59 %.

I løbet af 2020 blev der anmeldt 465 fuphjemmesider relateret til falske låne- og investeringsmuligheder. Det svarer til en stigning på 113 pct. i forhold til sidste år. Dette modus ved fuphjemmesider er det mest hyppige og falske låne- og investeringsmuligheder udgør 84,4 pct. af anmeldelserne om fuphjemmesider i 2020. Falske låne- og investeringsmuligheder var ligeledes det hyppigste modus i forbindelse med fuphjemmesider i 2019.

Den store stigning i antallet af anmeldte fuphjemmesider vedrørende falske låne- eller investeringsmuligheder kan skyldes det negative rentemiljø og coronanedlukningen, der har givet en række private investorer incitament og tid til at kaste sig over private investeringer i 2020.

Udover anmeldelser om falske låne/investeringsmuligheder, modtog LCIK i 2020 46 anmeldelser om falske webshops. Fuphjemmesider, der tager udgangspunkt i falske konkurrencer/indsamlinger og abonnementsfælder, er stadig et relativt lille fænomen blandt anmeldelserne, og LCIK modtog blot hhv. 15 og 3 anmeldelser om denne slags fuphjemmesider.

Forurettede i sager om it-relateret økonomisk kriminalitet

POLITI

Antal forurettede udsat for it-relateret økonomisk kriminalitet i 2020

23.764 forskellige personer

har været udsat it-relateret økonomisk kriminalitet.

1.229 forskellige professionelle

har været udsat it-relateret økonomisk kriminalitet.

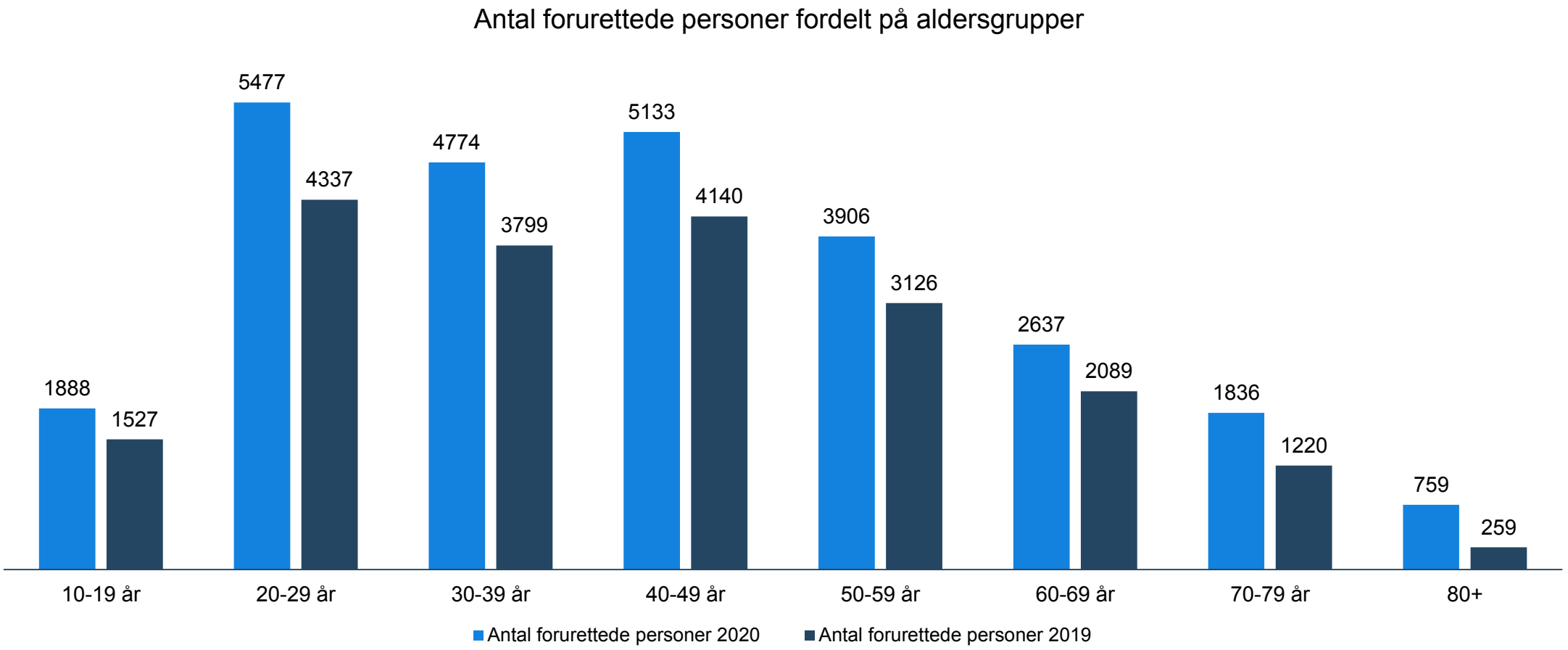
Om de forurettede

Denne del af rapporten tager udgangspunkt i de personer, som har været ofre for it-relateret økonomisk kriminalitet i 2020. I strafferetslige termer benævnes ofret for kriminalitet ofte som den forurettede part i sagen. Derfor bruges betegnelsen 'forurettede' om ofrene for it-relateret økonomisk kriminalitet i årsrapporten.

For mere detaljeret viden om hvilke personkategorier som gruppen af forurettede består af, henvises til side 82.

Langt de fleste forurettede har også selv anmeldt den kriminalitet, de har været udsat for og fremgår med personkategorien A/F (anmelder og forurettet). Derfor er der ikke store forskelle mellem anmelderne af it-relateret økonomisk kriminalitet og de forurettede heraf. Personkategorien FOU dækker over personer eller organisationer, som har været forurettet i forbindelse med et kriminelt forhold, og som ikke selv har anmeldt. De to kategorier udgør samlet set gruppen af forurettede for it-relateret økonomisk kriminalitet.

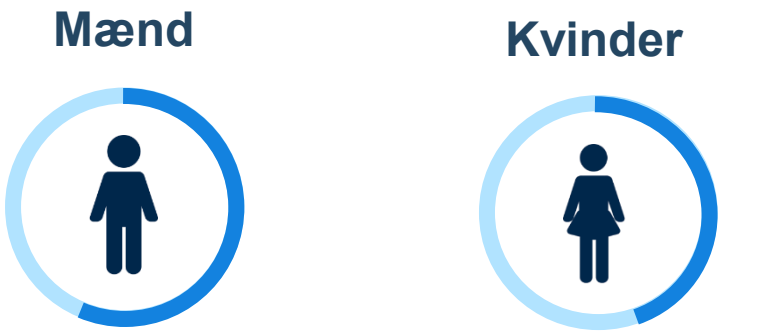
Stigningen i it-relateret økonomisk kriminalitet har ramt alle aldersgrupper



Base: (26.410) Private forurettede af it-relateret økonomisk kriminalitet anmeldt til LCIK i 2020.

Flere mænd end kvinder er udsat for it-relateret økonomisk kriminalitet

Kønsfordeling blandt forurettede



Kønsfordeling

Med udgangspunkt i anmeldelser til LCIK er flere mænd end kvinder i 2020 blev udsat for it-relateret økonomisk kriminalitet. Der er i alt tilknyttet 26.410 forurettede personer på de anmeldelser, som LCIK modtog i 2020. 14.358 af dem er mænd, imens 12.052 er kvinder.

Da langt de fleste forurettede også er anmeldere af kriminaliteten, kan det ikke udelukkes, at mænd blot er bedre til at anmelde denne type kriminalitet og ikke er mere udsatte end kvinderne.

De forurettede mænd er i gennemsnit yngre end kvinderne

Den gennemsnitlige alder for de forurettede er 43,1 år. Mændenes gennemsnitsalder er 41,1 år, imens gennemsnitsalderen for kvinder er 45,5 år.

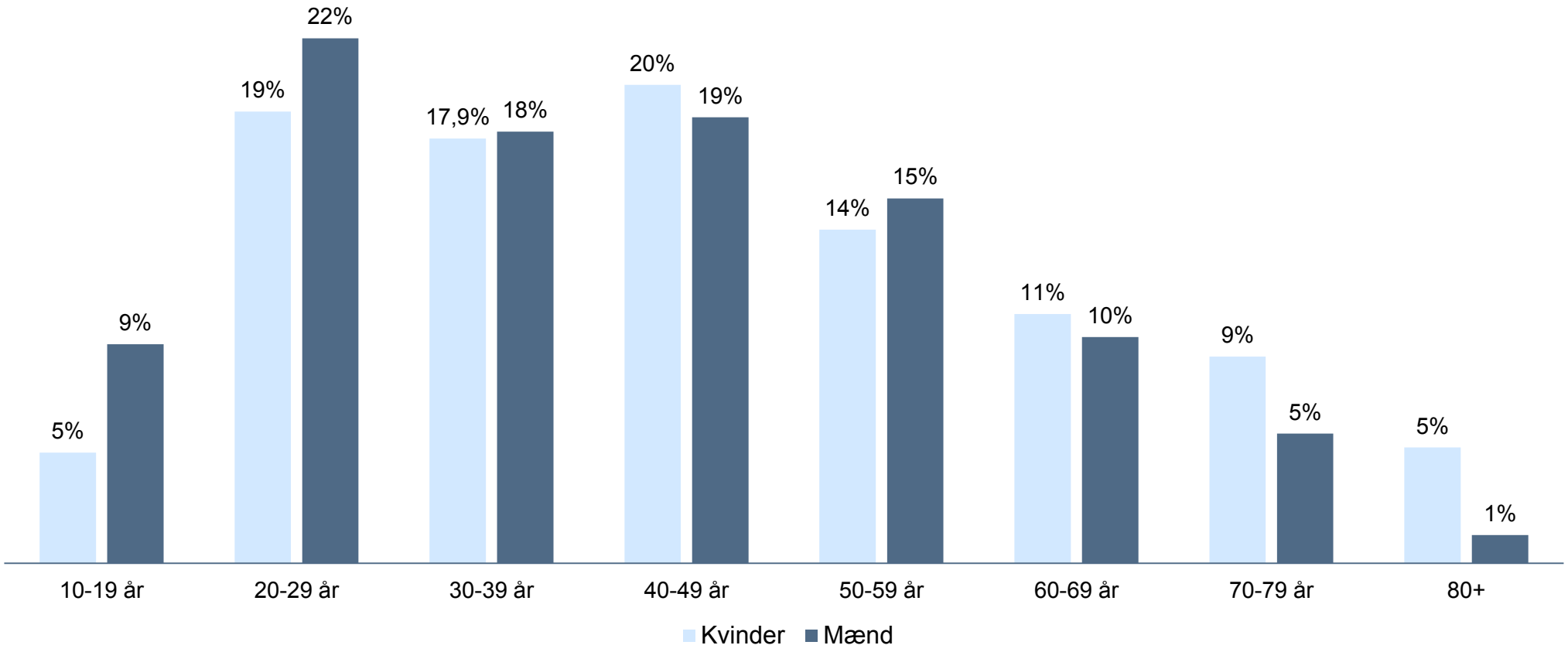
Nationalitet

9 ud af 10 forurettede i sager om it-relateret økonomisk kriminalitet er danskere.

Andre nationaliteter blandt anmelderne dækker bl.a. Polen, Syrien, Tyskland og Tyrkiet.

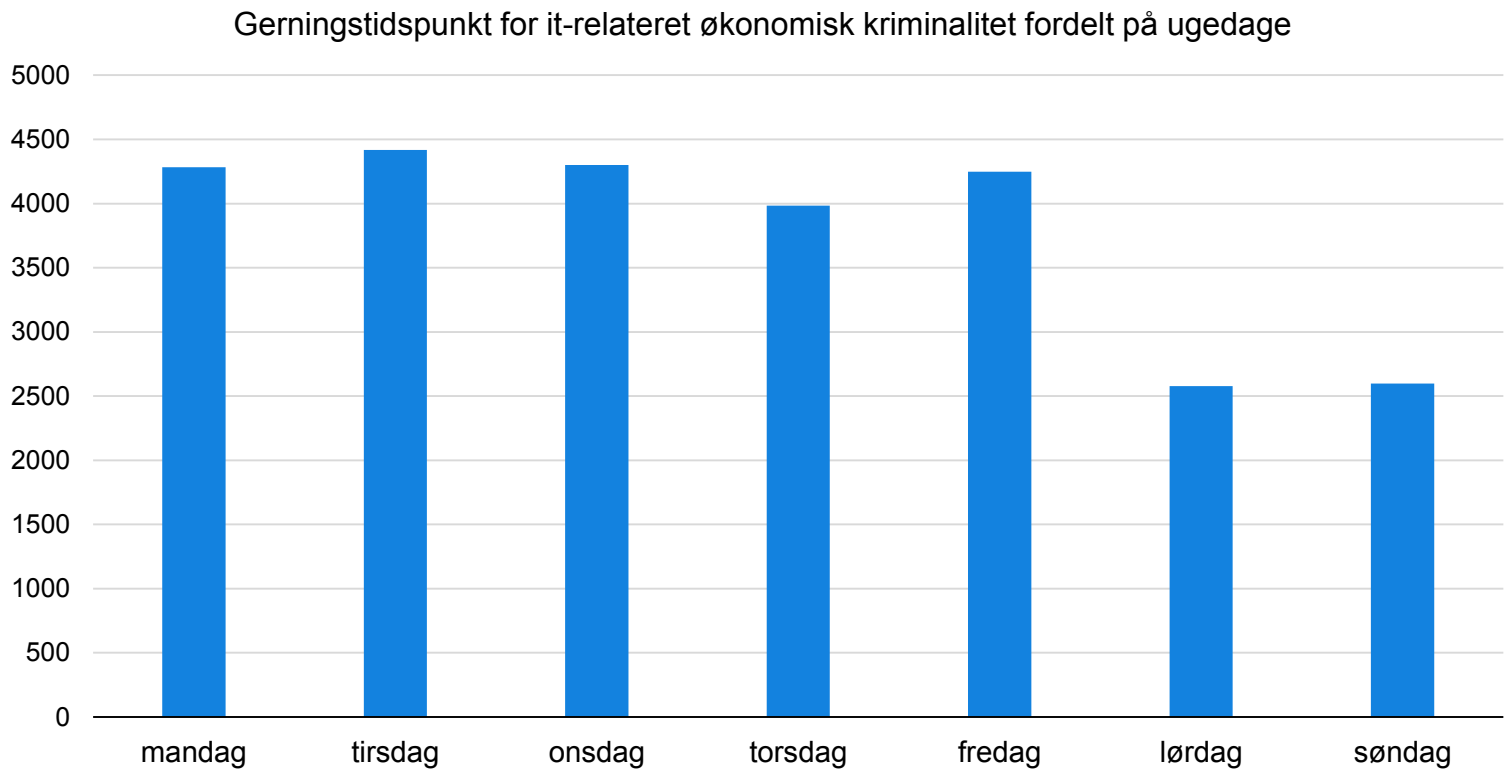
Base: (26.410) Private forurettede af it-relateret økonomisk kriminalitet anmeldt til LCIK i 2020.

Køn- og aldersfordelingen for forurettede i sager om it-relateret økonomisk kriminalitet



Base: (26.410) Private forurettede af it-relateret økonomisk kriminalitet anmeldt til LCIK i 2020.

Flest borgere udsættes for it-relateret økonomisk kriminalitet i hverdagene



Gerningstidspunkt for it-relateret økonomisk kriminalitet

I 2020 blev flest private forurettede udsat for it-relateret økonomisk kriminalitet i hverdagene.

I 2019 identificerede LCIK's 1-års analyse samme mønster blandt gerningstidspunkterne for it-relateret økonomisk kriminalitet.

Hvorvidt resultaterne skyldes, at de forurettede er nemmere at bedrage i hverdagene, er ikke til at sige på nuværende tidspunkt. Det vil være interessant at undersøge, om weekender også i fremtiden er karakteriseret af lavere niveauer af it-relateret økonomisk kriminalitet.

Base: (26.410) Private forurettede af it-relateret økonomisk kriminalitet tilknyttet anmeldelser anmeldt til LCIK i 2020.

Antal private forurettede per 1.000 indbyggere i hver politikreds

På landsplan udsættes 4 personer for it-relateret økonomisk kriminalitet pr. 1.000 indbygger

Nordjyllands Politi
3,8 forurettede pr. 1.000 indbyggere.

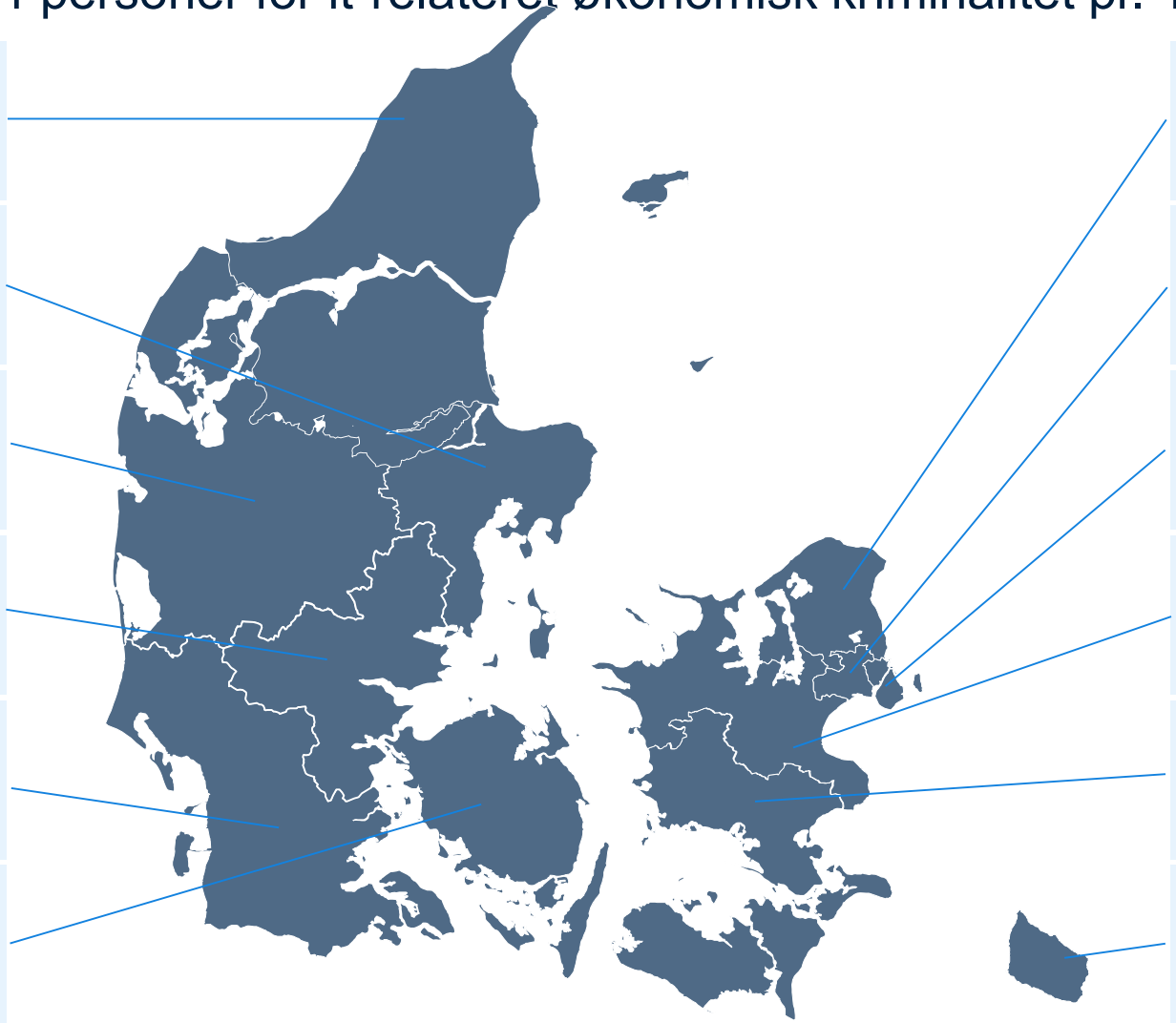
Østjyllands Politi
3,9 forurettede pr. 1.000 indbyggere.

Midt- og Vestjyllands Politi
3,8 forurettede pr. 1.000 indbyggere.

Sydøstjyllands Politi
3,8 forurettede pr. 1.000 indbyggere.

Syd- og Sønderjyllands Politi
3,7 forurettede pr. 1.000 indbyggere.

Fyns Politi
4,5 forurettede pr. 1.000 indbyggere.



Nordsjællands Politi
4,2 forurettede pr. 1.000 indbyggere.

Københavns Vestegns Politi
3,8 forurettede pr. 1.000 indbyggere.

Københavns Politi
4,8 forurettede pr. 1.000 indbyggere.

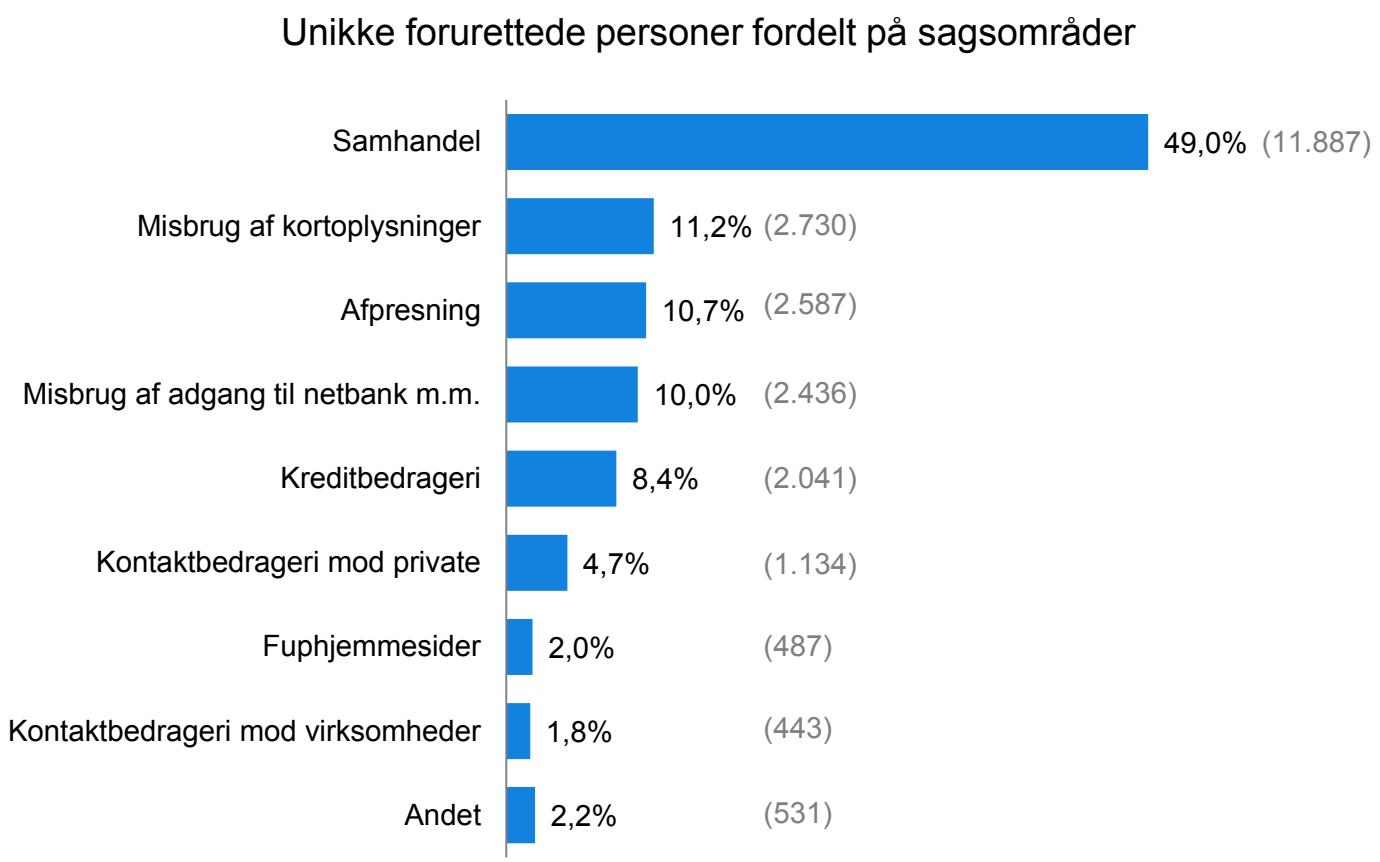
Midt- og Vestsjællands Politi
3,7 forurettede pr. 1.000 indbyggere.

Sydsjælland og Lolland-Falsters Politi
3,9 forurettede pr. 1.000 indbyggere.

Bornholms Politi
3,4 forurettede pr. 1.000 indbyggere.

Base: (23.764) Unikke private forurettede af it-relateret økonomisk kriminalitet tilknyttet anmeldelser anmeldt til LCIK i 2020.
Note: Der er benyttet befolkningstal fra Danmarks Statistik (FOLK1A) optalt i 4. kvartal 2020.

Næsten halvdelen af de private forurettede udsættes for samhandelsbedrageri



Antallet af unikke forurettede per sagsområde

Grafen til venstre er opgjort sådan, at én forurettet (person) kan tælle én gang for hvert sagsområde. På den måde opnås et bedre estimat for, hvad de forurettede for it-relateret økonomisk kriminalitet udsættes for, end ved en opgørelse på baggrund af rå anmeldelser.

Ved at opgøre LCIK's sagsområder på denne måde stryger digital afpresning op ad listen som en kriminalitetsform mange forurettede udsættes for. Sagsområdet kreditbedrageri rangerer derimod lavere, hvilket skyldes, at mange af de forurettede i forbindelse med denne type kriminalitet er professionelle virksomheder og ikke privatpersoner.

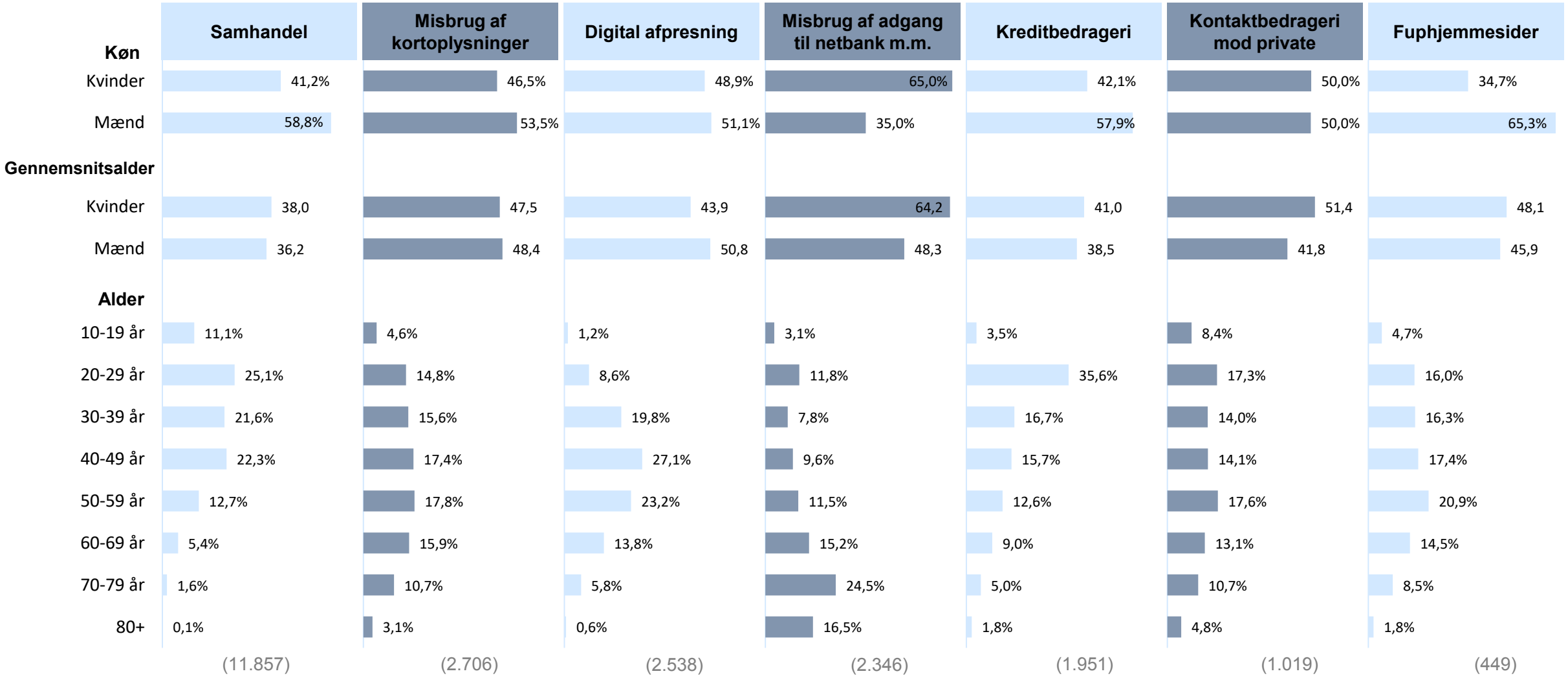
Det bliver endvidere tydeligt, at nogle privatpersoner anmelder på vegne af virksomheder og dermed kommer til at fremgå som anmelder og forurettede (A/F) blandt LCIK's anmeldelser. Derfor fremgår det at 443 personer udsættes for kontaktbedrageri mod virksomheder.

'Andet'

Kategorien 'Andet' dækker over de anmeldelser, som falder uden for LCIK's etablerede sagsområder, eller anmeldelser der afventer kategorisering af en sagsbehandler.

Base: (24.276) Antal unikke private forurettede inden for hvert sagsområde i 2020.

Profil over private forurettede for it-relateret økonomisk kriminalitet fordelt på sagsområder



Base: (23.764) Unikke private forurettede af it-relateret økonomisk kriminalitet tilknyttet anmeldelser anmeldt til LCIK i 2020.

Top 3 over sagsområder baseret på antal af private forurettede i hver politikreds

Nordjyllands Politi
1. Samhandel
2. Misbrug af adgang til netbank m.m.
3. Misbrug af kortoplysninger

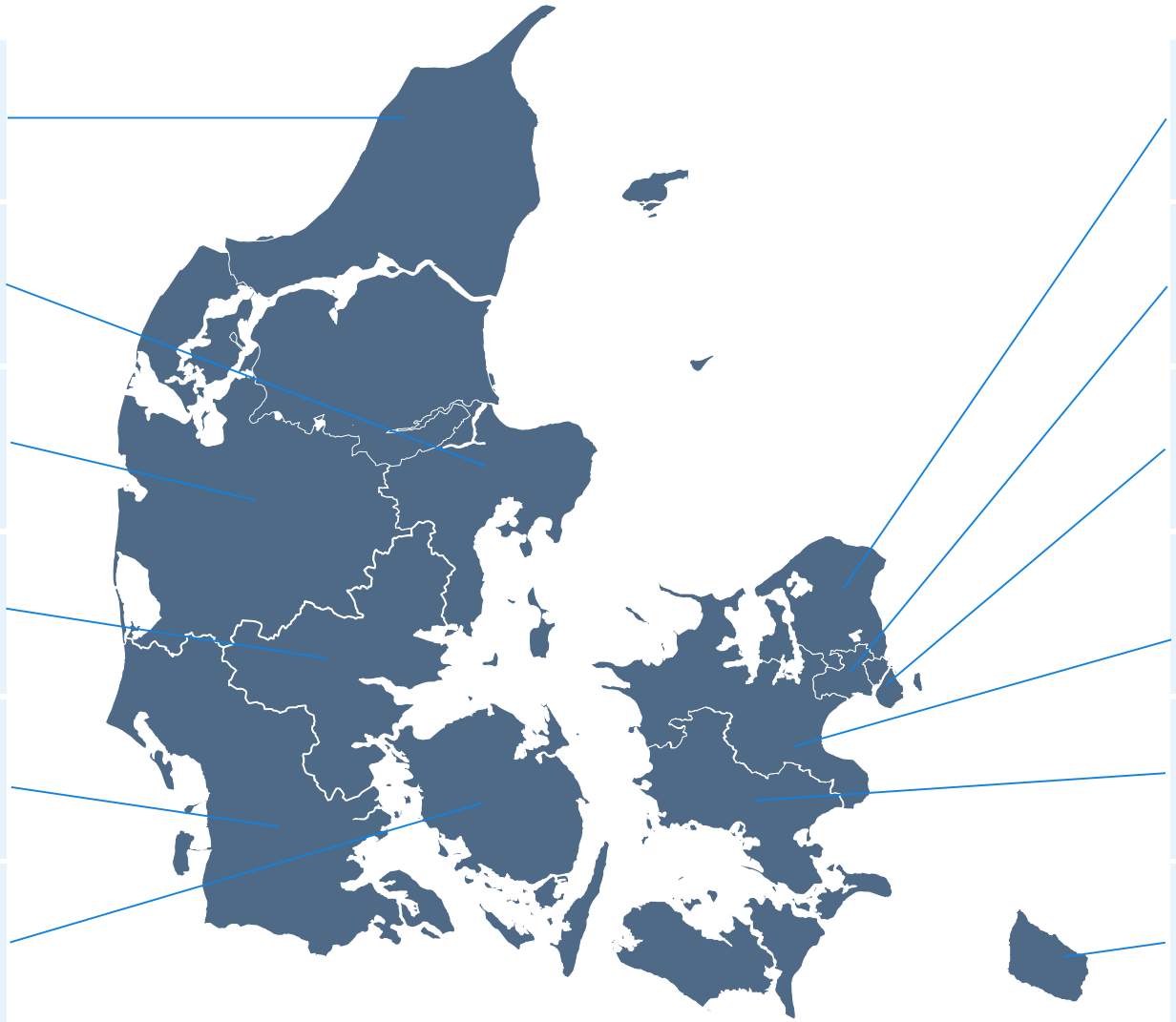
Østjyllands Politi
1. Samhandel
2. Misbrug af kortoplysninger
3. Digital afpresning

Midt- og Vestjyllands Politi
1. Samhandel
2. Misbrug af adgang til netbank m.m.
3. Misbrug af kortoplysninger

Sydøstjyllands Politi
1. Samhandel
2. Misbrug af adgang til netbank m.m.
3. Misbrug af kortoplysninger

Syd- og Sønderjyllands Politi
1. Samhandel
2. Misbrug af adgang til netbank m.m.
3. Misbrug af kortoplysninger

Fyns Politi
1. Samhandel
2. Kreditbedrageri
3. Misbrug af adgang til netbank m.m.



Nordsjællands Politi
1. Samhandel
2. Digital afpresning
3. Misbrug af kortoplysninger

Københavns Vestegns Politi
1. Samhandel
2. Digital afpresning
3. Misbrug af kortoplysninger

Københavns Politi
1. Samhandel
2. Digital afpresning
3. Misbrug af kortoplysninger

Midt- og Vestsjællands Politi
1. Samhandel
2. Misbrug af kortoplysninger
3. Digital afpresning

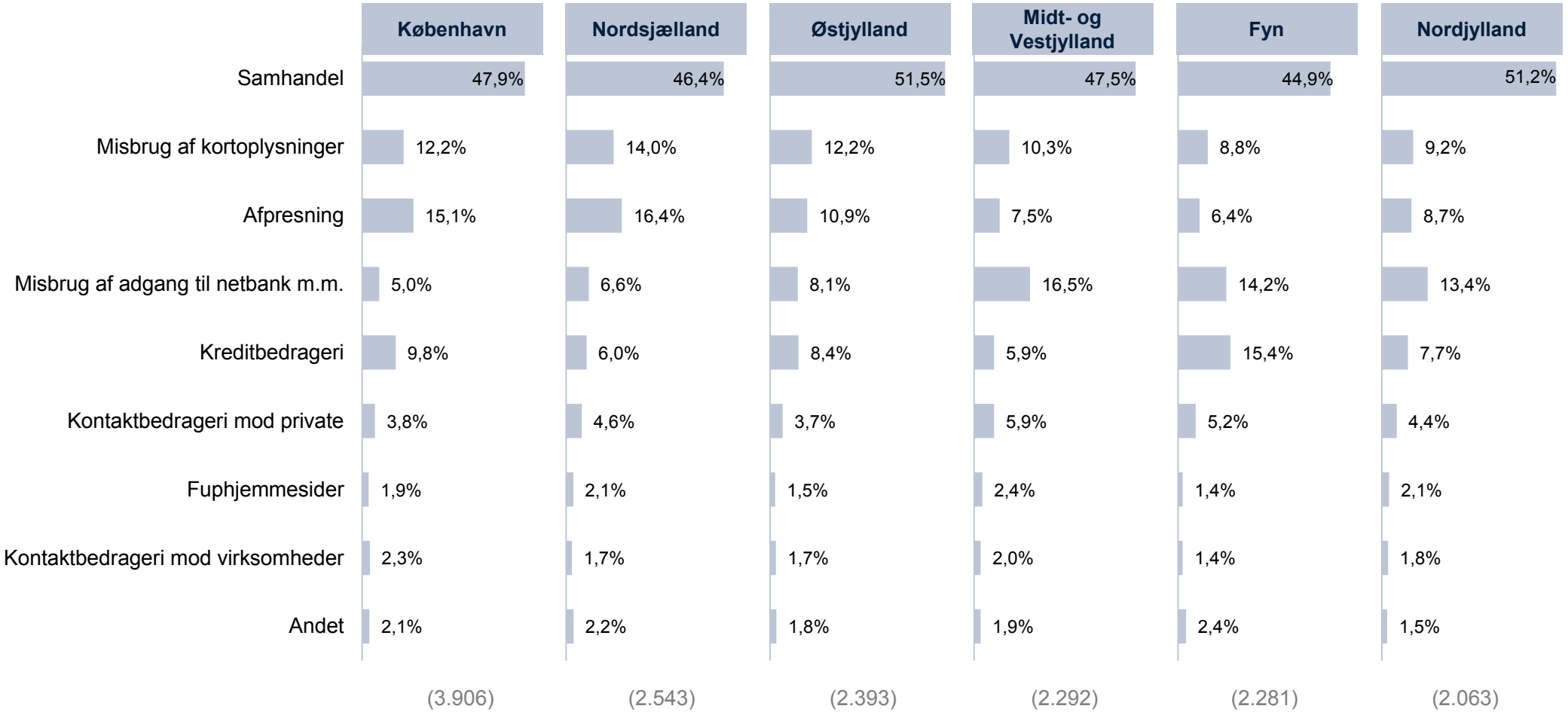
Sydsjælland og Lolland-Falsters Politi
1. Samhandel
2. Misbrug af adgang til netbank m.m.
3. Misbrug af kortoplysninger

Bornholms Politi
1. Samhandel
2. Misbrug af kortoplysninger
3. Misbrug af adgang til netbank m.m.

Base: (24.276) Antal unikke private forurettede inden for hvert sagsområde i 2020.

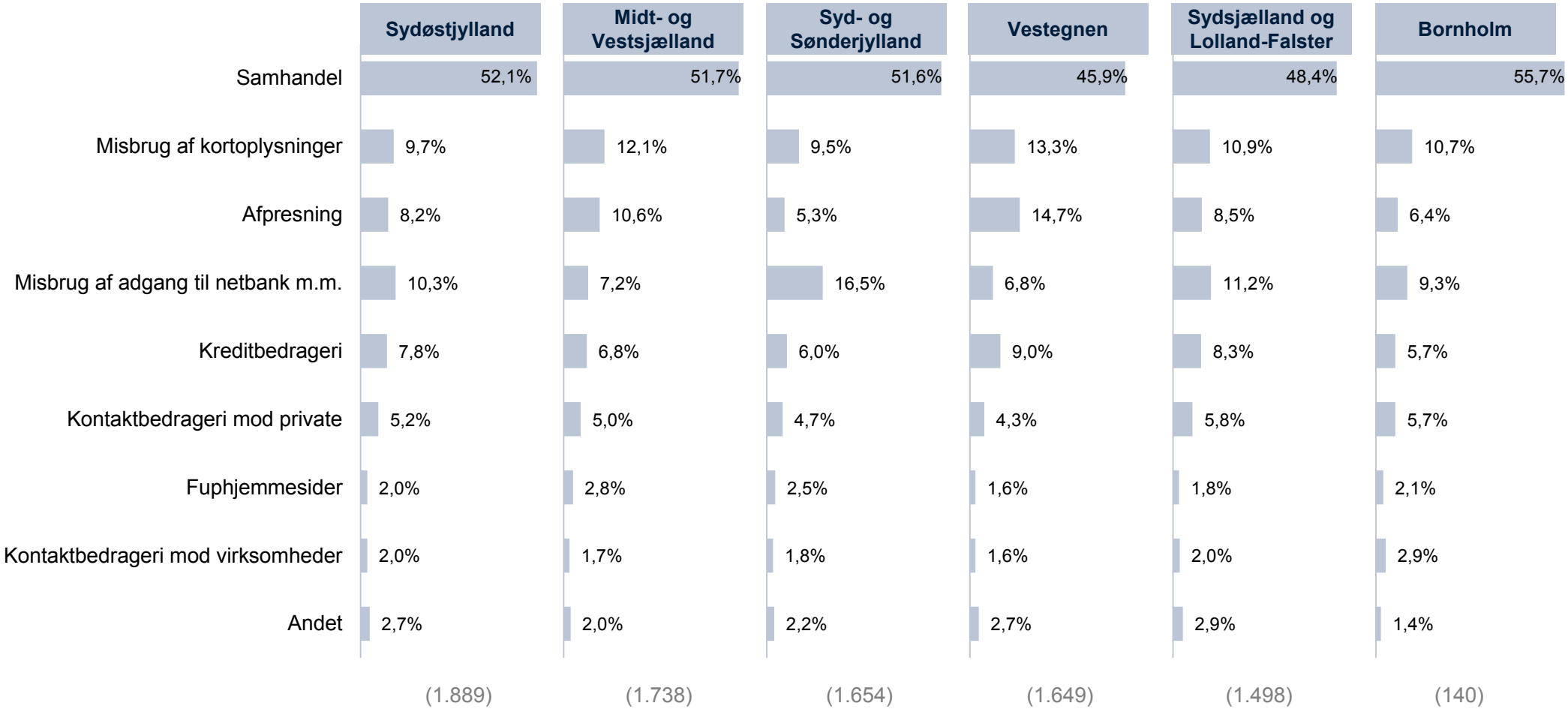
Hvad udsættes de private forurettede i politikredsene for?

Antallet af forskellige forurettede per sagsområde fordelt på politikredse (1/2)

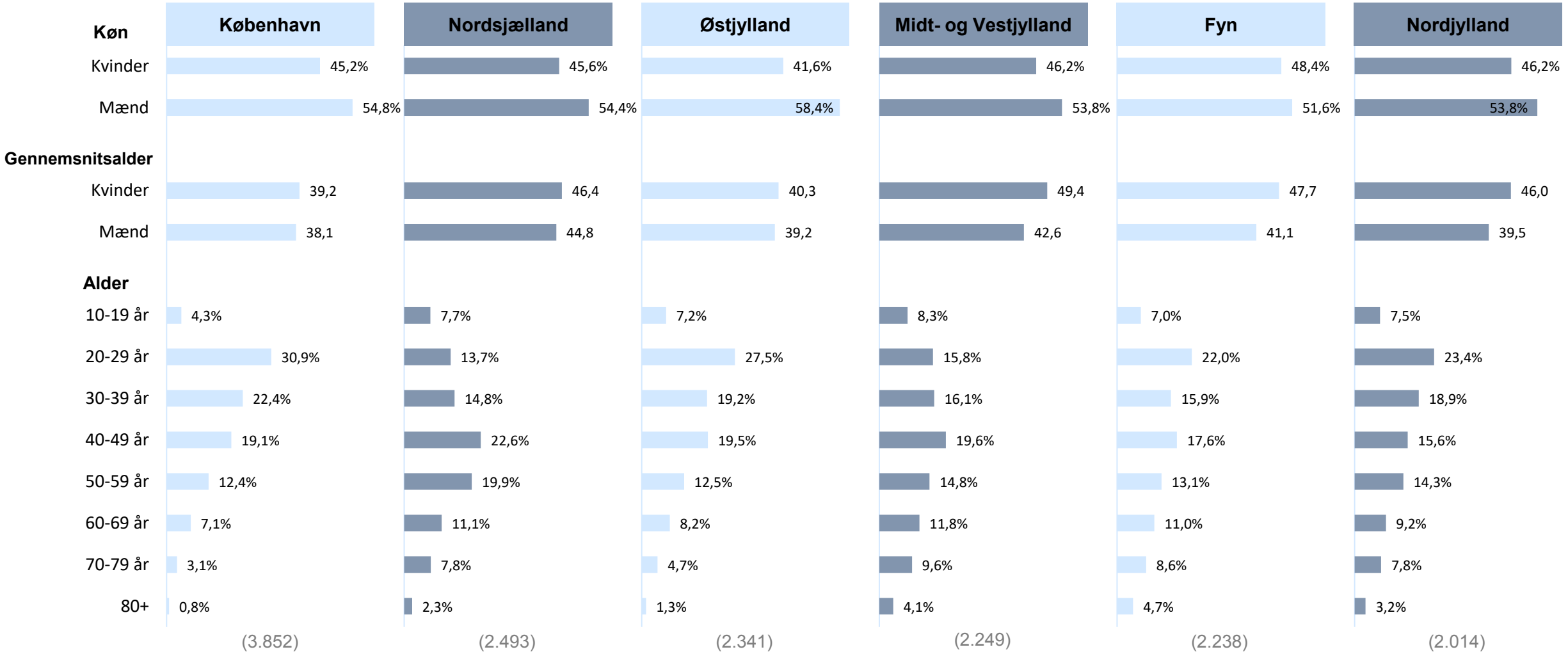


Hvad udsættes de private forurettede i politikredsene for?

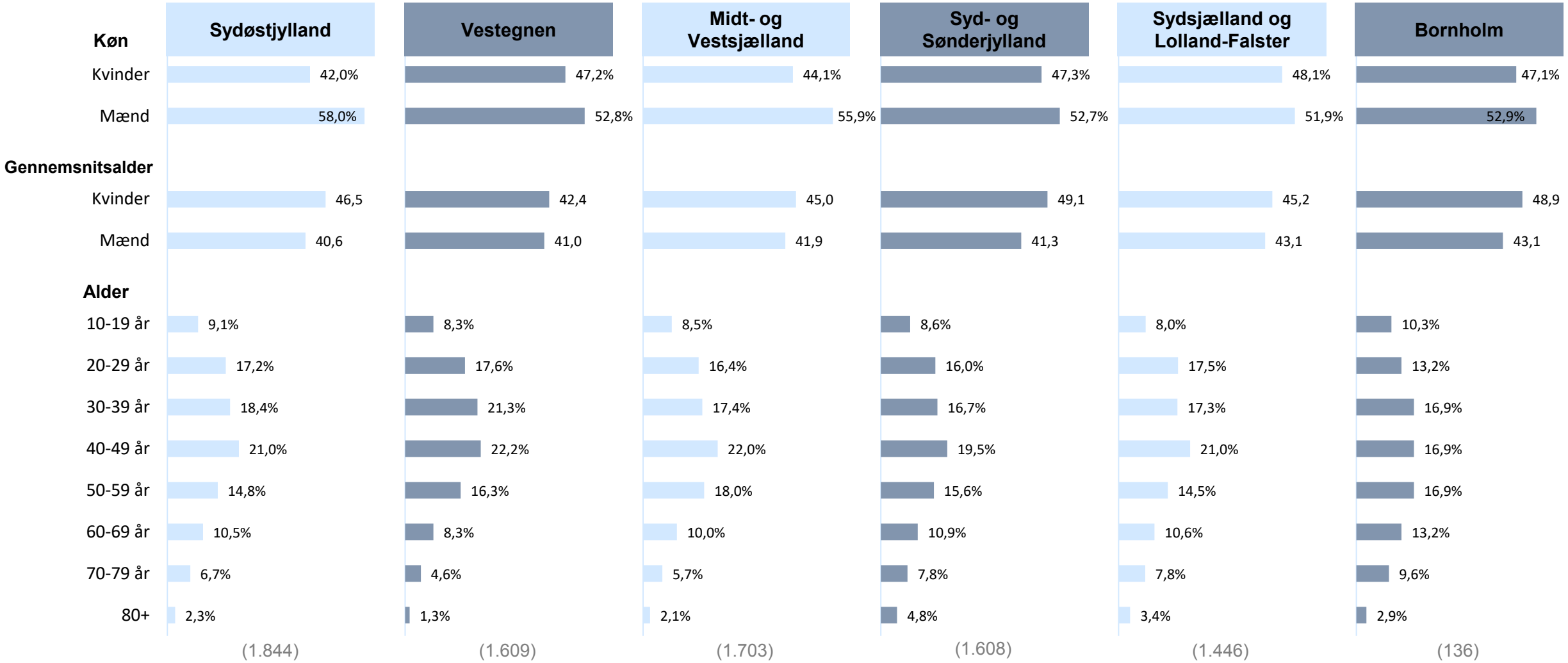
Antallet af forskellige forurettede per sagsområde fordelt på politikredse (2/2)



Profil over private forurettede for it-relateret økonomisk kriminalitet fordelt på politikredse (1/2)



Profil over private forurettede for it-relateret økonomisk kriminalitet fordelt på politikredse (2/2)



Opsummering på private forurettede 1/2

Hvem udsættes it-relateret økonomisk kriminalitet?

LCIK kan konstatere, at 24.973 personer blev udsat for it-relateret økonomisk kriminalitet anmeldt til LCIK i 2020. Langt størstedelen af de forurettede er privatpersoner, mens en mindre del er professionelle aktører i form af virksomheder, myndigheder, foreninger m.m.

På landsplan har fire privatpersoner pr. 1.000 indbygger været udsat for it-relateret økonomisk kriminalitet i 2020. Gennemsnitsalderen for disse personer er 42,7 år. I 2019 var gennemsnitsalderen også omkring 42 år. Mændene er generelt yngre end kvinderne, der har været udsat for it-relateret økonomisk kriminalitet, og flere mænd end kvinder har været udsat for it-relateret økonomisk kriminalitet i 2020 (hhv. 54,4 og 45,6 pct.). Mændene er i gennemsnit knap 5 år yngre end de kvindelige forurettede.

Privatpersoner i alle aldre udsættes for it-relateret økonomisk kriminalitet. Den aldersgruppe der har været udsat for mest it-relateret økonomisk kriminalitet er de 20-29 årige. Blandt mændene er det også den aldersgruppe med flest forurettede personer. Den mest udsatte aldersgruppe blandt kvinderne er de 40-49 årige tæt efterfulgt af de 20-29 årige.

Over 90 % af de forurettede privatpersoner er danskere. Andre nationaliteter blandt anmelderne er bl.a. Polen, Syrien og Tyskland.

Langt de fleste forurettede har også anmeldt kriminaliteten og fremstår derfor både som anmelder og forurettet (A/F).

Der er flest forurettede per indbyggere i hhv. Københavns politikreds, Fyns politikreds og Nordsjællands politikreds. Alle tre politikredse har flere forurettede per indbygger end antallet af forurettede per indbygger på landsplan.

De forurettede udsættes oftest for samhandelsbedrageri

Samhandelsbedrageri er den kriminalitetstype, som flest private anmeldere anmelder. Næsten halvdelen af de private anmeldere anmelder bedrageri i form at samhandel. I 78 % af samhandelsanmeldelserne er der tale om samhandelsbedrageri med fysiske varer.

Det næststørste kriminalitetstype som privatpersoner udsættes for, er misbrug af kortoplysninger. 11,2 % af de forurettede har fået misbrugt deres kortoplysninger.

På tredjepladsen findes digital afpresning. 10, 7 % af de forurettede for it-relateret økonomisk kriminalitet blev i 2020 udsat for digital afpresning. I langt de fleste tilfælde er der tale om afpresning i form af masseafpresning.

På tværs af politikredsene udsættes flest forurettede for samhandelsbedrageri. Ud over samhandelsbedrageri er der en smule variation i, hvilken type af it-relateret økonomisk kriminalitet de forurettede personer udsættes for på tværs af politikredsene. Generelt er det bedrageri i form af misbrug af kortoplysninger, digital afpresning, misbrug af adgang til netbank m.m. og kreditbedrageri som flest privatpersoner udsættes for på tværs af landets politikredse.

Opsummering på private forurettede 2/2

Forskellig offerprofil på tværs af kriminalitetstyper

De forskellige kriminalitetstyper rammer forskellige profiler baseret på alder og køn. For eksempel bliver de yngste forurettede typisk udsat for samhandelsbedrageri. Dette fund falder fint i tråd med DBA's Genbrugsindex 2020, der finder, at flere unge handler brugt. Blandt et repræsentativt udsnit i befolkningen har 88 % af de 18-30 årige i undersøgelsen angivet, at de har handlet brugt inden for de sidste 12 måneder.

Ud over at personer der udsættes for samhandelsbedrageri kan karakteriseres som yngre end øvrige ofre for it-relateret økonomisk kriminalitet, er flere af de udsatte personer mænd. Mændene er i gennemsnit knap et par år yngre end de kvinder, som udsættes for samhandelsbedrageri. Gennemsnitsalderen for personer udsat for samhandelsbedrageri er 37 år. Der blev identificeret en lignende offerprofil for samhandelsbedrageri i 2019.

Anderledes forholder det sig blandt ofre for digital afpresning. Her udsættes næsten lige mange mænd og kvinder for masseafpresning af forskellige karakter. Ofrene for denne type it-relateret økonomisk kriminalitet er i gennemsnit 47,4 år. Mændene er i gennemsnit ældre end kvinderne og der findes flest forurettede personer i aldersgruppen 40-49 år.

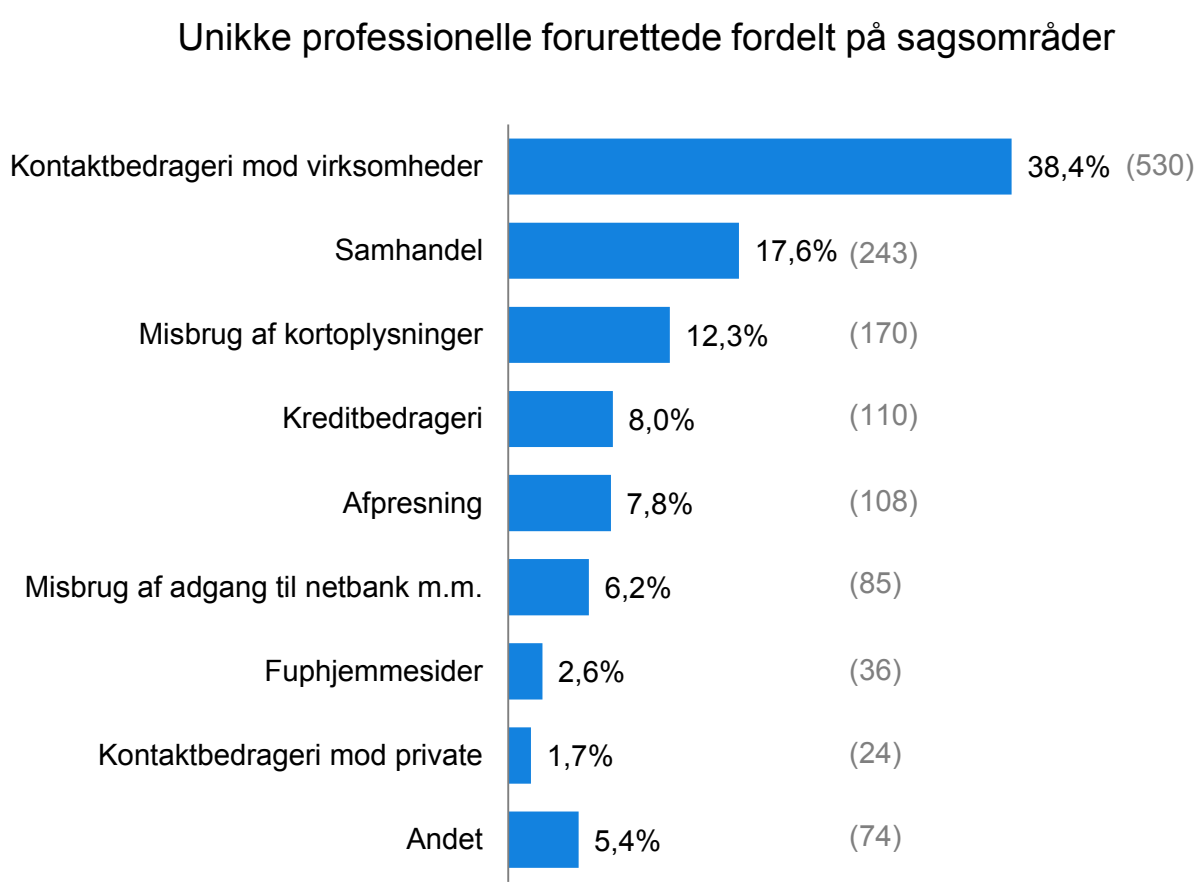
De typer it-relateret økonomisk kriminalitet hvor flere eller lige mange kvinder som mænd har været udsat er hhv. misbrug af adgang til netbank m.m. og kontaktbedrageri. De kvinder der er udsat for disse typer bedragerier er karakteriseret ved at være ældre og har den højeste gennemsnitsalder blandt kvinder på tværs af de forskellige typer af it-relateret økonomisk kriminalitet. Til sammenligning er mændene udsat for disse kriminalitetstyper hhv. 15,9 år (misbrug af adgang til netbank) og 9,6 år (kontaktbedragerier) yngre.

Ud fra anmeldelserne kan vi på baggrund af gerningstidspunkter generelt se, at de forurettede privatpersoner hovedsageligt bliver bedraget i hverdagene. Antallet af anmeldte bedragerier er væsentligt lavere i weekenden.

Professionelle forurettede i sager om it-relateret økonomisk kriminalitet

POLITI

Over en tredjedel af de professionelle forurettede i 2020 blev udsat for kontaktbedrageri



Fordeling af professionelle forurettede på LCIK's sagsområder

I grafen er LCIK's sagsområder opgjort på baggrund af antallet af unikke professionelle forurettede. Denne gruppe består af de virksomheder, myndigheder, foreninger m.m., der blev udsat for it-relateret økonomisk kriminalitet anmeldt i 2020. Opgørelsen giver indblik i, hvor mange forskellige professionelle forurettede der rammes af de forskellige typer af it-relateret økonomisk kriminalitet.

En professionel forurettet kan tælle én gang under hvert sagsområde.

Mest anmeldte sagområde blandt de professionelle anmeldere

Over en tredjedel af de professionelle anmeldere blev udsat for kontaktbedrageri. Disse kontaktbedragerier er oftest i form af BEC eller CEO fraud.

Base: (1.380) Antal unikke professionelle forurettede organisationer inden for hvert sagsområde i 2020.

Opsummering på professionelle forurettede

Om de professionelle forurettede

Der var i 2020 1.229 unikke professionelle forurettede, der blev udsat for it-relateret økonomisk kriminalitet.

84,5 % af de professionelle forurettede var udsat for it-relateret økonomisk kriminalitet én gang imens 15,5 % var udsat to eller flere gange.

Anmeldelsestallene peger på, at en lille gruppe professionelle forurettede har været udsat for it-relateret økonomisk kriminalitet mange gange i løbet af 2020. Dette mønster skyldes med al sandsynlighed, at denne gruppe er særligt gode til, at anmelde den it-relaterede økonomiske kriminalitet til politiet.

De 25 professionelle forurettede, som var udsat for mest it-relateret økonomisk kriminalitet, var samlet set udsat for 58,3 % af tilfældene af it-relateret økonomisk kriminalitet mod professionelle i 2020. Top 25-listen består hovedsageligt af virksomheder fra den finansielle sektor. Der er tale om flere af de store bankinstitutioner i Danmark samt andre låne- og kreditgivere. Derudover findes et par teleselskaber på listen over de 25 mest udsatte professionelle forurettede i 2020, og der fremgår også en række virksomheder, som har en stor del af deres handelsaktivitet online fx Elgiganten og Nemlig.com.

De professionelle forurettede udsættes mest for BEC/CEO fraud

38,4 % af de professionelle forurettede i 2020 blev udsat for kontaktbedrageri. Over to tredjedele af kontaktbedragerierne var i form af BEC/CEO fraud imens knap en fjerdedel var i form af fakturasvindel. Det er en bred gruppe af professionelle forurettede, der udsættes for BEC/CEO fraud, og gruppen dækker over alt fra store internationale virksomheder med base i Danmark til den lokale sejlklub og grundejerforening.

De professionelle forurettede udsættes også for samhandelsbedrageri

De professionelle forurettede udsættes også for samhandelsbedrageri. I 2020 blev 17,6 %. af de professionelle forurettede udsat for samhandelsbedrageri. Samhandelsbedrageri mod professionelle forurettede adskiller sig overordnet fra samhandelsbedrageri mod private forurettede på følgende vis: Hvor private forurettede oftest oplever samhandelsbedrageri i form af at have købt og betalt for en vare, der aldrig dukker op, oplever professionelle forurettede hovedsageligt, at deres CVR/EAN-nummer benyttes af gerningspersoner til at købe varer over nettet.

Når professionelle forurettede udsættes for misbrug af kortoplysninger

Professionelle forurettede kan, som private forurettede, opleve at få misbrugt kortoplysninger tilknyttet de kreditkort, som organisationen råder over.

Over halvdelen af tilfældene af misbrug af kortoplysninger (51,8 %) handlede dog om misbrug gennem webshops. Typisk er der tale om sager, hvor en virksomhed havde solgt og sendt en vare til en gerningsperson, der havde misbrugt en anden persons kortoplysninger. Nets kan efterfølgende foretage en chargeback af beløbet på vegne af den privatperson, der har fået misbrugt sine kortoplysninger hos den pågældende virksomhed. Dermed får privatpersonen sine penge tilbage, men webshoppen risikerer ikke at få dækning for den vare, som de har sendt afsted til gerningspersonen.

I 22,4 % af tilfældene af misbrug af kortoplysninger har de professionelle forurettede været udsat for phising eller smishing af deres kortoplysninger.

Metode

POLITI

Metode

Rapporten bygger på to datasæt. Ét datasæt, der er forbundet til anmeldelserne af it-relateret økonomisk kriminalitet, og ét der er forbundet til de personer, som er involveret i sager om it-relateret økonomisk kriminalitet - enten som anmelder eller forurettet i sagen. Begge datasæt er behandlet i Excel, som er det primære analytiske redskab i rapporten.

Datasæt 1

Rapportens første datasæt består af anmeldelsestal fra politiets sagsstyringssystem (POLSAS).

- Tallene er trukket gennem Qlikview rapporten Kriminalitet og dækker kalenderåret 2020.
- Der er kun trukket sager med '01LC'-journalnumre. (LCIK Journalnumre).
- Data er dynamiske og er trukket den 5. januar 2021.

Datasæt 2

Den del af rapporten, der handler om anmeldere, forurettede og andre personer beror på et datasæt fra Polmaplite.

Data er fundet ved at søge på sager i "politikredsen" '01LC', samt på en liste af gerningskoder, der relaterer sig til LCIK's sagsområde. (Se liste over gerningskoder i bilag).

- Data er dynamiske og er trukket den 5. januar 2021.

Prioriteringsnøgle

LCIK har udviklet en prioriteringsnøgle, der udvælger én søgenøgle blandt flere, når en sag har tilknyttet flere søgenøgler på samme trin.

Prioriteringsnøglen sikrer, at hver anmeldelse kun fremgår én gang i rapporten, selvom de opgøres på tværs af forskellige kriminalitetsområder. (Læs mere om prioriteringsnøglen i bilag).

Forbehold og definition

1. Kategorisering af forurettede

LCIK's Årsrapport tager udgangspunkt i anmeldelsestallene fra 2020. Borgere og virksomheder kan være tilknyttet anmeldelser som forurettet (FOU), anmelder (ANM), anmelder og forurettet (A/F) og sigtet (SIG).

Borgere og virksomheder oprettes automatisk som både anmelder og forurettet (A/F)

Når en borger eller virksomhed anmelder til LCIK gennem anmeldelsesportalen, oprettes de automatisk som både anmelder og forurettet (A/F). Det skyldes, at anmelderen skal være registreret som forurettet for, at LCIK kan sende en kvittering for at modtage anmeldelsen.

Personkategorier: Langt de fleste anmeldere udgør også den forurettede part i sagen

Kategorien A/F har gjort det vanskelligt for LCIK at udtale sig om forurettede, da der ikke er garanti for, at anmelder og forurettet er samme person. Efter to år med anmeldelsesportalen er det dog LCIK's erfaring, at langt de fleste anmeldere også udgør den forurettede part i sagen. I denne årsrapport er data om forurettede derfor baseret på følgende personkategorier:

Gruppen af forurettede består af personkategorierne: **A/F** og **FOU**. Den førstnævnte gruppe (A/F) dækker over de personer og organisationer, som er forurettede og selv har anmeldt til politiet. Den anden gruppe (FOU) dækker udelukkende over personer og organisationer, som er forurettede i forbindelse med den pågældende anmeldelse.

LCIK's måde at forholde sig til personkategorierne er af metodisk og principiel karakter. Derudover er det også for at sikre sammenlignelighed med fremtidige rapporter og analyser med samme fremgangsmåde.

Modsat 1-årsanalysen 2019 har LCIK i 2020 valgt udelukkende at beskæftige sig med de forurettede og ikke anmelderne. Valget er truffet pga. af det store sammenfald mellem de to grupper, da ca. 90 pct . er både anmelder og forurettet. Det store sammenfald medfører, at de to grupper er meget ens på tværs af forskellige statistiske fordelinger.

Forbehold og definition

2. Tildeling af journalnumre til underforhold

Nogle af LCIK's professionelle anmeldere gør brug af LCIK's API-løsning, når de anmelder it-relateret økonomisk kriminalitet. Ved anmeldelser gennem API-løsningen oprettes der automatisk underforhold i sagen. Der vil fx være et nyt underforhold for hver uautoriseret pengetransaktion i en sag om misbrug af kortoplysninger.

Det er almindeligt at oprette underforhold til eksisterende sager, når efterforskningen skrider frem, og politiet opdager flere ulovlige forhold. Det nye består i, at underforhold, som oprettes automatisk gennem LCIK's API-løsning, får et LCIK journalnummer. Sager, som anmeldes gennem anmeldelsesportalen, vil i mange tilfælde først få tilknyttet alle underforhold i løbet af den videre efterforskning i politikredsene. Disse underforhold oprettes derfor med politikredsens journalnummer.

I denne rapport er der taget udgangspunkt i sager om it-relateret økonomisk kriminalitet, som har et LCIK-journalnummer. Underforhold oprettet i politikredsene indgår derfor ikke i analysen.

2.1 Ny opgørelsesmetode: underforhold genereret gennem LCIK's API-løsning er fratrukket i årsrapporten 2020

Både Danske Bank og MobilePay bruger LCIK's API-løsning til at anmelde. Det påvirker fordelingen af anmeldelser mellem LCIK's forskellige sagsområder, da stort set alle underforhold i disse sager vil have et LCIK-journalnummer, mens det ikke er tilfældet ved anmeldelser fra anmeldelsesportalen. Det påvirker især anmeldelsestallene inden for sagsområderne "Misbrug af adgang til netbank m.m." og "Misbrug af kortoplysninger".

For at opnå et mere retvisende billede af kriminalitetsniveauet* i LCIK's årsrapport 2020 har LCIK valgt at fratrække de underforhold, som er genereret ved anmeldelser gennem LCIK's API-løsning.

Underforholdende er defineret ud fra at de er: 1) anmeldt gennem LCIK's API-løsning, 2) adjournaliseret til et journalnummer, der ikke er identisk med eget journalnummer. Definitionen er tilpasset registreringspraksis i LCIK. Information om, hvorvidt en sag er anmeldt gennem LCIK's API-løsningen fremgår af Qlikviewrapporten "LCIK_ledelsesinformation".

Note: Kriminalitetsniveauet for it-relateret økonomisk kriminalitet målt ud fra antallet af anmeldelser til LCIK.

Forbehold og definition

3. Sager der ikke skulle være anmeldt til LCIK

Anmeldelser til LCIK bliver visiteret i centerets Sektion for anmeldelse og visitation. Her identificeres løbende sager, som falder uden for sagskategorien 'it-relateret økonomisk kriminalitet', og som LCIK derfor ikke behandler. Sagerne videresendes til rette politikreds og udkorrigeres i POLSAS.

I denne rapport er der brugt dynamiske tal. Da rapporten dermed er baseret på et øjebliksbillede af anmeldelserne, vil der være sager, som falder uden for LCIK's sagsområde, men som endnu ikke er udkorrigeret.

For at frasortere disse sager identificeres sagerne blandt dem, som LCIK's sektion for Anmeldelses og Visitation sagsplacerer på funktionsbrugeren "IKKE LCIK". De pågældende journalnumre fra sagerne kan herefter udfindes i Qlikviewrapporten "LCIK_ledelsesinformation.qvw", hvorefter de frasorteres i opgørelserne over den it-relaterede økonomiske kriminalitet.

Sidste år var der praksis for, at LCIK's Sektionen for anmeldelse og visitation indtastede ordene 'IKKELCIK' i resumé-feltet ved anmeldelser uden for de sagsområder, som LCIK er ansvarlig for. Disse sager blev derefter frasorteret i datagrundlaget i 1-års analysen 2019. Der er derfor tale om en ændring i registreringspraksis af IKKE-LCIK-sager mellem år 2019 og 2020, som gerne skulle give et mere retvisende billede af, hvor mange af LCIK's sager, der falder uden for LCIK's sagsområder, og dermed giver et mere præcist billede af, hvor mange af LCIK's anmeldelser, der reelt set omhandler it-relateret økonomisk kriminalitet.

4. Beskrivelser af LCIK's sagsområder

Årsrapporten indeholder beskrivelser af LCIK's respektive sagsområder (samhandelsbedrageri, kreditbedrageri, misbrug af kortoplysninger etc.).

Beskrivelserne er udarbejdet med udgangspunkt i efterforskernes erfaringer fra de respektive sagsområder i 2020. Formålet med beskrivelserne er todelt. For det første skal de give læseren den nødvendig introduktion til sagsområderne. For det andet gør beskrivelserne det muligt at følge udviklingen af sagområderne på et mere kvalitativt grundlag med udgangspunkt i, hvordan det ser ud i 2020.

Forbehold og definition

5. Professionelle anmeldere

Teknisk definition

Data om professionelle anmeldere i Årsrapporten er trukket fra programmet Polmaplite. De professionelle anmeldere er defineret ud fra de anmeldelser, hvor anmelderne ikke har fået tildelt en alder. Personer, der anmelder it-relateret økonomisk kriminalitet igennem LCIK's anmeldelsesportal på politi.dk, får automatisk tildelt en alder, da de logger ind og gennemfører anmeldelsen med deres NemID.

Antallet af professionelle anmeldere

Antallet af professionelle anmeldere er højst sandsynligt højere end de tal, der præsenteres i Årsrapporten. Dette skyldes, at nogle personer anmelder på vegne af virksomheder. Det kan både være mindre erhvervsdrivende, men også andre organisationer, hvor anmelderen ikke har adgang til et NemID for virksomheden. I rapporten bliver dette tydeligt, når det fremgår, at private anmeldere bl.a. har anmeldt kontaktbedragerier mod virksomheder.

LCIK
LANDSDÆKKENDE CENTER FOR IT-RELATERET ØKONOMISK KRIMINALITET

POLITI

LCIK's Årsrapport 2020

Udarbejdet af:

Karim Brandt, Forebyggelse- og analysekonsulent

Trine Gundorph, Forebyggelseskonsulent