NCIK
NATIONALT CENTER FOR IT-KRIMINALITET

POLITI

NCIK årsrapport 2021

En rapport om it-relateret økonomisk kriminalitet anmeldt i 2021

Indholdsfortegnelse

Indledning	**3**
Om it-relateret økonomisk kriminalitet	**4**
Resumé	**7**
Anmeldelser om it-relateret økonomisk kriminalitet i 2021	**11**
Samhandelsbedrageri	22
Misbrug af kortoplysninger	25
Kreditbedrageri	28
Misbrug af adgang til netbank m.m.	31
Digital afpresning	34
Kontaktbedrageri mod private	37
Kontaktbedrageri mod virksomheder	40
Fuphjemmesider	43
Forurettede i sager om it-relateret økonomisk kriminalitet	**46**
Metode	**50**
Litteraturliste	**57**

Indledning

I denne rapport præsenterer vi anmeldelsesbilledet, som det så ud for it-relateret økonomisk kriminalitet i 2021. Politiets Nationale Center for It-Kriminalitet (NCIK) har nu været i drift i lidt over tre år, og i den periode har vi generelt modtaget et stigende antal anmeldelser, selvom det samlede anmeldelsestal faldt fra 2020 til 2021.

Coronaepidemien og de deraf følgende nedlukninger og restriktioner har påvirket vores dagligdag og vaner de seneste par år. Dermed påvirker det også den måde, vi udsættes for it-relateret økonomisk kriminalitet, og det afspejler sig til dels i anmeldelsestallene. Vi har blandt andet set en stigning i handlen på internettet – også mellem private borgere – og der har været nedlukninger af nattelivet, som har resulteret i, at færre blev udsat for den type misbrug af betalingskort og betalingstjenester, som typisk foregår dér.

Årsrapporten indeholder vores officielle tal om it-relateret økonomisk kriminalitet og viser, hvordan billedet ser ud, når vi opgør anmeldelserne på de forskellige sagsområder. Indledningsvis beskriver vi kriminalitetsområdet og nogle af de aspekter, som er med til at gøre it-kriminalitet til noget særligt. Dernæst opgøres anmeldelsestallene, hvorefter vi i den følgende del af rapporten går i dybden med de enkelte kriminalitetsområder. Her opridser vi, hvad NCIK har fokus på i 2022. Rapporten henvender sig til alle, der har interesse i it-relateret økonomisk kriminalitet og bekæmpelse deraf.

God læselyst.

Jesper Kracht, Centerchef i NCIK

Om it-relateret økonomisk kriminalitet

POLITI

Beskrivelse af kriminalitetsområdet 1/2

Kriminalitetsområdet
It-relateret økonomisk kriminalitet er økonomisk kriminalitet med gerningssted på internettet, hvor it-systemer bruges til at opnå berigelse. Det er bedrageri i form af eksempelvis misbrug af betalingskort, kreditmisbrug og samhandelsbedrageri, hvor køber overfører penge for en vare, som aldrig bliver sendt af sælger. Kriminalitetsområdet omfatter også de sager, hvor der bruges afpresning til at opnå berigelse. Det kan være i form af ransomware eller masseafpresning, hvor et stort antal borgere modtager en mail om, at de har kompromitterende materiale på deres computer, og at der hurtigt skal betales et beløb til afsender, hvis materialet ikke skal videresendes til alle deres kontakter.

Hastighed og omfang
Det særlige ved it-kriminalitet er, at gerningspersonen på meget kort tid kan påvirke mange mennesker over store geografiske områder og gøre skade på ofrene. Geografi spiller ikke samme rolle som ved fysisk kriminalitet, og én gerningsperson kan begå kriminalitet mod personer i hele landet – og på tværs af lande – inden for kort tid. Der opstår derved en asymmetrisk relation i forhold til eksponering, hvor en gerningspersons rækkevidde øges markant, og hvor ofrenes udsathed stiger tilsvarende. Samtidig har de kriminelle gode muligheder for at udveksle metoder og afkast fra kriminaliteten hurtigt på tværs af geografiske afstande. Hastighed og volumen er således nøgleord, når man beskæftiger sig med it-relateret økonomisk kriminalitet.

Teknologi og den menneskelige faktor
I takt med, at de teknologiske sikkerhedsforanstaltninger bliver bedre og bedre på flere områder, stiger kriminelles brug af såkaldte social engineering-teknikker. Begrebet social engineering dækker over manipulation af andre personer fx med henblik på at få dem til at sende fortrolige data eller overføre større pengebeløb.

Social engineering handler derfor i høj grad om, at kriminelle bruger mange forskellige overtalelsesmetoder til at omgå de sikkerhedsforanstaltninger, man i stigende grad implementerer på nettet. Eksempelvis når en borger ringes op af en person, som udgiver sig for at være fra politiet, og derved udsætter personen for bedrageri.

Beskrivelse af kriminalitetsområdet 2/2

Stor sagsvolumen og mindre individuel skade
It-relateret økonomisk kriminalitet varierer meget i forhold til økonomisk skade. I nogle af de sager, politiet modtager, er det beløb, den enkelte har mistet, relativt begrænset. Til gengæld ser vi gerningspersoner, der udsætter en lang række borgere for samme type bedrageri og derved opnår et betydeligt udbytte. Her har vi særligt fokus på seriekriminelle, der bedrager personer via platforme, hvor der handles brugt. De personlige omkostninger for den enkelte i samhandelssager er ofte ikke enorme, men kriminaliteten er med til at finansiere en kriminel løbebane for gerningspersonerne og kan have negative konsekvenser for onlinehandlen.
Af undersøgelsen *It-anvendelse i befolkningen* fremgår det, at 20% af dem, der fravælger at handle online, gør det, fordi de er bekymrede for sælgerens troværdighed (Danmarks Statistik, 2021:17). Tallet inkluderer også webshops, men viser, at mangel på sikkerhed kan være en barriere for at handle online.

Færre anmeldelser og stor skade
På nogle af de sagsområder, NCIK behandler, kan skaden for den enkelte borger eller virksomhed være stor. I 2021 blev der anmeldt 56 sager om ransomware. Det er et relativt begrænset antal sager i forhold til det samlede antal anmeldelser i NCIK, men når en virksomhed får låst sine data i et ransomwareangreb, kan det have enorme konsekvenser. Samtidig udvikler kriminelle hele tiden nye teknikker på området til at lave fokuserede angreb mod udvalgte virksomheder (Europol, 2021:21).

Antallet af personer, der investerer i aktier eller lignende via nettet er steget i 2021 (Danmarks Statistik 2021:21). Samtidig er der i de seneste år set et voksende antal anmeldelser til politiet om falske låne- eller investeringsmuligheder. Ofte er der tale om meget store økonomiske tab i sager om investeringssvindel, og med den øgede interesse for onlineinvesteringer vurderer NCIK, at det er sandsynligt, at flere borgere vil eksponeres for falske investeringsmuligheder. Derfor er forebyggelse vigtigt, så befolkningens modstandskraft øges.

Et andet eksempel på et område, som ikke fylder meget i anmeldelsesbilledet, men har store økonomiske og personlige konsekvenser for den enkelte, er datingsvindel. Her er tale om organiserede kriminelle, der typisk måludpeger deres ofre via sociale medier. NCIK ser både internationalt og i Danmark sager, hvor datingsvindel og investeringssvindel kombineres ved, at den kriminelle etablerer kontakt via fx datingsider, indleder en online relation og efterfølgende får forurettede til at investere på falske investeringssider og/eller i kryptovaluta (Europol, 2021:32; FBI, 2021:1).

Resumé

POLITI

Væsentlige tal 1/2

Anmeldelser om it-relateret økonomisk kriminalitet

- NCIK modtog i 2021 26.588 anmeldelser om it-relateret økonomisk kriminalitet.
- I 2020 var anmeldelsestallet særligt højt, og det er faldet med 9% fra 2020 til 2021. Der er dog samlet set sket en stigning i antal anmeldelser fra 2019 til 2021.
- Samhandel er stadig NCIKs største sagsområde og udgør 43,4% af anmeldelserne.
- Private borgere anmeldte mest samhandel og misbrug af betalingskort.
- Professionelle anmeldte mest sager om misbrug af kortoplysninger, misbrug af adgang til tjenester og kreditbedrageri. På disse områder er der enkelte store virksomheder, som står bag mange anmeldelser.
- Cirka halvdelen af de professionelle anmeldte sager om kontaktbedrageri (primært BEC/CEO fraud). 18,3% anmeldte samhandelssager og 12,6% af de professionelle anmeldte sager om misbrug af kortoplysninger.

Væsentlige tal 2/2

Udviklingen indenfor NCIKs forskellige sagsområder

- Antallet af sager om misbrug af kortoplysninger steg fra 2020 til 2021 med 39%. Tallet inkluderer misbrug i forbindelse med betalingsapps. Dette skal ses i lyset af et fald på området med 12% fra 2019 til 2020. Udviklingen over de tre år skyldes formentlig en kombination af et periodevist lukket natteliv og øget sikkerhed ved online handel med betalingskort.
- I 2021 blev der anmeldt færre sager om kreditbedrageri end i både 2020 og 2019, og der ses særligt et fald i misbrug af stjålen eller falsk identitet.
- Der blev anmeldt 23% færre sager om misbrug af adgang til netbank m.m. i 2021 end i 2020, men der er dog en stigning i forhold til anmeldelsestallet fra 2019.
- Antallet af sager om digital afpresning er faldet markant med 66% fra 2020 til 2021, og vi så ikke i 2021 en lige så stor bølge af sager om masseafpresning som i 2020. Der var dog i marts 2021 et udsving i anmeldelsestallet, som blandt andet skyldtes en stigning i masseafpresningssager i pågældende måned.
- Antallet af sager om kontaktmisbrug mod private steg markant fra 2020 til 2021 med 57%. Her er modus typisk, at gerningspersonen ringer forurettede op og lokker vedkommende til at overføre et pengebeløb under påskud af noget hastende eller som en del af længere tids opbygning af en relation.
- Generelt er der fortsat en tendens til at tekniske sikkerhedsforanstaltninger omgås via manipulation af forurettede til at afgive koder mv. eller selv udføre bankoverførelser, køb at varer, investering i falske værdipapirer etc.

Sådan er sagstallene opgjort i årsrapporten

Når politiet modtager en anmeldelse om it-relateret økonomisk kriminalitet, beriges denne med en såkaldt søgenøgle, som fortæller noget om kriminalitetens art og modus operandi. Det vil sige, at sagen kategoriseres ud fra, hvad der er sket, og hvordan det er sket. Det er disse søgenøgler, der i denne rapport bruges som grundlag for at opgøre antallet af sager på de forskellige områder.

I nogle tilfælde er der overlap mellem de forskellige sagstyper, og der kan også indgå flere former for modus operandi. Eksempelvis kan en sag om investeringssvindel være startet som datingsvindel. Her kan den forurettede have opnået tæt kontakt med en person på en datingplatform og kan derefter være blevet lokket til at investere i kryptovaluta, hvilket sidenhen kan vise sig at være investeringssvindel. For at have det bedst mulige datagrundlag og viden om kriminalitetsbilledet, er sagen i forbindelse med behandlingen blevet kategoriseret både som datingsvindel og investeringssvindel, da begge elementer er indeholdt i sagen. Selve kategoriseringen af sager har ingen betydning for NCIKs indledende efterforskning i sagerne. NCIK bruger primært kategorisering til analyse og statistik.

I denne årsrapport tælles sager ikke flere gange. Heller ikke i de tilfælde, hvor der indgår flere forskellige kriminalitetstyper og modus operandi. NCIK anvender til dette formål en prioriteringsnøgle, hvorved en sag kun tælles i én sagskategori, selvom den også indeholder elementer af en anden. I ovennævnte eksempel ville sagen således tælle med som en sag om datingsvindel, selvom den også handler om investeringssvindel. At investeringssvindel er placeret under kategorien fuphjemmesider, skyldes den datastruktur, man lavede, da NCIK blev oprettet i 2018. Som kriminalitetsområdet har udviklet sig, er investeringssvindel imidlertid flyttet pr. 1 januar 2022 til kategorien kontaktbedrageri mod private.

For yderligere detaljer om data og til- og fravalg, se metodeafsnittet på side 50 i rapporten.

Anmeldelser om it-relateret økonomisk kriminalitet i 2021

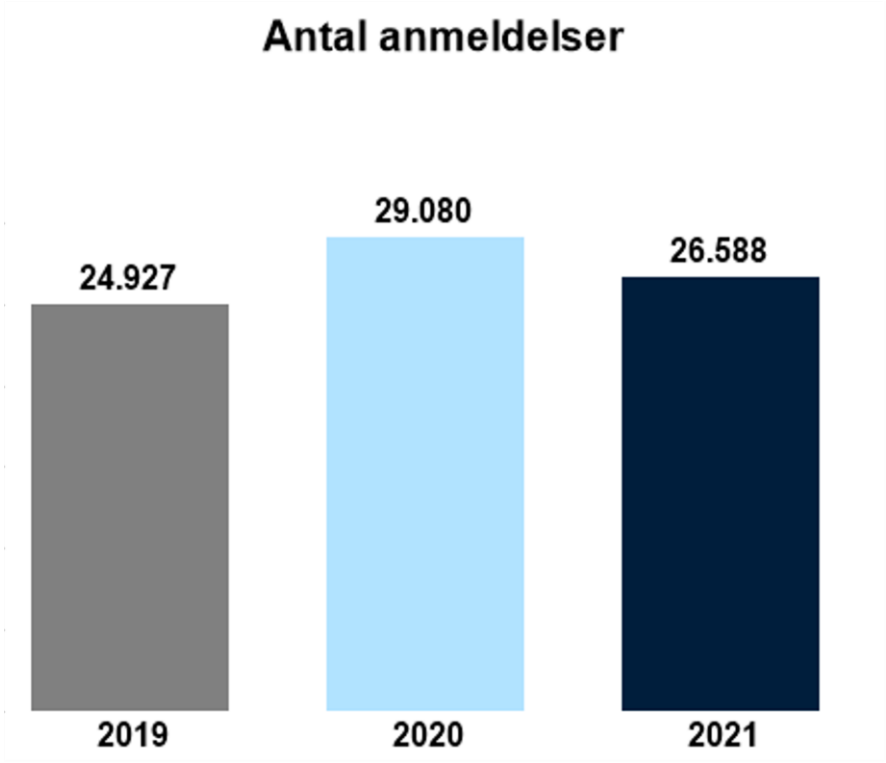
POLITI

26.588

I 2021 modtog NCIK 26.588 anmeldelser om it-relateret økonomisk kriminalitet. Dette tal udgør den primære base gennem hele årsrapporten*

*Se metodeafsnittet for mere information om datagrundlaget i denne rapport.

NCIK modtog 9% færre anmeldelser i 2021 i forhold til 2020



2.492 færre anmeldelser i 2021

NCIK modtog i 2021 26.588 anmeldelser om it-relateret økonomisk kriminalitet. Det er 2.492 færre anmeldelser end i 2020, hvilket svarer til et fald på ca. 9%.

Dette fald skal ses i lyset af, at der i 2019 var 24.927 anmeldelser, og der er således samlet set sket en stigning i anmeldelsestallet i løbet af de seneste to år.

2020 var et særligt år

Ser vi på anmeldelsestallene og deres fordeling i de tre foregående år, stikker 2020 ud på nogle områder. Året var præget af de første bølger af corona og deraf ændringer i adfærd.

Der var i 2020 en stor stigning i andelen af privatpersoner, som handlede med hinanden på nettet og samtidig steg antallet af samhandelssager markant fra 2019 til 2020. Den stigende samhandel er formentlig også et resultat af et øget fokus på genbrug i samfundet.

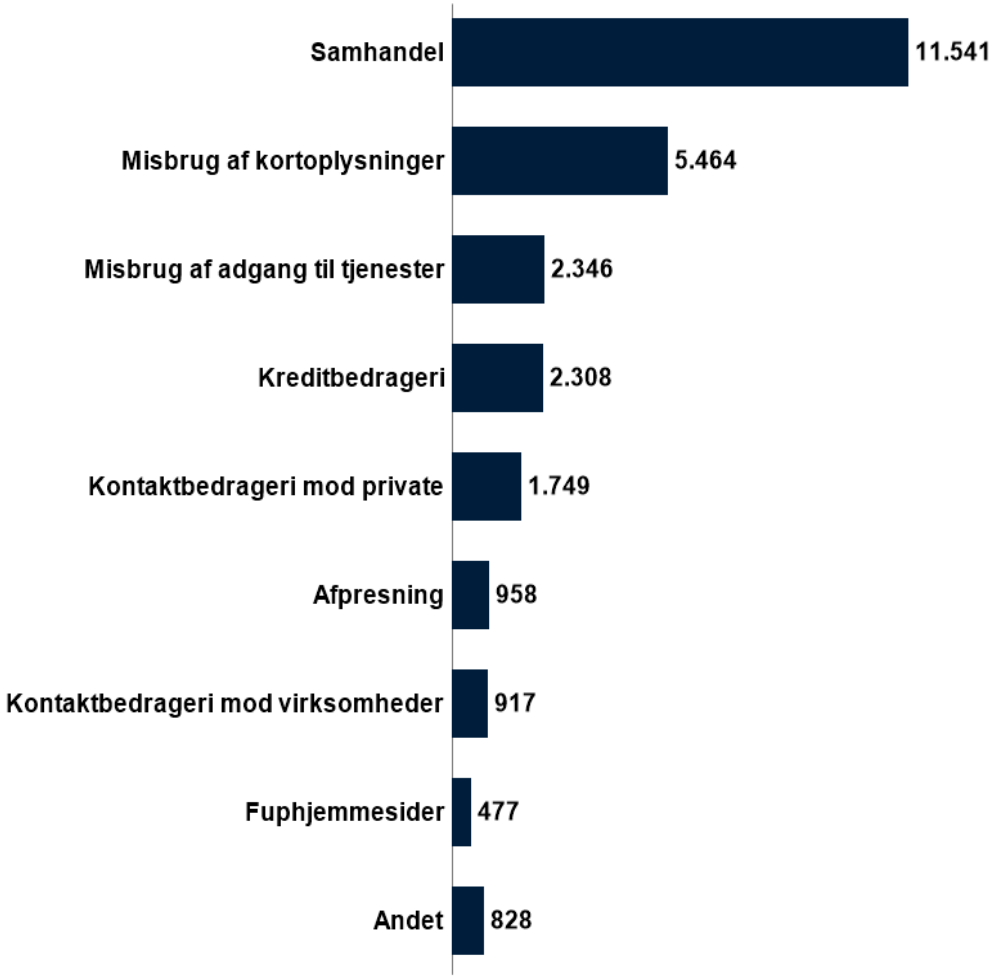
Derudover var nattelivet lukket i store dele af året. Det er en medvirkende årsag til, at vi i 2020 så færre sager om misbrug af betalingskort samtidig med, at implementering af to-faktorverifikation også spiller en rolle.

Ændret opgørelsesmetode i 2021

Det totale anmeldelsestal for 2020 og for 2019 er lavere end det tal, der fremgik af årsrapporten for de to tidligere år. Dette skyldes to faktorer. Dels er anmeldelsesdata dynamiske i de systemer, de trækkes fra, hvorfor der hele tiden sker justeringer, efterhånden som en sag behandles. Dels har NCIK i år justeret i kriterierne for datatrækket. For detaljer om disse ændringer, se metodeafsnittet.

Base: (26.588) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos NCIK i år 2021.

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



Base: (26.588) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos NCIK i år 2021.

Samhandel er stadig NCIKs største sagsområde

43,4% af alle de sager, NCIK modtog i 2021 omhandlede samhandel – det vil sige bedrageri ved handel mellem (oftest) private på online platforme. Selvom sagstallet er faldet med ca. 8% fra 2020 til 2021, er det et område, der fortsat er i vækst, når der sammenlignes med sagstallet for 2019.

Stigning i antallet af sager om misbrug af kortoplysninger

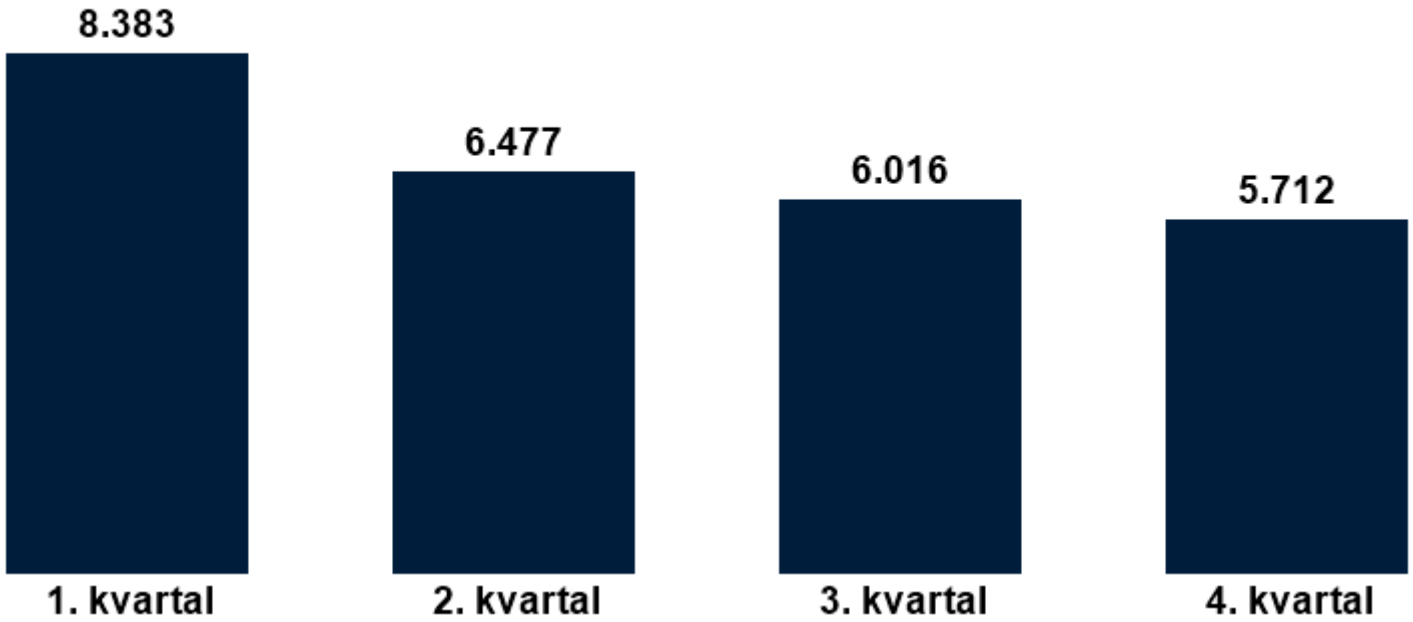
Der er en stigning i antallet af sager om misbrug af kortoplysninger fra 2019 til 2021. Antallet af sager faldt dog i 2020. Det skyldes formentlig både nedlukningen af nattelivet og implementering af to-faktorverifikation af betalinger på nettet (Finanstilsynet 2021; Nets 2020).

At anmeldelsestallet samlet set er steget fra 2019 til 2021, skal formentlig ses som et resultat af en stigning i onlinehandel samtidig med, at vi ser en stigning i sager, hvor der bruges forskellige social engineering-metoder.

Om kategorien 'Andet'

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

NCIK modtog i 2021 særligt mange anmeldelser i 1. kvartal



Gennemsnitligt antal anmeldelser i kvartalet

NCIK modtog i gennemsnit 6.647 anmeldelser i kvartalet i 2021. I 2020 modtog NCIK i gennemsnit 7.476 anmeldelser i kvartalet.

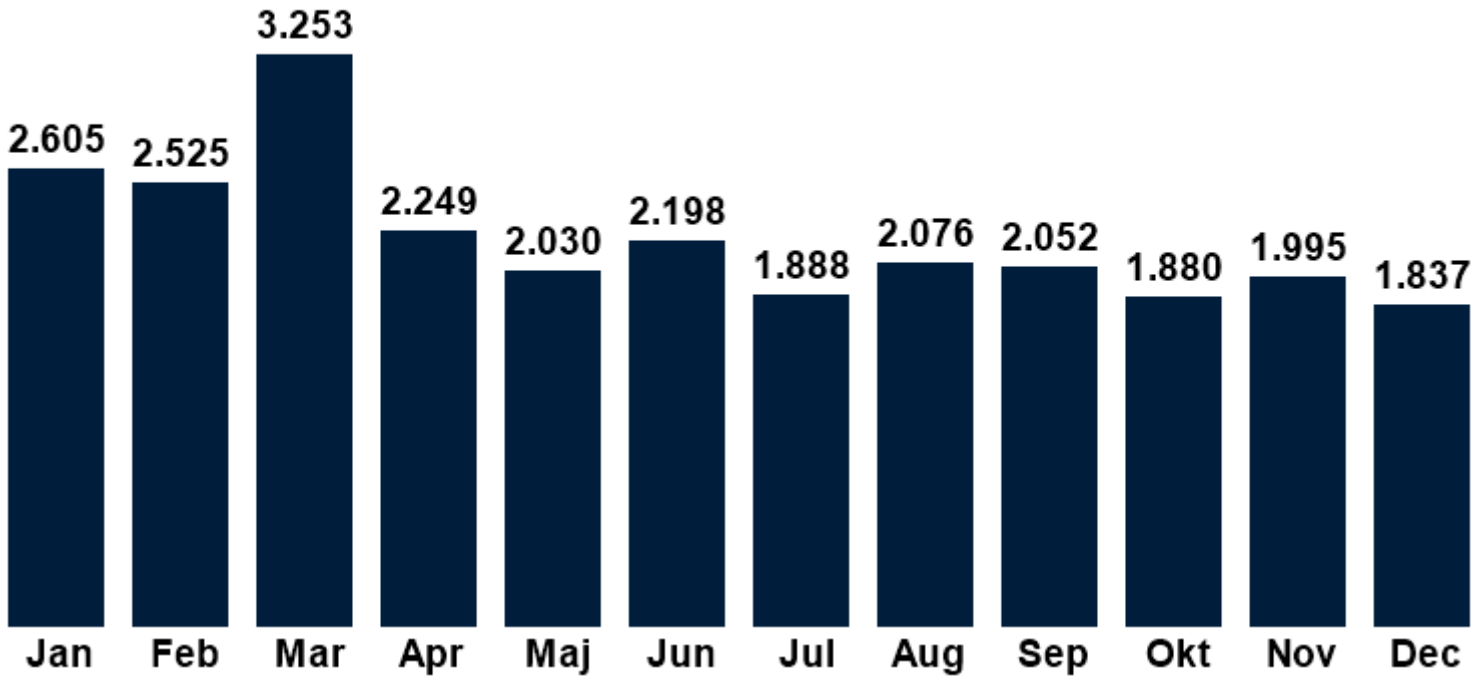
Flest anmeldelser i første halvdel af 2021

56% af anmeldelserne blev modaget i første halvdel af 2021. Det skyldes særligt, at der i marts måned var en bølge af anmeldelser om masseafpresning.

Cirka en tredjedel af anmeldelserne i 2021 blev dermed modtaget i første kvartal.

Base: (26.588) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos NCIK i år 2021.

I 2021 modtog NCIK i gennemsnit 2.215 anmeldelser om måneden



Anmeldelser om måneden

NCIK modtog i gennemsnit 2.215 anmeldelser om it-relateret økonomisk kriminalitet om måneden i 2021.

Til sammenligning modtog NCIK gennemsnitligt 2.492 anmeldelser månedligt i 2020.

Stigningen i marts

Anmeldelsestallet lå i marts 2021 ca. 1.000 sager højere end gennemsnittet. Det skyldes blandt andet, at der var en større bølge af sager om digital afpresning i marts. Der er tale om masseafpresning, hvor et stort antal borgere modtager en mail, hvori der trues med distribution af følsomme oplysninger (som afpresser typisk ikke er i besiddelse af), hvis ikke der betales et beløb i bitcoin.

Herudover er der tale om tilfældige udsving i anmeldelsesbilledet.

Base: (26.588) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos NCIK i 2020.

Langt de fleste anmeldelser om it-relateret økonomisk kriminalitet stammer fra private anmeldere

85% er private anmeldere

I 2021 modtog NCIK 22.675 anmeldelser fra private anmeldere svarende til 85% af alle anmeldelser i 2021.

15% er professionelle anmeldere

I 2021 modtog NCIK 3.943 anmeldelser fra professionelle anmeldere svarende til 15% af alle anmeldelser i 2021.

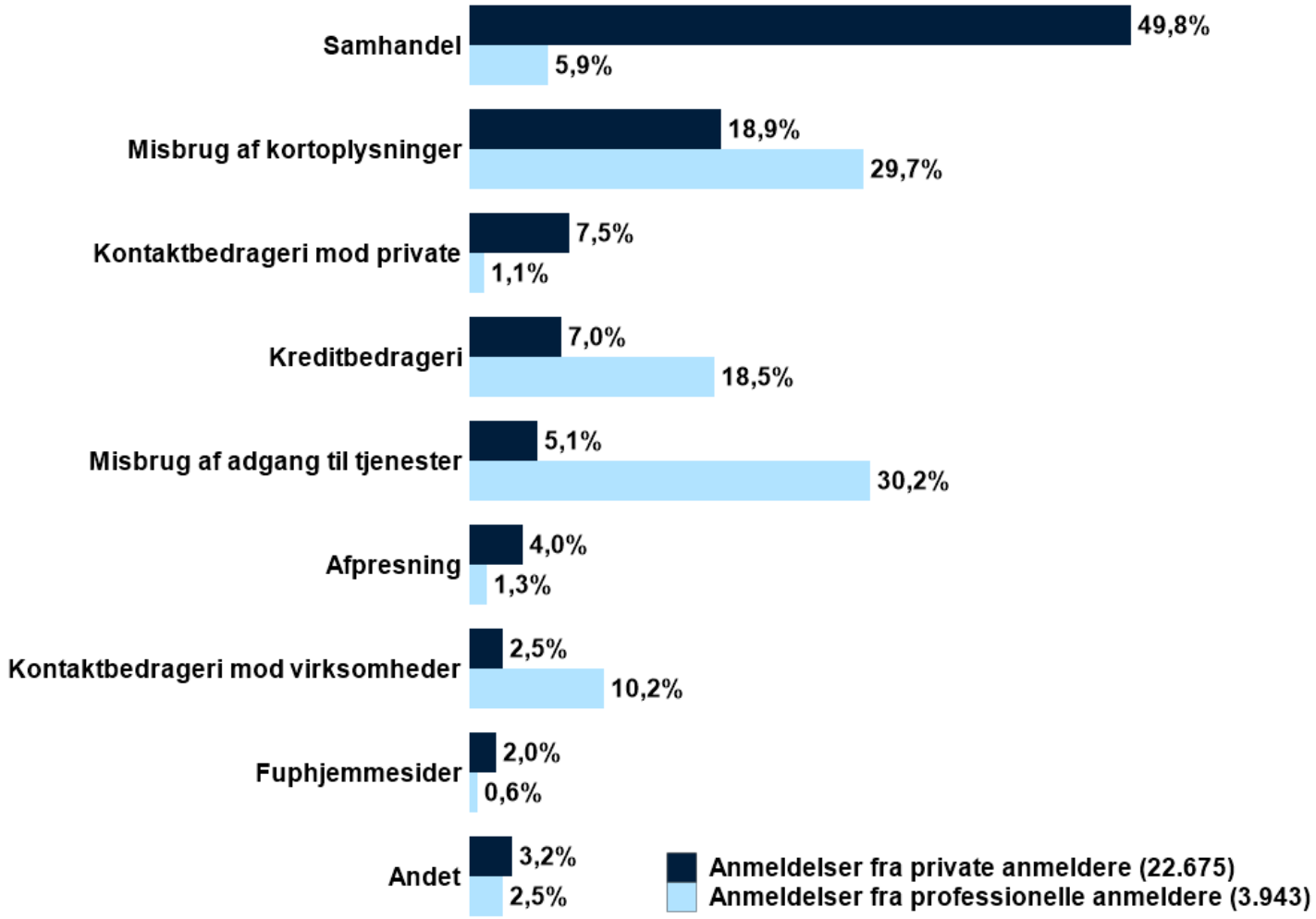
Anmeldere af it-relateret økonomisk kriminalitet opdeles i to grupper

I årsrapporten opdeles anmeldere 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.

Der vil i opgørelsen i nogle tilfælde være tale om, at en person anmelder på vegne af en virksomhed, organisation eller myndighed men anvender sit eget NemID til at registrere anmeldelsen. I disse tilfælde vil den tælle som en anmeldelse fra privatperson, og der vil derfor være en lidt større andel af anmeldelserne, som er fra virksomheder, end opgivet her.

Base: 22.675 anmeldelser er fra privatpersoner. 3.943 anmeldelser er fra professionelle. Nogle anmeldelser har både en privat og en professionel anmelder tilknyttet. Derfor overstiger basen i denne tabel (26.618) det samlede anmeldelsestal (26.588).

Private anmeldte mest samhandel – professionelle anmeldte mest misbrug af kortoplysninger og adgang til tjenester



Private anmeldte i høj grad samhandelsbedrageri

Ca. halvdelen af anmeldelserne fra private anmeldere handlede om samhandel.

Knap 20% af anmeldelserne fra de private anmeldere drejede sig om misbrug af kortoplysninger.

Anmeldelser fra 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. Cirka 60% af anmeldelserne fra professionelle anmeldere kom fra banker og lånevirksomheder. Disse anmeldelser fordeler sig på ca. 50 forskellige professionelle anmeldere.

Base: 22.675 anmeldelser er fra privatpersoner. 3.943 anmeldelser er fra professionelle. Nogle anmeldelser har både en privat og en professionel anmelder tilknyttet. Derfor overstiger basen i denne tabel (26.618) det samlede anmeldelsestal (26.588).

Anmeldelser fra private og professionelle om it-relateret økonomisk kriminalitet fordelt på politikredse

Nordjyllands Politi
1.953 anmeldelser (**7,3%**)

Østjyllands Politi
2.376 anmeldelser (**8,9%**)

Midt- og Vestjyllands Politi
2.059 anmeldelser (**7,7%**)

Sydøstjyllands Politi
1.866 anmeldelser (**7,0%**)

Syd- og Sønderjyllands Politi
1.555 anmeldelser (**5,8%**)

Fyns Politi
2.241 anmeldelser (**8,4%**)

Nordsjællands Politi
2.466 anmeldelser (**9,3%**)

Københavns Vestegns Politi
1.616 anmeldelser (**6,1%**)

Københavns Politi
6.776 anmeldelser (**25,5%**)

Midt- og Vestsjællands Politi
1.727 anmeldelser (**6,5%**)

Sydsjælland og Lolland-Falsters Politi
1.586 anmeldelser (**6,0%**)

Bornholms Politi
120 anmeldelser (**0,5%**)

Base: (26.300) Kortet ovenfor viser 26.341 sager. I 41 sager er der flere anmeldere tilknyttet, som er bosat i forskellige politikredse. Disse 41 sager tæller derfor dobbelt. Herudover er der 243 anmeldelser, hvor bopælskredsen er ukendt.

Særligt mange sager i Københavns politikreds

Hver fjerde anmeldelse i 2021 blev foretaget af en person eller en virksomhed med bopæl i Københavns politikreds. Årsagen til det høje anmeldelsestal i Københavns politikreds er, at langt de fleste virksomheder, der anmelder it-relateret økonomisk kriminalitet har hovedsæde i København. De professionelle anmeldere kan eksempelvis være finansielle institutioner såsom banker, Mobilepay, Nets og lånevirksomheder.

47% af anmeldelserne i Københavns politikreds i 2021 stammer fra professionelle anmeldere. På landsplan er tallet 15%.

Anmeldelser fra private anmeldere fordelt på politikreds

Nordjyllands Politi
1.904 private anmeldelser
Pr. 1.000 indbyggere: **3,6**

Østjyllands Politi
2.312 private anmeldelser
Pr. 1.000 indbyggere: **3,8**

Midt- og Vestjyllands Politi
2.011 private anmeldelser
Pr. 1.000 indbyggere: **3,4**

Sydøstjyllands Politi
1.784 private anmeldelser
Pr. 1.000 indbyggere: **3,7**

Syd- og Sønderjyllands Politi
1.495 private anmeldelser
Pr. 1.000 indbyggere: **3,4**

Fyns Politi
2.144 private anmeldelser
Pr. 1.000 indbyggere: **4,3**

Nordsjællands Politi
2.412 private anmeldelser
Pr. 1.000 indbyggere: **4,1**

Københavns Vestegns Politi
1.529 private anmeldelser
Pr. 1.000 indbyggere: **3,7**

Københavns Politi
3.645 private anmeldelser
Pr. 1.000 indbyggere: **4,6**

Midt- og Vestsjællands Politi
1.692 private anmeldelser
Pr. 1.000 indbyggere: **3,7**

Sydsjælland og Lolland-Falsters Politi
1.537 private anmeldelser
Pr. 1.000 indbyggere: **4,1**

Bornholms Politi
116 private anmeldelser
Pr. 1.000 indbyggere: **2,9**

Base: (22.674) Antal anmeldelser fra private anmeldere modtaget hos NCIK i 2021 med tilknyttede personoplysninger. I 99 anmeldelser var bopælskredsen ukendt.
I seks sager er der flere anmeldere tilknyttet, som er bosat i forskellige politikredse. Disse seks sager tæller derfor dobbelt.

Samhandelsbedrageri

POLITI

Beskrivelse af samhandelsbedrageri

Generelt om samhandelsbedrageri

Samhandelsbedrageri er 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 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 hvorfra de aldrig modtager den købte vare. Sidstnævnte eksempel kan også ramme virksomheder, der køber produkter/ydelser på andre virksomheders hjemmesider (B2B).

I sager om samhandel benytter gerningspersonerne ofte muldyr eller udnytter andres identitet. Et muldyr en person, der modtager penge af gerningsmanden for at sløre pengesporet, eller på anden vis stiller sin konto til rådighed for kriminelle. Derved risikerer muldyret at medvirke til hvidvask.

Fysiske varer

Den udbudte/handlede vare er en fysisk genstand. Det er ofte elektronik, tøj, tasker og tilbehør, der indgår i sagerne. Oftest sætter gerningsmanden en vare til salg, som aldrig fremsendes.

Billetter

Den udbudte/handlede vare er billetter – typisk til populære eller udsolgte koncerter, festivaller, sportsarrangementer mv.

Ved denne form for bedrageri opsøger gerningsmanden ofte den forurettede, efter vedkommende har efterspurgt specifikke billetter på sociale platforme.

Virtuelle effekter

Den udbudte/handlede vare er en virtuel genstand. Handlerne foregår oftest i online spilverdener eller på spilplatforme. Den handlede vare er oftest skins eller virtuel valuta.

Boligudlejning

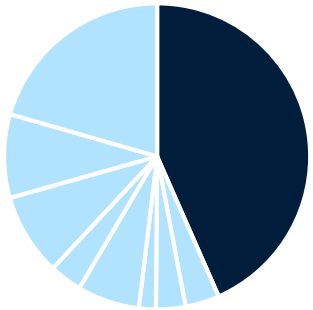
Den udbudte/handlede vare er en bolig til enten langvarig beboelse eller ferieophold.

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

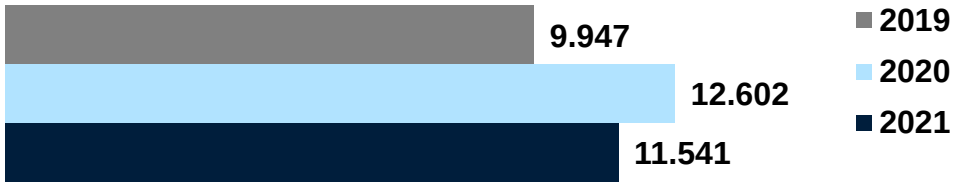
Opmærksomhedspunkter for 2022:

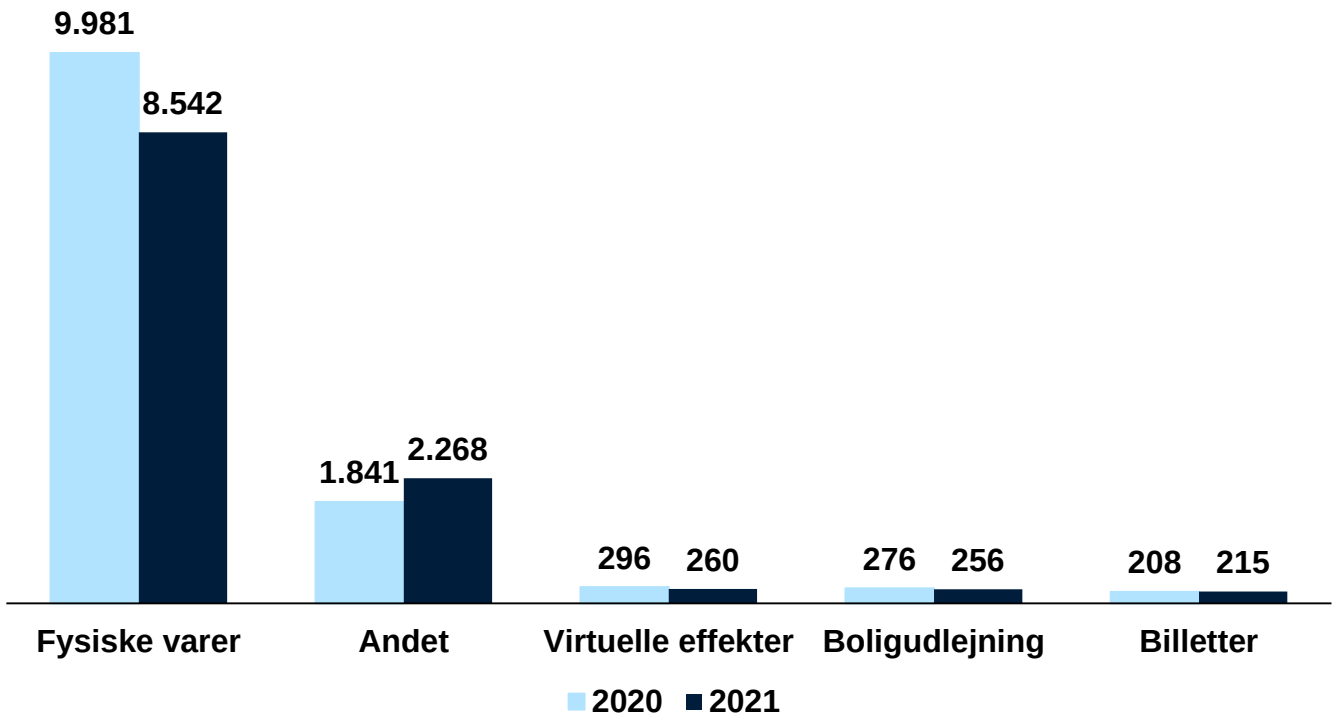
- Der vil igen være adgang til koncerter og festivaler efter COVID-19, og dermed er NCIK opmærksomme på svindel med billetter.
- NCIK har fokus på muldyr, der ofte bruges i samhandelssager i forsøg på at sløre pengesporet.
- NFT er en form for digital vare, fx en fil, et billede eller en sang. Handel med disse varer er populær, og NCIK har allerede set de første sager om svindel med NFT.

Samhandel



43,4% af anmeldelserne til NCIK handlede i 2021 om samhandel (11.541)





Samhandelsbedrageri foregår på forskellige platforme

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

De fleste sager handler om fysiske varer

Ca. 74% af alle sager om samhandel handlede i 2021 om fysiske varer. Der er i både 2020 og 2021 kun ca. 2% af sagerne, der omhandler billetter. Denne del forventes at stige i takt med, at samfundet og muligheden for kulturelle arrangementer er åbnet op efter COVID-19.

Færre sager i 2021 end i 2020

Anmeldelsestallet på samhandelsområdet er faldet med cirka 8% fra 2020 til 2021. Det ligger dog højere end i 2019. Det høje anmeldelsestal i 2020 er formentlig et resultat af fokus på at handle miljøbevidst og grundet nedlukning, som generelt fik e-handlen til at vokse. Ifølge Genbrugsindeks 2021 steg danskernes aktivitet på platformen med 29% i 2020 sammenlignet med året før (DBA, 2021).

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 eller overfører penge 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 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 er det webshoppen, der lider det økonomiske tab.

I andre tilfælde har kortholder ubevidst udleveret oplysninger via forskellige social engineering-metoder. Det kan være opkald fra personer, der udgiver sig for at være vedkommendes bank, SKAT eller anden myndighed (vishing), eller det kan være sms'er eller mails, som får personen til at afgive betalingskortoplysninger.

En nyere form for misbrug af kortoplysninger består af, at gerningsmændene bestiller virtuelle betalingskort på den forurettedes netbank, når de har fået adgang til denne. Det virtuelle betalingskort, som er tilknyttet den forurettedes konto, bliver efterfølgende tilknyttet en betalingsapp og misbrugt.

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, til en postboks eller som elektronisk vare på e-mail.

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

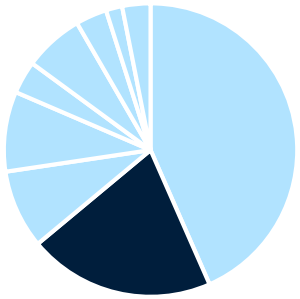
I nogle tilfælde benytter gerningspersoner de stjålne kortoplysninger til at betale for odds hos spillefirmaer. Efterfølgende gevinster udbetales til gerningspersonen, og pengene er herefter vasket hvide.

Opmærksomhedspunkter for 2022

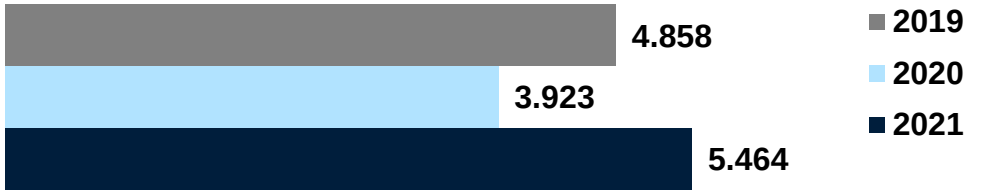
- NCIK retter løbende opmærksomheden mod de forskellige metoder, kriminelle tager i brug for at manipulere med ofrene for at omgå tekniske sikkerhedsforanstaltninger. Det kan blive mere nødvendigt for kriminelle at lokke ofre til at godkende køb på NemID/MitID eller at franarre dem disse oplysninger.

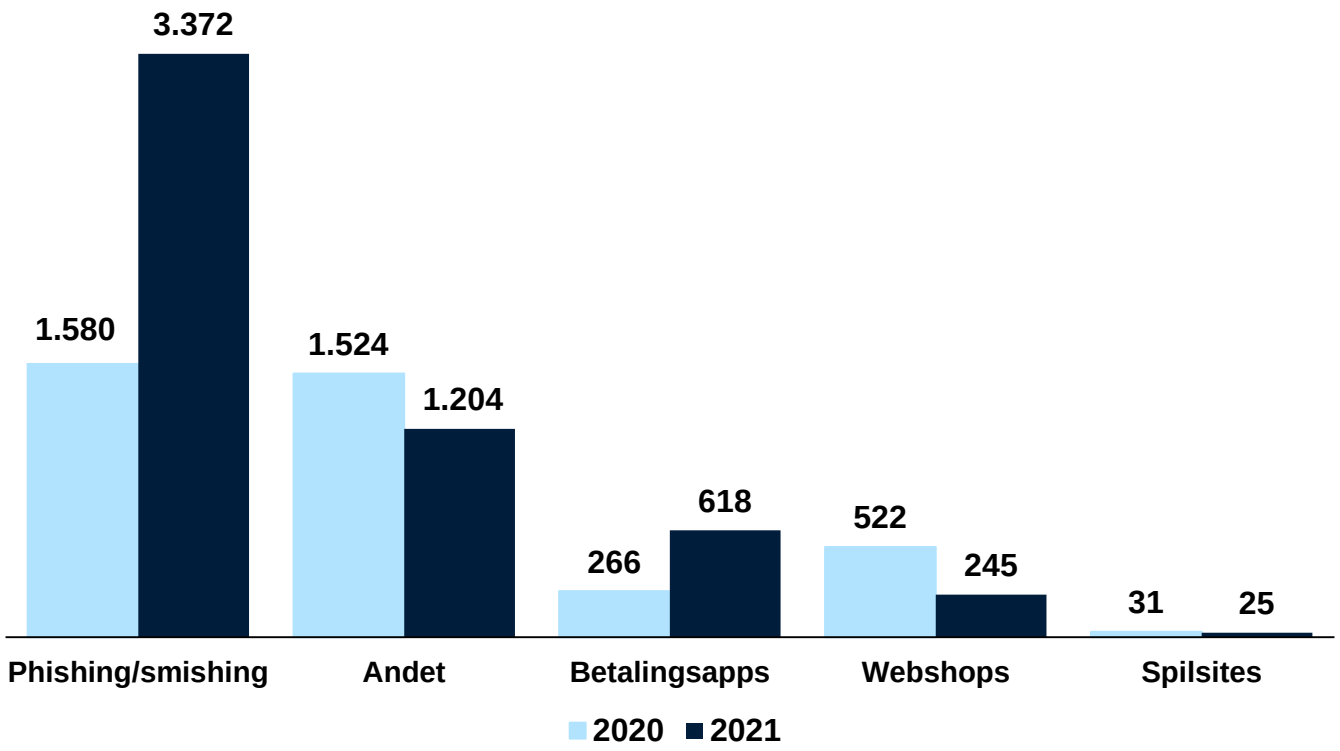
- Genåbning af nattelivet kan føre til øget misbrug af kortoplysninger, fx i forbindelse med misbrug af adgang til betalingsapps.

Misbrug af kortoplysninger



20,6% af anmeldelserne til NCIK handlede i 2021 om misbrug af kortoplysninger (5.464)





Stigning i antallet af sager om misbrug af kortoplysninger

Antallet af sager om misbrug af kortoplysninger er steget med ca. 39% fra 2020 til 2021. Den store stigning skal ses i lyset af, at sagstallet faldt med 12% fra 2019 til 2020. En del af faldet skal formentlig ses som et resultat af nedlukning af nattelivet pga. COVID-19 (og dermed en begrænsning af muligheden for at franarre kort og koder på restaurationer) samt det øgede sikkerhedsniveau på området. Eksempelvis indførslen af to-faktor-godkendelse. Misbrug af kortoplysninger er også misbrug af betalingsapps som fx Mobilepay og tjenester som Apple Pay.

Flere sager omhandler phishing/smishing

Samtidig med øget sikkerhed via to-faktorverifikation ses i 2021 en stigning i antallet af sager, hvor forskellige former for phishing bruges til at opsnappe betalingskortnumre og koder samt opsnappe verificerings-sms'er. I ca. 70% af disse sager er der ikke oplyst et tab.

Kategorien 'Andet'

Kategorien 'Andet' fylder forholdsvis meget i opgørelsen. Det er typisk anmeldelser, hvor anmelder kan se, at der er sket et tab, men ikke ved, hvad der er sket.

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, 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/MitID, 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.

Det er dog blevet sværere at ændre Nemkonto, da der nu sendes fysisk brev ud til godkendelse ved ændring af Nemkonto.

Gerningspersoner får typisk adgang til NemID/MitID og personoplysninger gennem opkald, hvor gerningspersonen udgiver sig for at være fra bank, myndigheder eller lignende, eller ved på anden måde at franarre oplysningerne fra den forurettede.

Kreditbedragerier med falsk eller stjålen identitet

En gerningsperson har fået adgang til en borgers personoplysninger, og misbruger vedkommendes identitet til at oprette lån- eller leasingaftaler. 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 kunder 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 smartphone 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.

NCIK ser sager, hvor den forurettedes identitet bliver misbrugt til at bestille varer ved udenlandske virksomheder til levering i pakkeshops.

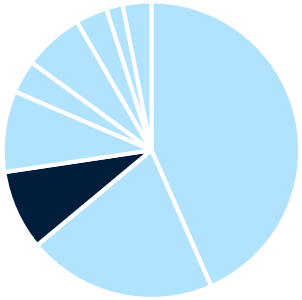
Kreditbedragerier med falske dokumenter

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.

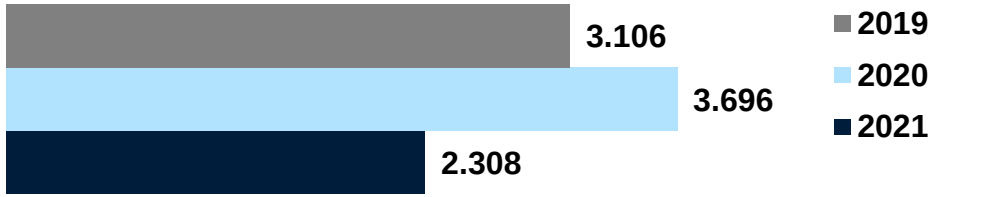
Opmærksomhedspunkter i 2022

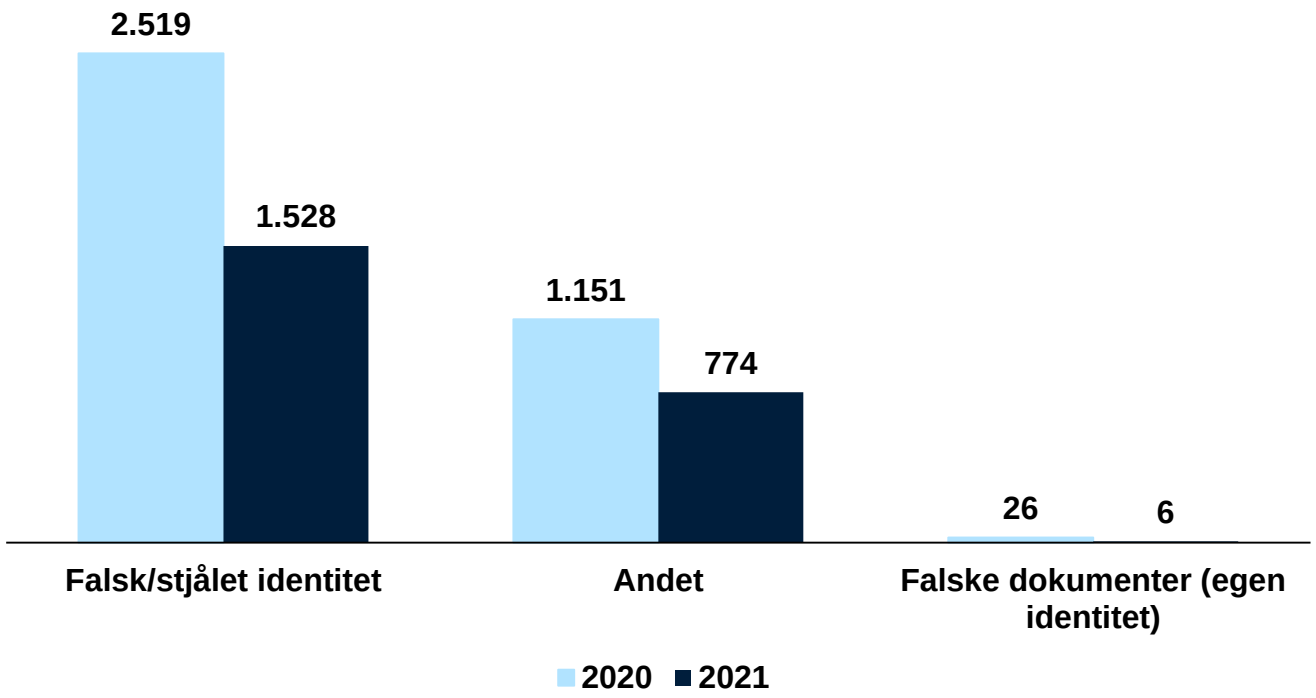
- Da MitID er en ny løsning, har NCIK øget opmærksomhed på eventuel svindel med dette.
- NCIK har desuden opmærksomhed på sager om kreditmisbrug, hvor der oprettes kreditaftaler i forbindelse med køb af fysiske varer på internettet. Disse kreditaftaler kan oprettes uden brug af NemID/MitID-validering.

Kreditbedrageri



8,7% af anmeldelserne til NCIK handlede i 2021 om kreditbedrageri (2.308)





Antallet af anmeldelser om kreditbedrageri er faldet i 2021

Der var fra 2019 til 2020 en stigning i antallet af anmeldelser om kreditbedrageri. Dette tal er faldet i 2021, hvor der var færre anmeldelser om kreditbedrageri end i både 2019 og 2020.

Der oprustes løbende på sikkerhed i sektoren, og det er formentlig med til at forklare det markante fald. Samtidig ser politiet dog også, at de kriminelle løbende forsøger at omgå to-faktorverifikation ved at misbruge identitetsoplysninger, som er franarret den forurettede via telefon, e-mail, sms etc.

Kreditbedrageri med falsk eller stjålen identitet

I de fleste anmeldelser om kreditbedrageri er der tale om en gerningsperson, der enten benytter falske eller stjålne identiteter til at optage kredit i en anden persons navn.

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.

Misbrug af adgang til netbank

Indbrud i netbank bliver ofte begået efter forudgående kontakt, hvor gerningspersonen typisk ringer til en borger 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.

Kriminalitetsformen omfatter ofte 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.

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 mv. Der er også set politianmeldelser, hvor gerningspersonen købte film, streamede sportsevents mv., 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.

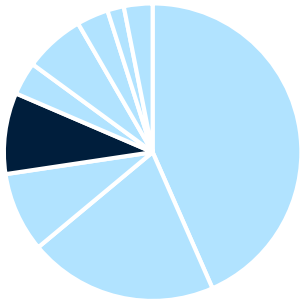
Misbrug af adgang til anden betalingstjeneste

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.

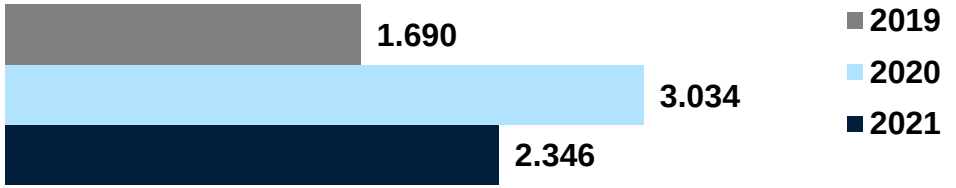
Opmærksomhedspunkter 2022:

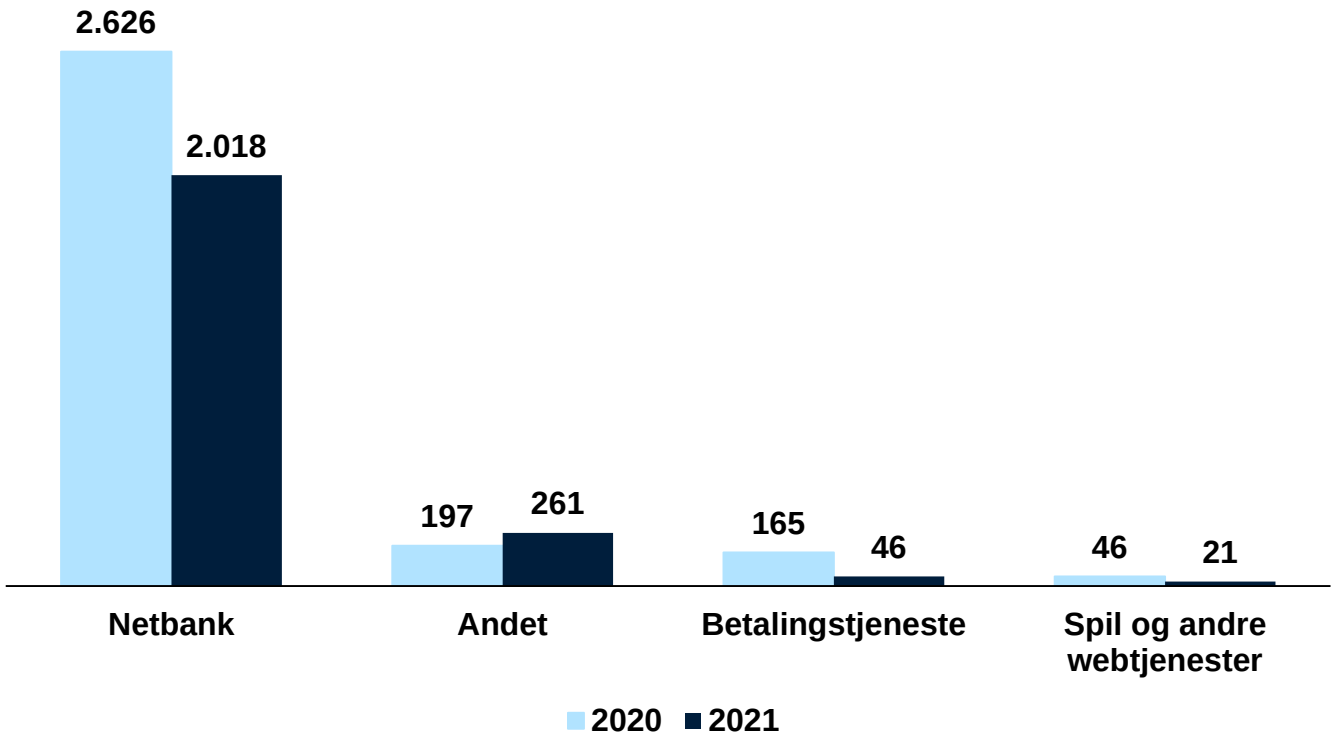
- NCIK har fokus på, at i takt med, det fysiske nøglekort udfases, er der en risiko for flere sager med vishing, hvor transaktionerne sker, mens forurettede er i røret.
- Med genåbning af nattelivet efter COVID-19 øges risikoen for at blive kontaktet af kriminelle, der vil låne en telefon/have hjælp til at få hævet kontanter og derved komme til at medvirke til hvidvask af penge fra bl.a. netbanksindbrud.

Misbrug af adgang til netbank m.m.



8,8% af anmeldelserne til NCIK handlede i 2021 om misbrug af adgang til netbank m.m. (2.346)





Fald i antallet af sager om misbrug af adgang til netbank m.m.

Antallet af anmeldelser om misbrug af adgang til netbank i 2021 er faldet med ca. 23% i forhold til 2020. Der var fra 2019 til 2020 tale om en stor stigning i anmeldelsestallet på dette område, og 2020 har dermed været et år med særligt mange anmeldelser om misbrug af adgang til netbank m.m.. Dette skyldes formentlig en kombination af, at kriminelle i stigende grad har haft held med social engineering-metoder, og at de er blevet mere målrettede og aktive på dette område.

Der er primært tale om sager, der omhandler misbrug af adgang til netbank. Det er et kriminalitetsområde, hvor de kriminelle ofte bruger forskellige social engineering-metoder til at lokke den forurettede til at give adgang til deres netbank.

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 ofte 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 formulering fremstår troværdig.

Der kan være mange forskellige temaer for digital afpresning. NCIK 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. Gerningspersonen forsøger typisk at presse de forurettede til at overføre mindre beløb i kryptovaluta for ikke at dele afpresningsmaterialet med forurettedes kontakter.

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.

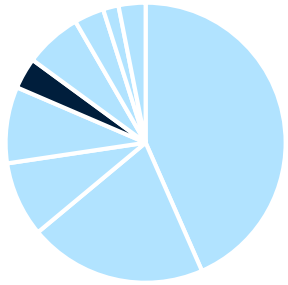
Afpresning med ransomware

Ransomware rettes mod borgere såvel som virksomheder med en overvægt af sidstnævnte. NCIK 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.

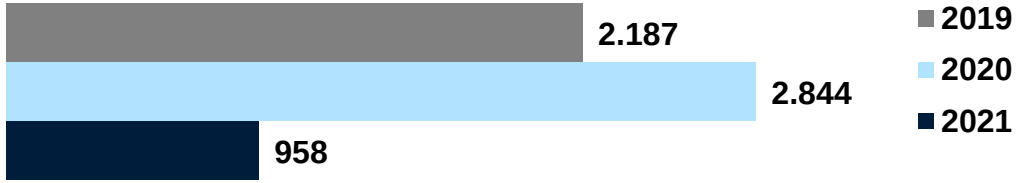
Opmærksomhedspunkter 2022

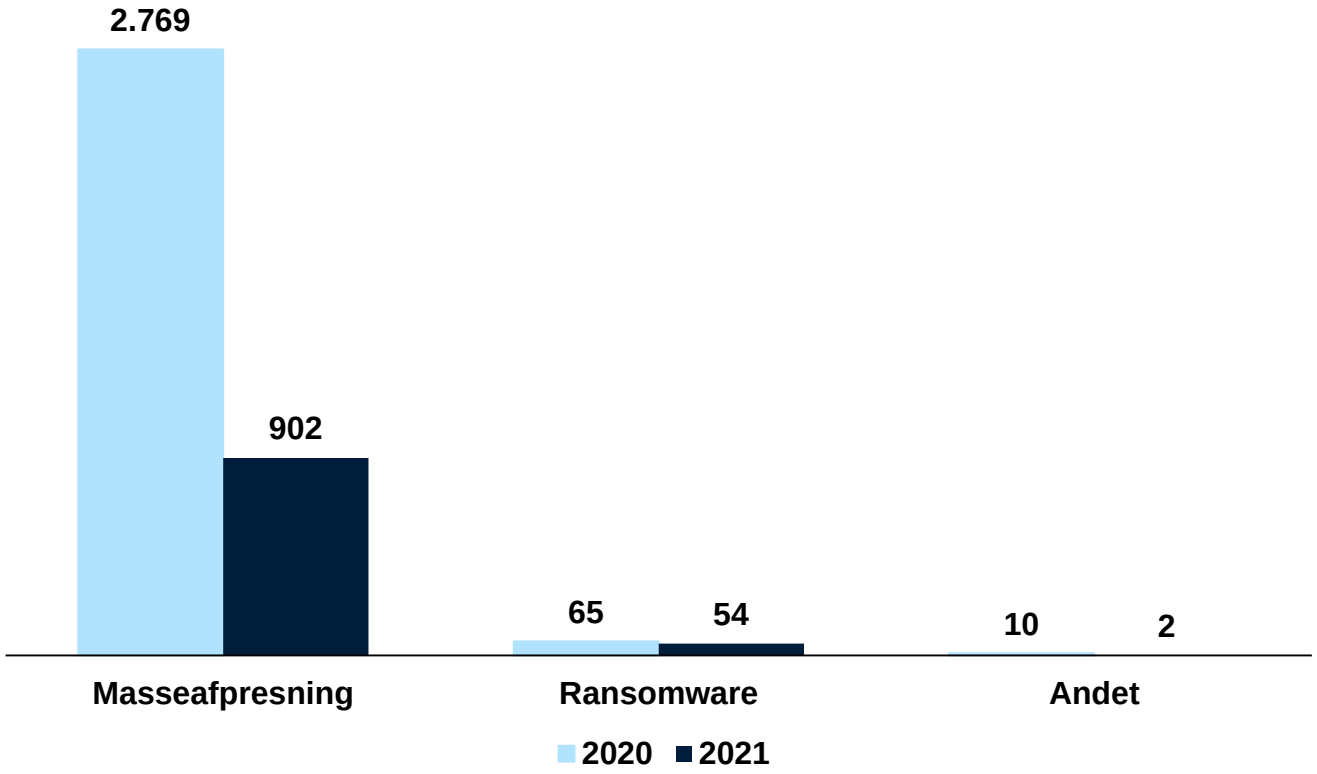
- Anmeldelsestilbøjeligheden er relativt begrænset ved ransomwareangreb, og derfor afspejler anmeldelsestal på området ikke nødvendigvis kriminalitetsudviklingen.
  Angreb med ransomware er målrettede, rettes mod værdifulde mål, og skaden kan være meget stor for den virksomhed, der rammes. Teknik og modus udvikles hele tiden af de kriminelle, og NCIK vil derfor fortsat være opmærksomme på forebyggelse af ransomwareangreb.

Digital afpresning



3,6% af anmeldelserne til NCIK handlede i 2021 om digital afpresning (958)





Stort fald i antallet af sager om digital afpresning i 2021

Sammenlignet med 2020 er antallet af anmeldelser om digital afpresning i 2021 faldet med 66%. Faldet skal ses i lyset af, at der i april 2020 var en stor bølge af masseafpresningssager. I 2021 så vi en mindre bølge af masseafpresningssager i marts måned.

Sager om masseafpresning driver udviklingen indenfor sagsområdet

Langt de fleste af anmeldelserne på området har karakter af masseafpresning, hvor gerningspersoner sender den samme afpresningsmail i generelle vendinger til mange modtagere på én gang. Vi ved, at gerningsmænd sender e-mails eller sms'er til mange respondenter i såkaldte "kampagner", og NCIK advarer derfor offentligheden, når der ses tendens til en ny bølge af disse.

Få anmeldelser om afpresning med ransomware

NCIK modtog i 2021 få anmeldelser om afpresning med ransomware. Vi ved dog, at anmeldelsestilbøjeligheden er lav på dette område, og det er fortsat en aktuel trussel, som både private og offentlige virksomheder bør være opmærksomme på og tage forholdsregler mod (CFCS, 2021:6-9).

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 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. NCIK arbejder med fire overordnede kategorier for kontaktbedrageri.

Microsoftscams

Microsoftscams involverer ikke nødvendigvis en gerningsperson, der udgiver sig for at være fra Microsoft. Det er blot en betegnelse for denne type svindel. 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. Det drejser sig ofte om løfter om større pengebeløb knyttet til en arv fra en udenlandsk advokat. Forud for udbetaling af arven bliver der stillet krav om betaling af arveafgift mv. af det lovede pengebeløb, som aldrig modtages.

Bekendt i knibe

Denne type svindel sker ofte ved, at forurettede bliver kontaktet via e-mail af en person, der udgiver sig for at være en bekendt af forurettede eller dennes nære relationer. Historien udspiller sig typisk således, at er opstået en nødsituation i udlandet, og den forurettede bliver derfor lokket til at foretage konto-til-kontooverførsler eller andre pengeoverførsler.

Datingsvindel

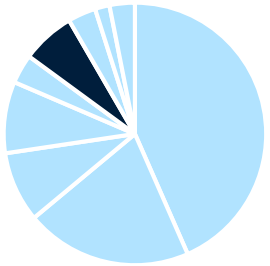
Datingsvindel tager udgangspunkt i, at en person danner relation til en person med falsk identitet via sociale medier. Gerningspersonen med den falske identitet udnytter forurettedes følelsesmæssige involvering og lokker penge ud af vedkommende ved kontooverførsler.

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 store pengebeløb til gerningspersonen.

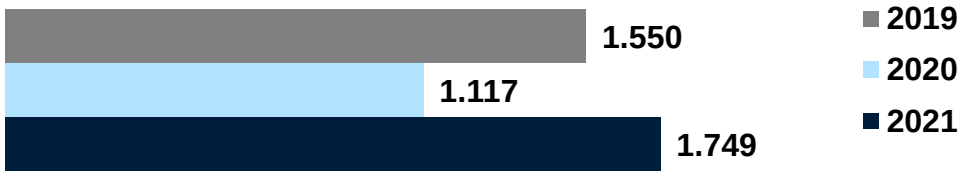
Opmærksomhedspunkter 2022

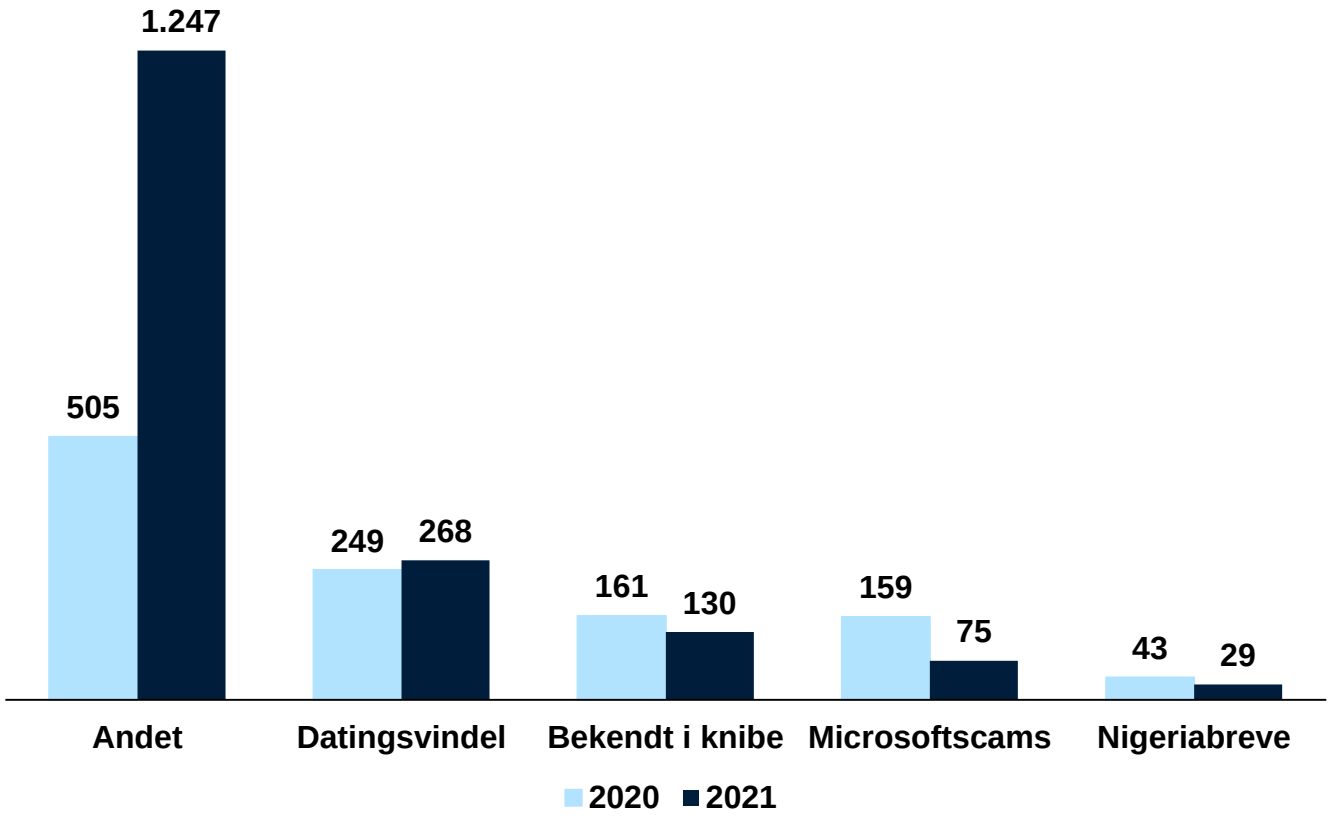
- I takt med indførslen af nye, tekniske løsninger til at forebygge svindel, anvender de kriminelle i stigende grad social engineering-metoder til at skaffe adgang til værdier og personlige oplysninger. I 2022 retter NCIK derfor fortsat opmærksomheden mod nye og vedvarende phishing, vishing og smishing-metoder.

Kontaktbedrageri mod private



6,6% af anmeldelserne til NCIK handlede i 2021 om kontaktbedrageri mod private (1.749)





Flere anmeldelser om kontaktbedragerier mod private

Fra 2020 til 2021 oplevede NCIK en stigning på ca. 57% i antallet af anmeldelser om kontaktbedrageri mod private.

Mange sager udenfor kategori

Den overordnede stigning i antallet af kontaktbedragerier er især båret af en stigning i antallet af anmeldelser, der er kategoriseret som 'Andet' – dvs. udenfor kategori/afventende visitering. Det er eksempelvis sager, hvor forurettede har en vare til salg, og bliver vildledt til at betale forsikring/fragt af en potentiel køber. Herudover er det sager om personer, der bliver kontaktet og franarret penge, idet de bliver kontaktet og lovet gevinst, hvis de spiller via en Oddset-gruppe. Der er også en stigning i anmeldelser, hvor gerningsmanden ringer op, påstår at være fra bank eller politi og lokker forurettede til at overføre penge til en "sikkerhedskonto", under påskud af at vedkommendes netbank er ved at blive hacket.

Andre former for kontaktbedrageri

Antallet af anmeldelser om kontaktbedragerier i form af datingsvindel er steget lidt i 2021, mens antallet af anmeldelser om bekendt i knibe er faldet.

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 det 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-mailkorrespondance mellem to eller flere aktører.

CEO fraud kaldes i Danmark også for direktørsvindel. Ved CEO fraud anvendes ofte spoofing eller typosquatting. Ved hjælp af 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 en medarbejder om at overføre et troværdigt beløb.

Ved typosquatting sørger gerningspersonen for 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 2021 var der flere sager, hvor en virksomhed eller forening modtog e-mails og i få tilfælde opfølgende telefonopkald fra gerningspersonen, der udgav sig for at være direktøren. Af de fremsendte e-mails fremgik det, 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 aktuelt stod på virksomhedens konto.

Kontaktbedrageri mod virksomheder i form af fakturasvindel

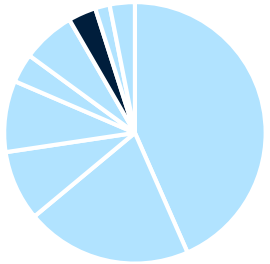
Fakturasvindel minder på mange måder om BEC/CEO fraud, idet gerningspersonen prøver at vildlede den økonomiansvarlige i en organisation til at betale en falsk faktura. Det sker typisk ved, at firmaet modtager en faktura fra gerningspersonen på e-mail, hvor modtagerkontoen kontrolleret af gerningspersonen.

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.

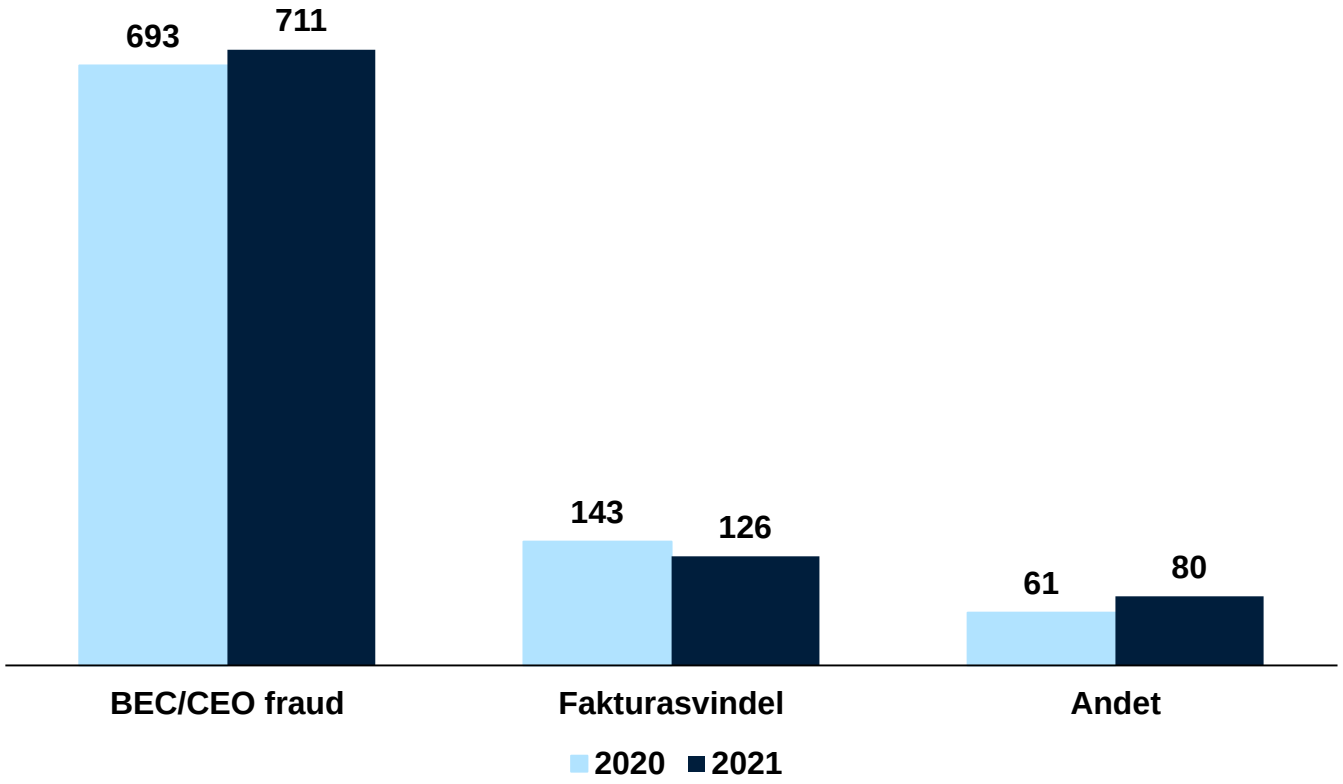
Opmærksomhedspunkter 2022

- BEC/CEO fraud er fortsat en trussel, og der vil i NCIK være opmærksomhed på, om angreb rettes mod særlige sektorer eller mindre professionelle typer af foreninger og organisationer.
- Der er siden efteråret 2020 set en række anmeldelser, hvor en regnskabsmedarbejder i en virksomhed presses både via falsk CEO og falsk afsender af faktura til at overføre et større beløb.

Kontaktbedragerier mod virksomheder



3,4% af anmeldelserne til NCIK handlede i 2021 om kontaktbedrageri mod virksomheder (917)



Flere anmeldelser om kontaktbedrageri mod virksomheder

Der blev i 2021 anmeldt lidt flere sager om kontaktbedrageri mod virksomheder end i 2020. De fleste af disse kontaktbedragerier var i form af BEC og CEO fraud.

Antallet af anmeldelser på området er steget med 9% fra 2019 til 2021 og med blot 2% fra 2020 til 2021.

BEC/CEO fraud fylder mest

De fleste anmeldelser i kategorien ”Kontaktbedrageri mod virksomheder” handler om BEC/CEO fraud, mens antallet af anmeldelser om fakturasvindel er mindre og er faldet lidt fra 2020 til 2021.

I 2021 var der 711 anmeldelser om BEC/CEO fraud og 126 anmeldelser om fakturasvindel. Hertil kommer 80 sager, der endnu ikke er kategoriseret.

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.

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 forskellige fora og annonceringer på sociale medier.

NCIK beskæftiger sig med fuphjemmesider i det omfang, der eksisterer et bedrageriforhold. Sager om selve fuphjemmesiden eller brud på markedsføringsloven er uden for NCIKs sagsområder.

Fuphjemmesider i form af falske låne- og investeringsmuligheder

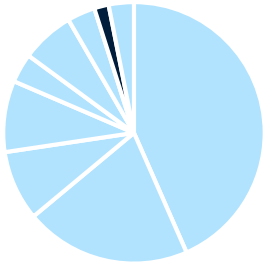
Fuphjemmesider i form af falske låne- og investeringsmuligheder var i 2021 præget af en overvægt til sidstnævnte og typisk i forbindelse med fiktive handler med kryptovaluta. De forurettede reagerede ofte på annoncer på legitime websites (nyhedsmedier, sociale medier mv.) og på fuphjemmesider, der til forveksling lignede legitime, danske 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.

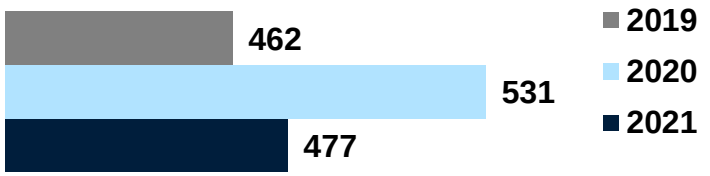
Opmærksomhedspunkter 2022

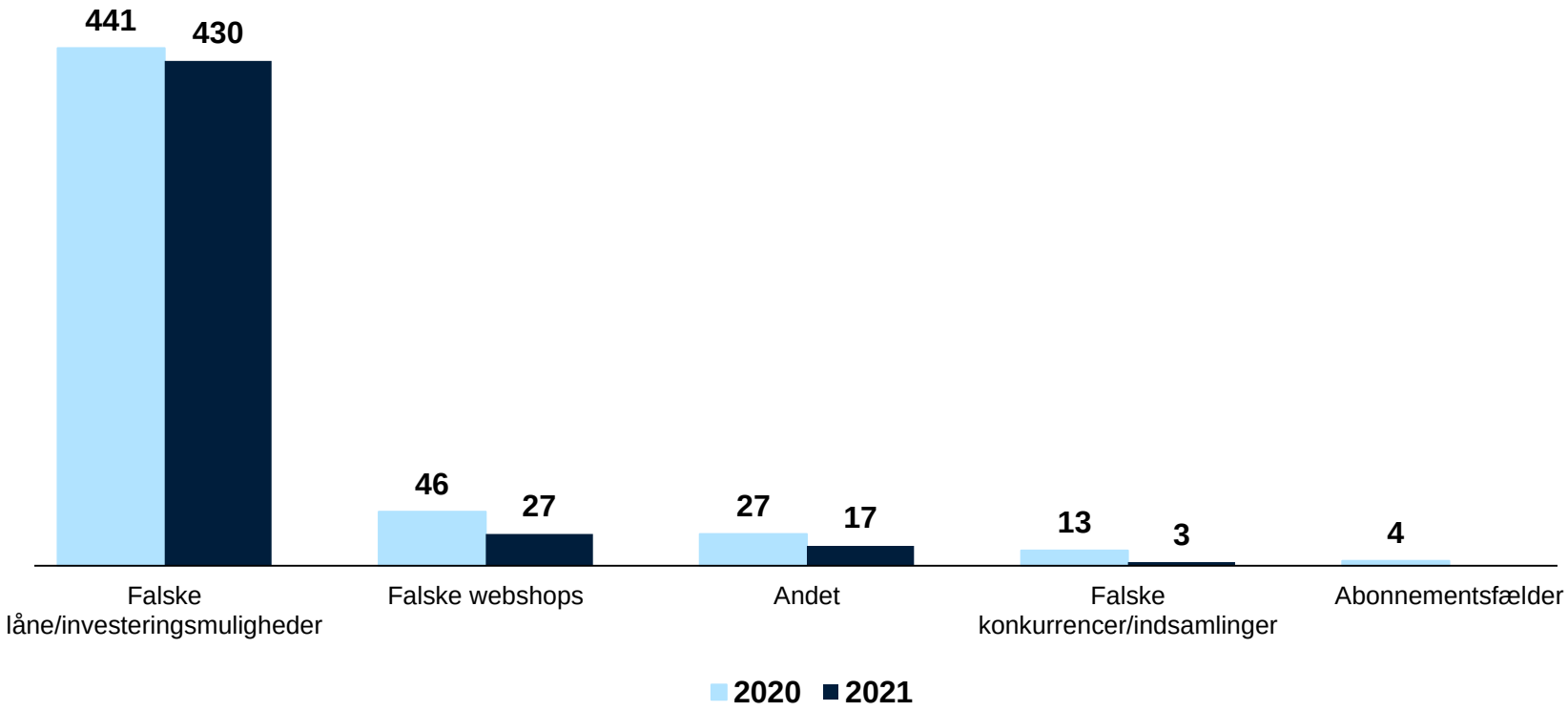
- Investeringssvindel er fortsat et opmærksomhedsområde hos politiet. Det er sager, hvor de forurettede ofte lider store tab, og samtidig er det oftest organiserede kriminelle, der står bag. De kriminelle udvikler løbende nye falske investeringsplatforme og metoder til at lokke investorer mod disse, og arbejder ofte meget professionelt med deres hjemmesider og kontakt til de forurettede. Politiet har bl.a. fokus på, at befolkningens modstandskraft styrkes gennem forebyggelse.

Fuphjemmesider



1,8% af anmeldelserne til NCIK handlede i 2021 om fuphjemmesider (477)





Falske låne/investeringsmuligheder er fortsat en udfordring

Der er i de senere år i dansk politi set et generelt voksende antal anmeldelser om falske låne- eller investeringsmuligheder.

De forurettede kontaktes typisk via sociale medier og hjemmesider og efterfølgende telefonisk af en person, som udgiver sig for at være investor eller investeringsrådgiver.

I nogle sager har forurettede opdaget, at vedkommende er blevet svindlet, men de kriminelle genoptager kontakten og udgiver sig for at være advokater eller lignende, som kan hjælpe med at få det tabte beløb tilbage.

Investeringssvindel er et kriminalitetsområde, der har bevågenhed internationalt, og ifølge Europol ses der en stigning i denne type svindel i hele Europa (Europol, 2021:32).

Forurettede i sager om it-relateret økonomisk kriminalitet

POLITI

Antal forurettede udsat for it-relateret økonomisk kriminalitet i 2021

22.846 forskellige personer

har været udsat for it-relateret økonomisk kriminalitet.

1.202 forskellige professionelle

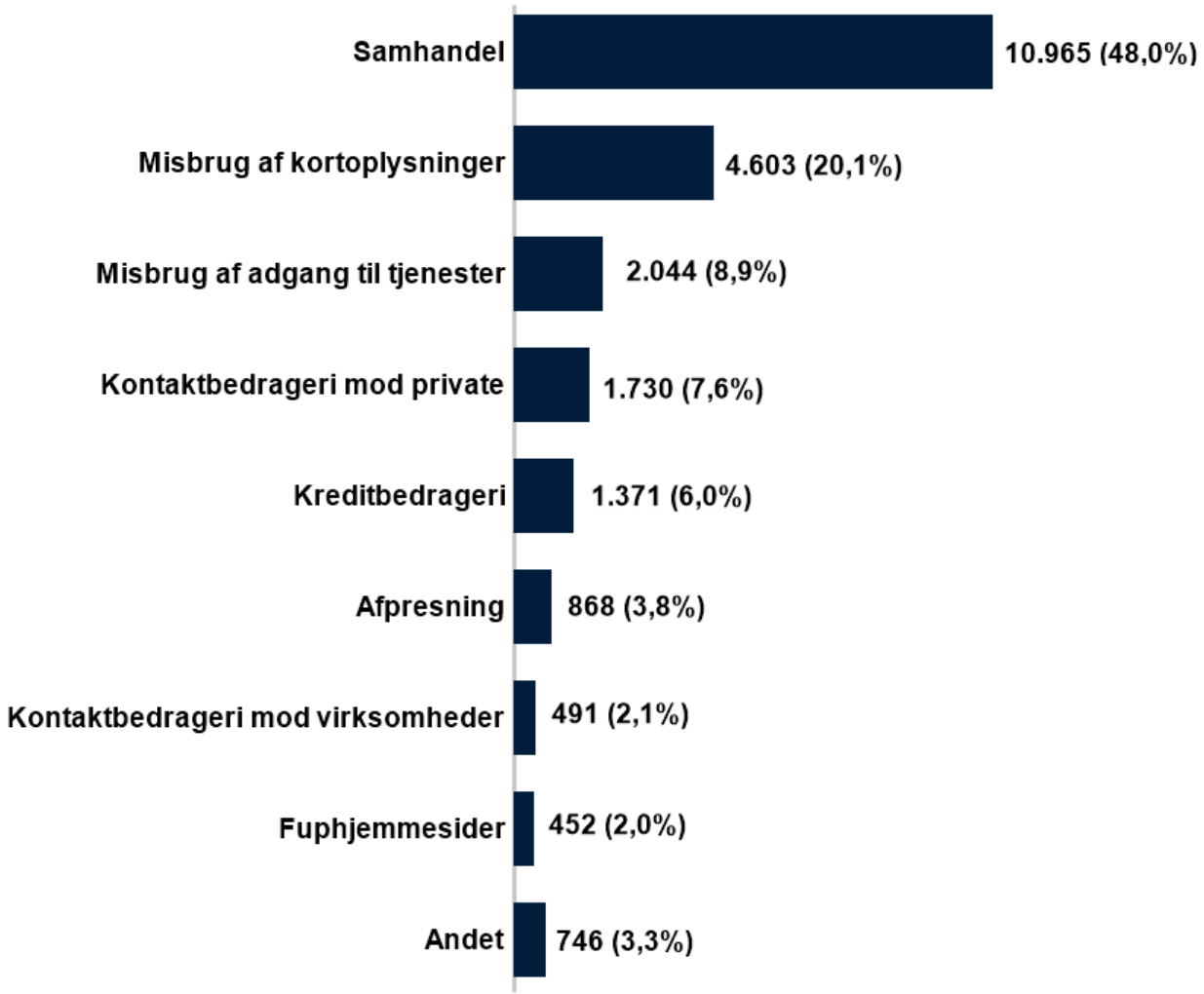
har været udsat for it-relateret økonomisk kriminalitet.

Om de forurettede

Denne del af rapporten tager udgangspunkt i de personer og virksomheder, som har været ofre for it-relateret økonomisk kriminalitet i 2021. I strafferetlige termer benævnes offeret for kriminalitet ofte som den forurettede part i sagen. Derfor bruges betegnelsen 'forurettede' om ofrene for it-relateret økonomisk kriminalitet i årsrapporten.

Som det fremgår af tallene til venstre, er der langt flere private personer, der anmelder it-relateret økonomisk kriminalitet.

Næsten halvdelen af de private forurettede udsættes for samhandelsbedrageri



Base: (23.270) Antal unikke private forurettede inden for hvert sagsområde i 2021.

Antallet af unikke forurettede per sagsområde

Figuren til venstre viser, hvor mange unikke forurettede, der var i 2021 for hvert kriminalitetsområde. Det vil sige, at én forurettet (person) kan tælle én gang for hvert sagsområde.

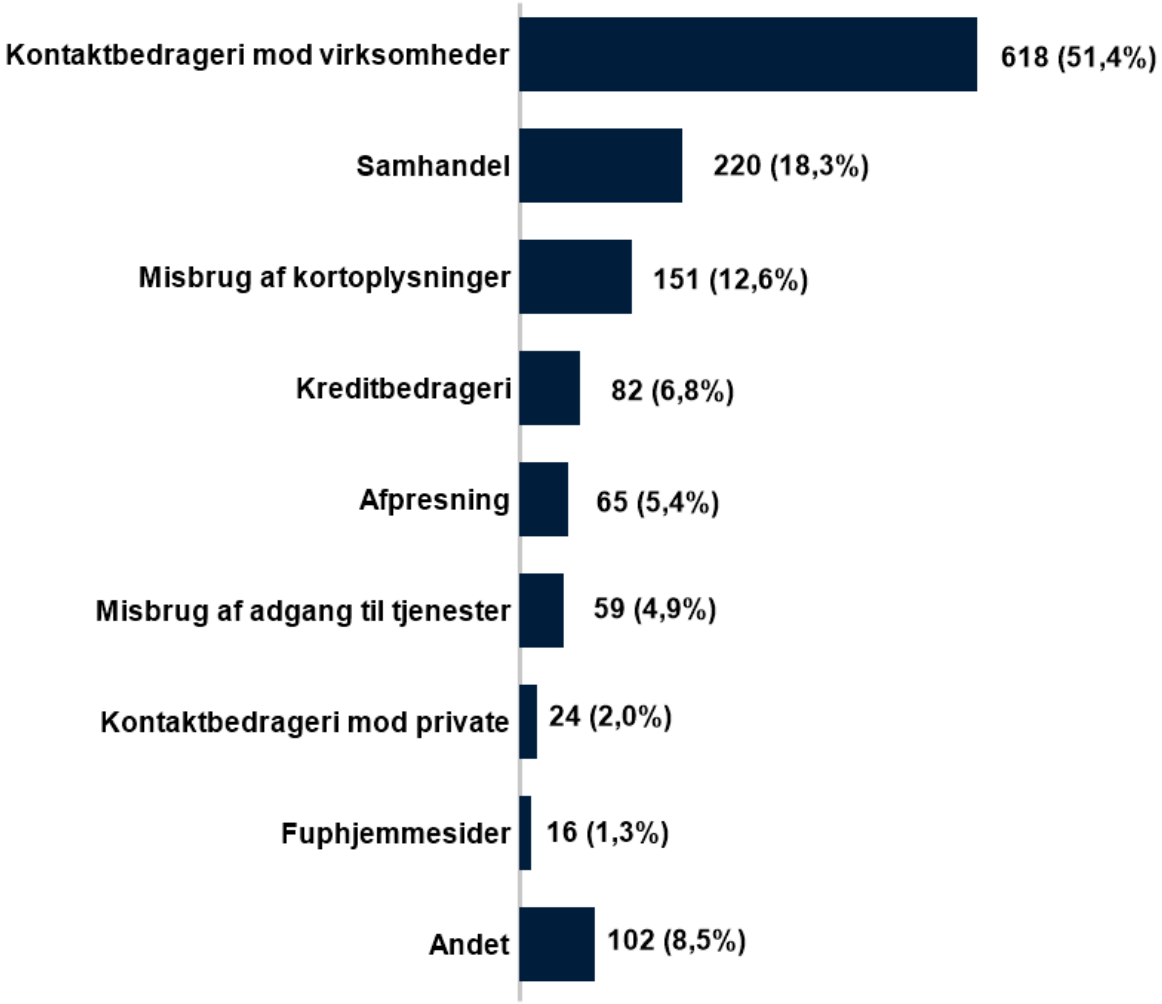
Virksomheder er sorteret fra, og der er således tale om privatpersoner. Knap halvdelen af de personer, der anmeldte til NCIK i 2021, var udsat for samhandelsbedrageri og knap 20% for misbrug af kortoplysninger.

Ca. 70% af privatpersonerne har tilsammen anmeldt sager vedrørende de to hyppigste anmeldelseskategorier. Der kan være stor forskel på det tab, der opleves. Misbrug af identitet og efterfølgende lånoptagelse kan eksempelvis antage mange tusinde kroner, mens der i en samhandelssag kan være tale om få hundrede kroner. Der er således ikke nødvendigvis en korrelation mellem volumen og skade i sager om it-relateret økonomisk kriminalitet.

'Andet'

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

Cirka halvdelen af de professionelle forurettede i 2021 blev udsat for kontaktbedrageri



Base: (1.337) Antal unikke professionelle forurettede organisationer inden for hvert sagsområde i 2021.

Fordeling af professionelle forurettede på NCIKs sagsområder

I figuren er NCIKs 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 2021.

Opgørelsen giver indblik i, hvor mange forskellige professionelle forurettede, der rammes af de forskellige typer af it-relateret økonomisk kriminalitet. Det vil sige, at den professionelle anmelder kan tælle med én gang for hvert kriminalitetsområde.

Hvis den person, der har oprettet anmeldelsen, har brugt sit eget private NemID i oprettelsen, vil anmeldelsen tælle som en privat anmeldelse. En virksomhed kan tælle én gang for hvert sagsområde.

Metode

POLITI

Metode

Rapporten bygger på data fra politiets sagsstyringssystem POLSAS. Derfra er trukket et datasæt med informationer om anmeldelser af it-relateret økonomisk kriminalitet, og de personer, som er involveret i sagen enten som anmelder eller forurettet. Datasættet er behandlet i Qlikview, som er det primære databehandlingsredskab i rapporten.

Opgørelse af anmeldelser

Rapportens datasæt består af anmeldelsestal fra politiets sagsstyringssystem (POLSAS). Data er behandlet i Qlikview-rapporten NCIK Forebyggelse (Årsrapport).

- Data dækker kalenderårene 2019-2021. Data er frosset 1. januar 2022, hvilket betyder, at registreringer foretaget efterfølgende ikke er med.
- Der er trukket sager med søgenøglen 'IT relateret økonomisk kriminalitet'.
- Der er trukket sager med '01LC'-journalnumre (NCIK journalnumre).
- NCIK modtager hver år et antal anmeldelser, der viser sig ikke at omhandle it-relateret økonomisk kriminalitet. Disse sager skal ikke behandles i NCIK og er derfor ikke med i opgørelsen.
- Underforhold skabt af API-løsningen er frasorteret (se også afsnittet om forbehold og definition).
- Hændelser er frasorteret.
- Nogle anmeldelser starter som undersøgelser og får herefter endnu et journalnummer med den relevante gerningskode. Disse undersøgelsesnumre er frasorteret for at undgå, at sagerne tæller dobbelt.

Prioriteringsnøgle

NCIK 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.

Metode

Ændret opgørelsesmetode i 2021

Som det fremgår af side 12 er opgørelsesmetoden ændret i 2021 i forhold til den metode, der er anvendt i årsrapporterne for 2019 og 2020. I denne årsrapport er sager registreret som hændelser fratrukket det totale sagstal. Det samme er sager med undersøgelsesnumre, der efterfølgende har fået endnu et journalnummer.

Desuden er API-sager fratrukket anmeldelsestallet for 2019 i denne rapport, hvilket ikke er tilfældet i tidligere årsrapporter. API-sager blev implementeret i december 2019. Data fra denne årsrapport kan derfor ikke direkte sammenlignes med data fra tidligere årsrapporter, da anmeldelsestallene er trukket på forskellige grundlag.

Dynamiske tal

Opgørelserne i rapporten er dannet på baggrund af dynamiske data. Det betyder, at data ændres løbende i takt med ændringer i registreringer af fx bopæl, personer tilknyttet en sag, søgenøgler etc. Data til denne rapport er låst den 1. januar 2022, men fordi data er dynamiske, betyder det, at data trukket den 1. januar 2022 ikke vil være de samme, som data trukket den 1. januar 2021. Det har naturligvis også betydning for sammenligningsgraden i forhold til tidligere års rapporter.

Metode

Tildeling af NCIK-journalnumre

Størstedelen af anmeldelserne til NCIK modtages gennem anmeldelsesportalen på Politi.dk. Her bliver anmeldelserne automatisk tildelt et NCIK-journalnummer.

En mindre andel af anmeldelserne om it-relateret økonomisk kriminalitet bliver optaget i kredsene og tildelt et kredsjournalnummer.

Frem til fjerde kvartal 2021 blev disse sager omdøbt til et NCIK-journalnummer, når de blev oversendt til NCIK. Omvendt blev sager omdøbt til et kredsjournalnummer, hvis de i visitationen i NCIK viste sig ikke at handle om it-relateret økonomisk kriminalitet.

Siden fjerde kvartal 2021 bliver disse grupper af sager ikke længere omdøbt, men beholder deres oprindelige journalnummer. Det betyder, at der kan være anmeldelser med et NCIK-journalnummer, som burde være frasorteret i opgørelsen og anmeldelser med kredsjournalnumre, der burde være inkluderet.

Det vurderes dog, at der kun er tale om et meget begrænset antal sager, der er overflyttet uden at være omdøbt.

Underforhold oprettet med API-løsningen

Underforhold, der er oprettet via NCIKs API-løsning, er ikke inkluderet i rapportens datasæt.

API-løsningen hjælper enkelte professionelle anmeldere, der anmelder mange forhold. Hvis en sag, der er anmeldt via API-løsningen, har mange underforhold, bliver de derved med det samme registreret med et unikt NCIK-journalnummer.

I sager, hvor API-løsningen ikke anvendes, bliver underforholdene først oprettet under den videre efterforskning i kredsene og får derved ikke et NCIK-journalnummer. Det betyder, at en sag med mange underforhold kan tælle som mange anmeldelser, hvis den anmeldes gennem API-løsningen. Hvis API-løsningen ikke anvendes, tælles sagen i første omgang som en enkelt anmeldelse. For at gøre opgørelsen af anmeldelser så retvisende som muligt, er underforhold oprettet af API-løsningen derfor frasorteret.

Metode

Beskrivelser af NCIKs sagsområder

Årsrapporten indeholder beskrivelser af NCIKs respektive sagsområder (samhandelsbedrageri, kreditbedrageri, misbrug af kortoplysninger etc.).

Beskrivelserne er udarbejdet med udgangspunkt i efterforskernes erfaringer fra de respektive sagsområder i 2021.

Formålet med beskrivelserne er todelt. For det første skal de give læseren den nødvendige 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 så ud i 2021.

Slutteligt skriver vi om NCIKS opmærksomhedspunkter for 2022.

Metode

Kategorisering af personer

Årsrapporten tager udgangspunkt i de personer, der er tilknyttet anmeldelser modtaget i 2021. Borgere og virksomheder kan være tilknyttet anmeldelser som forurettet (FOU), anmelder (ANM) og anmelder og forurettet (A/F).

Private borgere og professionelle anmeldere oprettes automatisk som både anmelder og forurettet (A/F)

Når en borger eller virksomhed anmelder til NCIK gennem anmeldelsesportalen, oprettes de automatisk som både anmelder og forurettet (A/F). Det skyldes, at anmelderen skal være registreret som forurettet, så NCIK kan sende en kvittering for at modtage anmeldelsen. Derfor er der et stort overlap mellem gruppen af anmeldere og forurettede.

Der er ingen garanti for, at anmelder og forurettede er samme person, men det er NCIKs erfaring, at langt de fleste anmeldere også udgør den forurettede part i sagen.

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 personer og organisationer, som er forurettede i forbindelse med den pågældende anmeldelse.

Gruppen af anmeldere består af grupperne: A/F og ANM. Gruppen ANM dækker over anmeldere, der ikke selv er forurettede i sagen.

Metode

Professionelle og private anmeldere

Professionelle anmeldere er defineret ved at have et SE-nummer, mens private personer har et CPR-nummer. Professionelle anmeldere består af virksomheder, myndigheder, foreninger m.m..

I nogle af sagerne er der tilknyttet både en privatperson og en professionel anmelder. Det skyldes oftest, at en person har anmeldt, men har gjort det på vegne af fx en virksomhed. Det betyder, at de private anmeldere og forurettede kan være overrepræsenterede i opgørelserne. Derfor bliver basen i disse opgørelser lidt højere end det samlede antal anmeldelser.

Samtidig kan de professionelle anmeldere være underrepræsenterede, idet en anmeldelse fra dem kan tælle som en privat anmeldelse. Det skyldes, at en person har anmeldt på vegne af en virksomhed, men har brugt sit eget private NemID i oprettelsen.

Da mange af NCIKs sager anmeldes digitalt, bliver oplysninger om anmeldere og forurettede automatisk tilknyttet sagen. Der er dog stadig en lille gruppe sager, hvor der ikke findes oplysninger om anmeldere og forurettede.

I nogle sager er der både private og professionelle anmeldere. I opgørelsen af anmeldere fordelt på de to grupper, er der derfor sager, der både optræder hos de private anmeldere og de professionelle.

Geografisk placering af anmeldelser

Anmeldelserne er placeret geografisk efter den politikreds, anmelder har bopæl i. En anmeldelse kan tælle i flere politikredse, hvis den har flere anmeldere, der bor i forskellige politikredse. En mindre gruppe anmeldelser optræder ikke i de geografiske opgørelser, da anmelders bopæl er ukendt. Der er her taget udgangspunkt i personkategorierne Anmelder/Forurettede og Anmelder.

En del af anmeldelserne fra de professionelle anmeldere kommer fra banker eller andre store virksomheder med mange adresser. Når de anmelder, bruger de deres hovedsæde, som ofte ligger i København. Det er en del af grunden til, at så mange af anmeldelserne placeres i Københavns politikreds.

Kildehenvisninger

DBA (2021) *Genbrugsindekset – 2021*, hentet den 4. marts 2022 fra: https://guide.dba.dk/livsstil/genbrugsindekset-2021

CFCS (2021) *Trusselsvurdering - Cybertruslen mod Danmark 2021,* hentet den 13. marts 2022 fra: https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-danmark-2021.pdf, Center for Cybersikkerhed, FE, juni 2021

Danmarks Statistik (2022) *It-anvendelse i befolkningen 2021,* Danmarks Statistik

Europol (2021) *Internet Organised Crime Threat Assesssment 2021***,** Europol 2021

FBI (2021) *Scammers Defraud Victims of Millions of Dollars in New Trend in Romance Scams,* hentet den 21. marts 2022 fra: https://www.ic3.gov/Media/Y2021/PSA210916

Finanstilsynet (2021) *Temaundersøgelse om brugen af stærk kundeautentifikation i e-handlen,* Finanstilsynet

Nets (2020) *Misbrug på dankort halveret,* Hentet d. 8. marts 2022 fra: https://www.nets.eu/dk-da/nyheder/Pages/Misbrug-pa-Dankort-halveret.aspx

NCIK
NATIONALT CENTER FOR IT-KRIMINALITET

POLITI

NCIK årsrapport 2021