NCIK
NATIONALT CENTER FOR IT-KRIMINALITET

POLITI

NCIK årsrapport 2022

En rapport om it-relateret økonomisk kriminalitet anmeldt i 2022

Indholdsfortegnelse

Indledning	**3**
Om it-relateret økonomisk kriminalitet	**4**
Resumé	**7**
Anmeldelser om it-relateret økonomisk kriminalitet i 2022	**11**
Samhandelsbedrageri	22
Misbrug af kortoplysninger	25
Kreditbedrageri	28
Kontaktbedrageri mod private	31
Misbrug af adgang til tjenester	34
Afpresning	37
Kontaktbedrageri mod virksomheder	40
Forurettede i sager om it-relateret økonomisk kriminalitet	**43**
Opmærksomhedspunkter	**48**
Metode	**53**
Litteraturliste	**59**

Indledning

I denne rapport præsenterer vi anmeldelsesbilledet, som det så ud for it-relateret økonomisk kriminalitet i 2022. Nationalt Center for It-Kriminalitet (NCIK), der hører under National enhed for Særlig Kriminalitet (NSK), har nu været i drift i lidt over fire år, og i den periode har vi generelt modtaget et stigende antal anmeldelser.

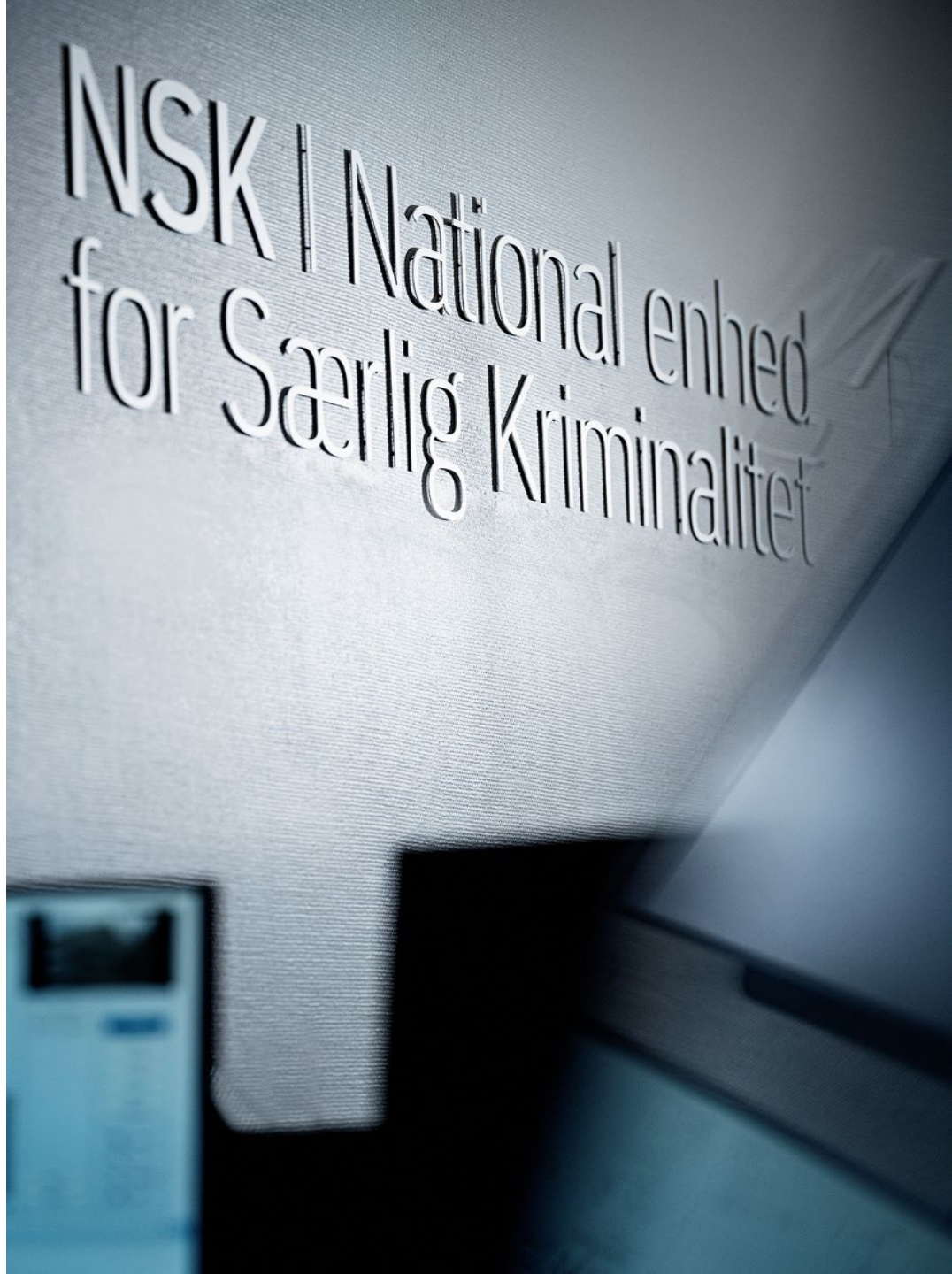
It-relateret økonomisk kriminalitet er et område, der er i konstant forandring, og NCIK arbejder løbende på at tilpasse vores indsatser til disse forandringer. Derfor har vi pr. 1. januar 2022 foretaget ændringer på nogle af kategorierne, som vi sætter på de anmeldelser, vi modtager. Trofaste læsere af årsrapporten vil derfor kunne se, at heller ikke denne årsrapport er én til én sammenlignelig med tidligere årsrapporter.

Årsrapporten indeholder NCIKs 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.

Som noget nyt i år opgør vi også den andel af vores anmeldelser, der kan kategoriseres som enten phishing, smishing eller vishing – og svindel med MitID/NemID. Til sidst i rapporten opridser vi, hvad NCIK har som særlige opmærksomhedspunkter i 2023.

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 og telefoner 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 mange af de sager, politiet modtager, er det beløb, den enkelte har mistet, 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 2022* fremgår det, at kun 30 procent af befolkningen føler sig i høj grad i stand til at genkende svindel på fx falske hjemmesider, mails og annoncer, mens 15 procent i mindre grad eller slet ikke føler sig i stand til at genkende svindel på nettet. De 15 procent udgør i alt 750.000 personer (Danmarks Statistik, 2023:59).

Færre anmeldelser og stor skade
På nogle af de sagsområder, NCIK behandler, kan skaden for den enkelte borger eller virksomhed være stor. I 2022 blev der anmeldt 27 sager om ransomware. Det er et meget 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.

Antallet af personer, der investerer i aktier eller lignende via nettet er faldet lidt i 2022 (Danmarks Statistik 2023:28). Samtidig er der i 2022 set et lille fald i antal anmeldelser til politiet om falske låne- eller investeringsmuligheder. Ofte er der tale om meget store økonomiske tab i sager om investeringssvindel, og FBI opgør i deres årlige Internet Crime Report, at det samlede tab i anmeldelser om investeringssvindel steg fra 1,45 milliarder dollars i 2021 til 3,31 milliarder dollars i 2022 (FBI, 2023:12).

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 ofte i datingsvindelssager, at 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.

Resumé

POLITI

Væsentlige konklusioner 1/2

NCIK modtog **27.066** anmeldelser om it-relateret økonomisk kriminalitet i 2022

Det er en stigning på **2,4** procent i forhold til 2021

Samhandel er stadig NCIKs største sagsområde og udgør ca. **39 procent** af anmeldelserne

Der er samlet set sket en **stigning i antal anmeldelser** fra 2019 til 2022

Væsentlige konklusioner 2/2

Der blev anmeldt ca. **ni procent færre sager om misbrug af adgang til tjenester** i 2022 end i 2021.

Der er primært tale om sager, der omhandler misbrug af adgang til netbank.

I 2022 var der en lille **stigning i sager om kreditbedrageri** i forhold til 2021.

Anmeldelsestallet er dog faldet markant, når der sammenlignes med tallene fra 2019 og 2020.

Antallet af anmeldelser registreret som **misbrug af kortoplysninger faldt fra 2021 til 2022 med ca. 16 procent.**

Faldet skyldes, at vi pr. 1. januar 2022 har oprettet nye og mere retvisende kategorier for denne type sager. Før 1. januar 2022 blev alle sager, hvor forurettede blev franarret oplysninger, registreret som misbrug af kortoplysninger. Med den nye registreringspraksis kan vi opgøre mere præcist, om det er MitID, NemID eller andre oplysninger, der er sagens omdrejningspunkt.

Det betyder, at en del af de sager, der tidligere lå registreret under misbrug af kortoplysninger nu registreres under tværgående tema.

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.

For yderligere detaljer om data og til- og fravalg, se metodeafsnittet på side 53 i rapporten.

Anmeldelser om it-relateret økonomisk kriminalitet i 2022

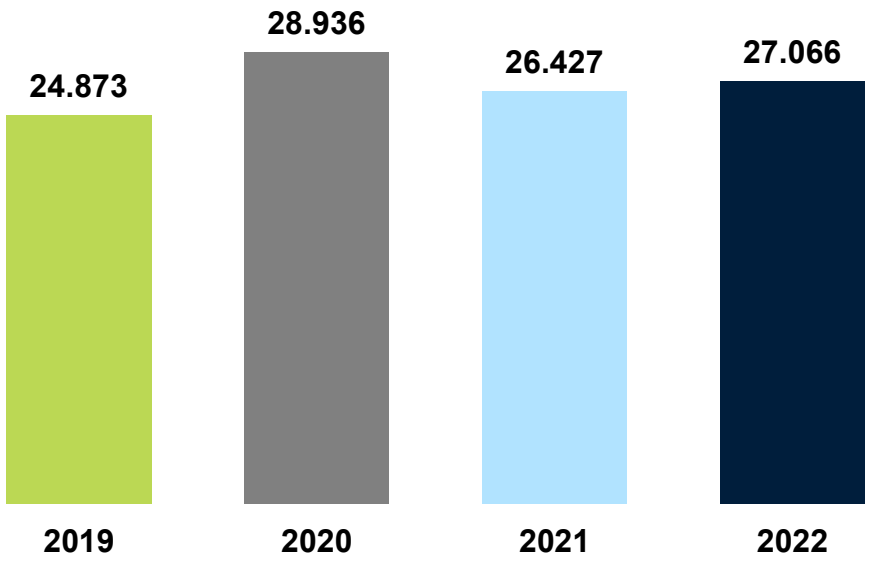
POLITI

27.066

I 2022 modtog NCIK 27.066 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 flere anmeldelser i 2022 i forhold til 2021



Lille stigning i anmeldelsestal

NCIK modtog i 2022 27.066 anmeldelser om it-relateret økonomisk kriminalitet. Det er 639 flere anmeldelser end i 2021, hvilket svarer til en stigning på 2,42 procent.

Denne stigning skal ses i lyset af en samlet stigning i antal anmeldelser om it-relateret økonomisk kriminalitet siden 2019. Ses der bort fra 2020, der var et helt særligt år inden for it-relateret økonomisk kriminalitet på grund af covid-19 og nedlukning af samfundet, er der siden NCIKs opstart i 2019 sket en støt stigning i antal anmeldelser om it-realeret økonomisk kriminalitet.

Ændrede kategoriseringer i 2022

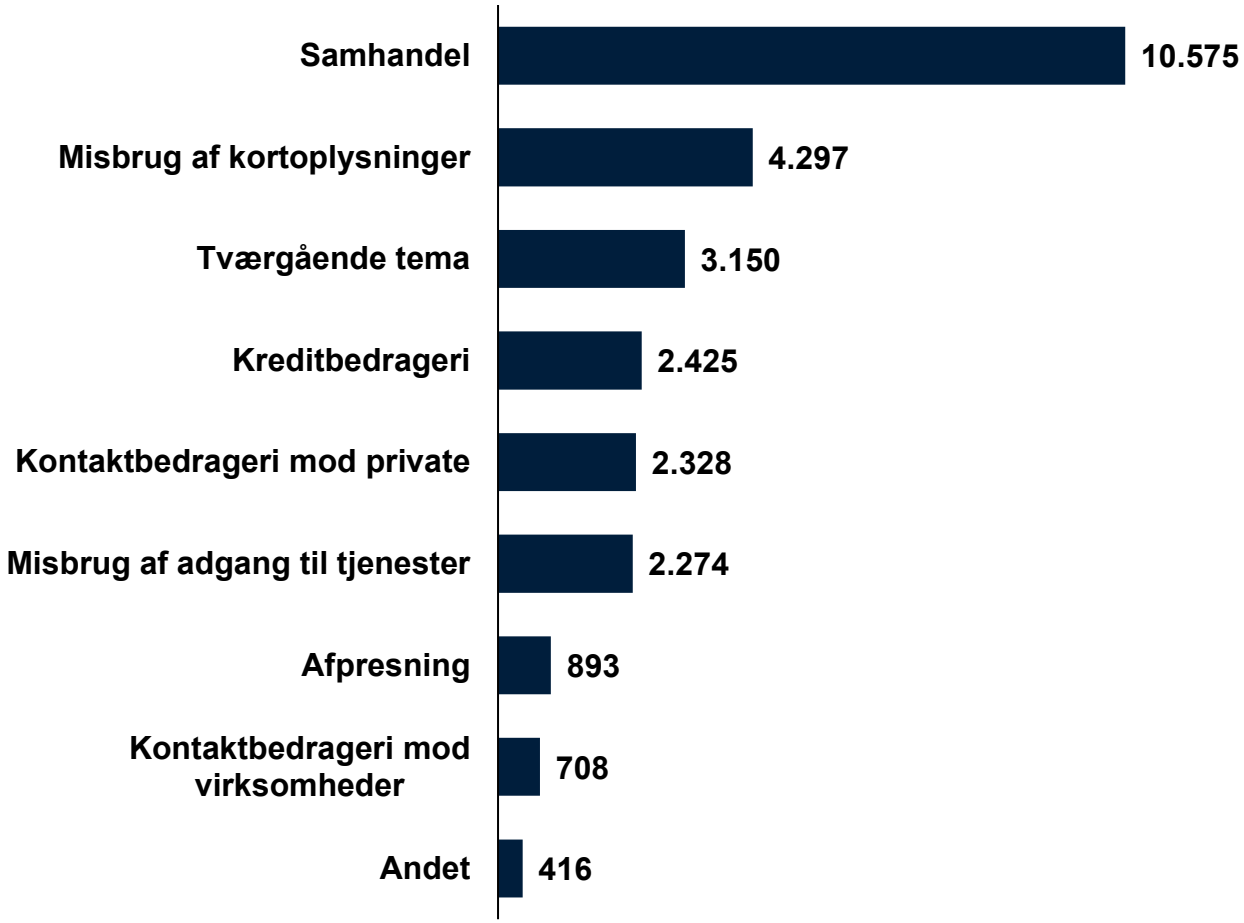
NCIK har pr. 1. januar 2022 ændret i nogle af de kategorier, der sættes på anmeldelserne. Dette er gjort for at tilpasse os kriminalitetsudviklingen. Eksempelvis er investeringssvindel ikke længere kategoriseret under fuphjemmesider, men under kontaktbedrageri mod private.

Dynamiske tal

Det totale anmeldelsestal for 2019, 2020 og 2021 er lavere end de tal, der fremgik af årsrapporterne for de pågældende år. Dette skyldes, at anmeldelsesdata er dynamiske i de systemer, de trækkes fra, hvorfor der hele tiden sker justeringer, efterhånden som en sag behandles. Justeringerne har ingen betydning for sagsbehandlingen.

Base: (27.066) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos NCIK i år 2022.

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



Samhandel er stadig NCIKs største sagsområde

Samhandel er stadig NCIKs største sagsområde. Der ses dog et fald på ca. otte procent i antallet af samhandelssager fra 2021 til 2022. Dette skal formentlig ses i lyset af et fald i antallet af personer, der har handlet nye eller brugte varer af en anden privatperson via handelsplatformene (Danmarks Statistik, 2023:24).

Fra 2021 til 2022 er antallet af anmeldelser om misbrug af kortoplysninger faldet med ca. 21 procent fra 2021 til 2022. Dette skyldes ikke et reelt fald i antallet af anmeldelser, men nærmere, at mange sager, der i 2022 blev registreret i kategorien tværgående tema, dækker over misbrug af kortoplysninger.

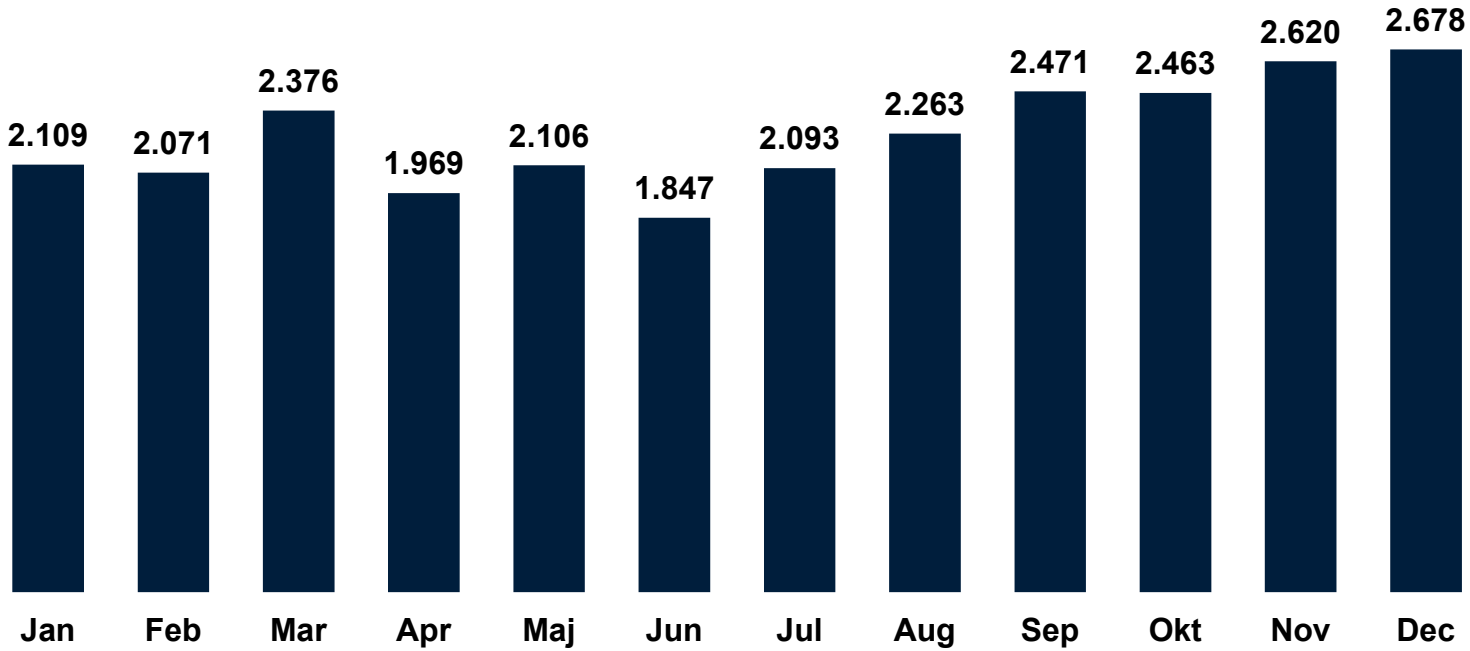
Anmeldelsestallet for kontaktbedrageri mod private er steget med ca. ni procent fra 2021 til 2022. En forklaring på denne stigning er, at vi siden januar 2022 kategoriserer investeringssvindel under kontaktbedrageri mod private, og at vi har set en stigning på ca. 800 sager om telefonsvindel.

Om kategorien Andet

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

Base: (27.066) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos NCIK i år 2022.

I 2022 modtog NCIK i gennemsnit 2.255 anmeldelser om måneden



Anmeldelser om måneden
NCIK modtog i 2022 i gennemsnit 2.255 anmeldelser om måneden om it-relateret økonomisk kriminalitet.

I modsætning til sidste år modtog NCIK flere anmeldelser i anden halvdel af 2022. Stigningen i andet halvår skyldes især en markant stigning i antallet af sager registreret under smishing og en mindre stigning i sager registreret under phishing. Dette dækker blandt andet over sager omhandlende misbrug af kortoplysninger og kontaktbedrageri mod private.

Stigning i marts
Udsvinget i marts måned skyldes en stigning i antallet af anmeldelser om kontaktbedrageri mod private, kreditbedrageri og misbrug af adgang til tjenester.

Udover dette er der tale om almindelige udsving i anmeldelsesbilledet.

Base: (27.066) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos NCIK i år 2022.

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

90 procent er private anmeldere

I 2022 modtog NCIK 24.408 anmeldelser fra private anmeldere svarende til 90 procent af alle anmeldelser.

10 procent er professionelle anmeldere

I 2022 modtog NCIK 2.672 anmeldelser fra professionelle anmeldere svarende til 10 procent af alle anmeldelser.

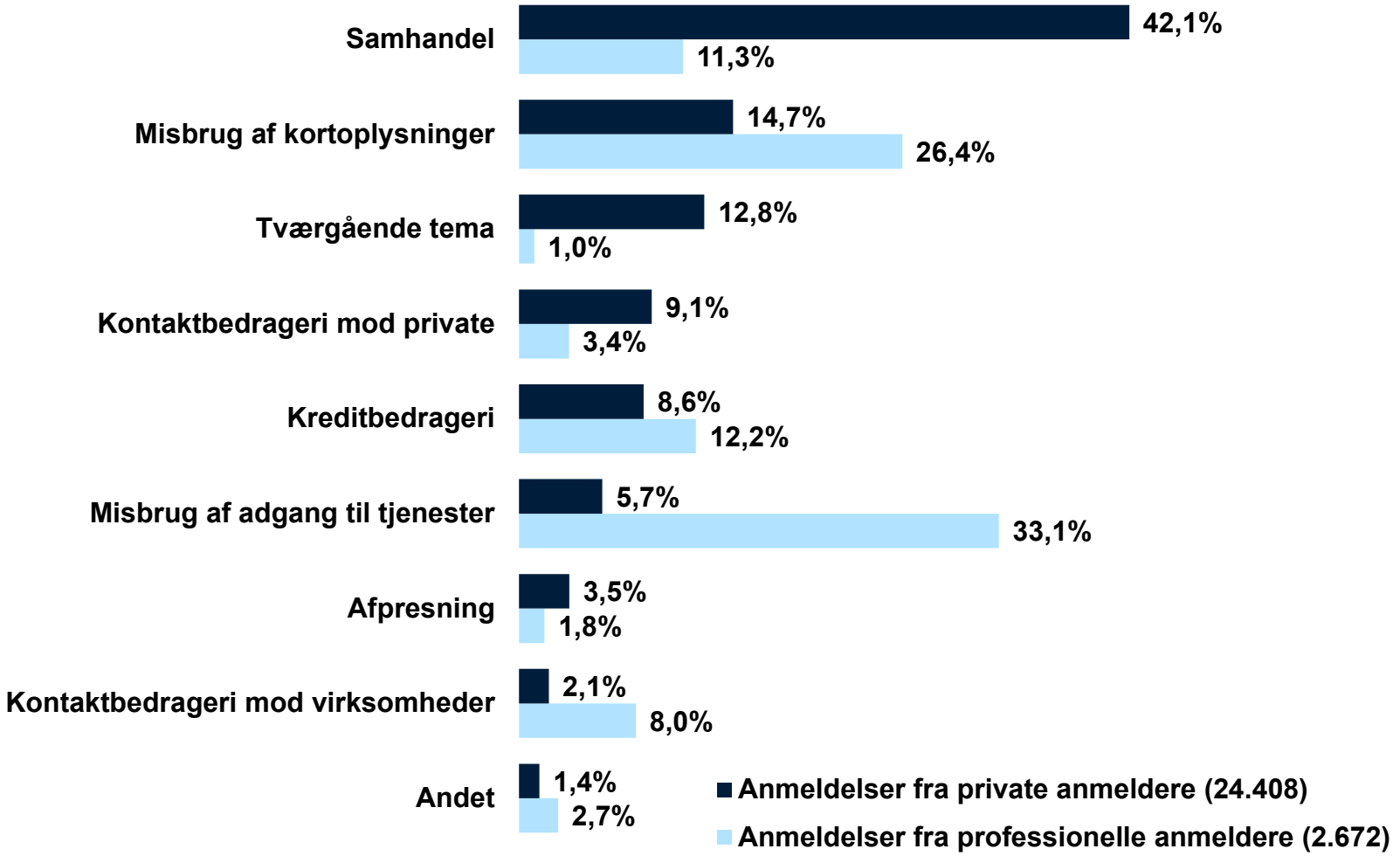
Anmeldere af it-relateret økonomisk kriminalitet opdeles i to grupper

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/MitID 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: 24.408 anmeldelser er fra privatpersoner. 2.672 anmeldelser er fra professionelle. Nogle anmeldelser har både en privat og en professionel anmelder tilknyttet. Derfor overstiger basen i denne tabel (27.080) det samlede anmeldelsestal (27.066).

Private anmeldte mest samhandel, mens professionelle anmeldte misbrug af adgang til tjenester



Private anmeldte i høj grad samhandelsbedrageri

42 procent af anmeldelserne fra private anmeldere handlede om samhandel.

Knap 15 procent 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 tjenester, misbrug af kortoplysninger og kreditbedrageri.

Det er ikke overraskende, at netop disse sagsområder fylder meget i anmeldelser fra professionelle anmeldere. Omtrent 50 procent af anmeldelserne fra professionelle anmeldere kom fra banker og lånevirksomheder. Disse anmeldelser fordeler sig på ca. 45 forskellige professionelle anmeldere.

Base: 24.408 anmeldelser er fra privatpersoner. 2.672 anmeldelser er fra professionelle. Nogle anmeldelser har både en privat og en professionel anmelder tilknyttet. Derfor overstiger basen i denne tabel (27.080) det samlede anmeldelsestal (27.066).

Anmeldelser fra private og professionelle fordelt på politikredse

Nordjyllands Politi
1.824 anmeldelser (**6,8%**)

Østjyllands Politi
2.303 anmeldelser (**8,6%**)

Midt- og Vestjyllands Politi
2.018 anmeldelser (**7,5%**)

Sydøstjyllands Politi
1.890 anmeldelser (**7,1%**)

Syd- og Sønderjyllands Politi
1.609 anmeldelser (**6,0%**)

Fyns Politi
2.221 anmeldelser (**8,3%**)

Nordsjællands Politi
3.417 anmeldelser (**12,8%**)

Københavns Vestegns Politi
1.905 anmeldelser (**7,1%**)

Københavns Politi
5.605 anmeldelser (**20,9%**)

Midt- og Vestsjællands Politi
2.047 anmeldelser (**7,6%**)

Sydsjælland og Lolland-Falsters Politi
1.791 anmeldelser (**6,7%**)

Bornholms Politi
178 anmeldelser (**0,7%**)

Base: (26.759) Kortet ovenfor viser 26.808 sager. I 49 sager er der flere anmeldere tilknyttet, som er bosat i forskellige politikredse. Disse 49 sager tæller derfor dobbelt. Herudover er der 276 anmeldelser, hvor bopælskredsen er ukendt.

Anmeldelser fra professionelle anmeldere fordelt på politikreds

Nordjyllands Politi
119 anmeldelser (**4,5%**)

Østjyllands Politi
193 anmeldelser (**7,2%**)

Midt- og Vestjyllands Politi
93 anmeldelser (**3,5%**)

Sydøstjyllands Politi
123 anmeldelser (**4,6%**)

Syd- og Sønderjyllands Politi
110 anmeldelser (**4,1%**)

Fyns Politi
161 anmeldelser (**6,0%**)

Nordsjællands Politi
120 anmeldelser (**4,5%**)

Københavns Vestegns Politi
124 anmeldelser (**4,6%**)

Københavns Politi
1.438 anmeldelser (**53,8%**)

Midt- og Vestsjællands Politi
97 anmeldelser (**3,6%**)

Sydsjælland og Lolland-Falsters Politi
90 anmeldelser (**3,4%**)

Bornholms Politi
4 anmeldelser (**0,1%**)

Base: (2.672) Antal anmeldelser fra professionelle anmeldere fordelt på politikreds.

Særligt mange sager i Københavns politikreds

Mere end hver anden anmeldelse fra professionelle anmeldere i 2022 blev foretaget 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.

Samhandelsbedrageri

POLITI

Beskrivelse af samhandel

Om samhandel

Samhandelsbedrageri er handel mellem to eller flere parter, hvor den ene part ikke overholder sin del af aftalen. Handlen er oftest mellem borgere, der handler med hinanden på handelsplatforme eller sociale medier.

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 eller ydelser på andre virksomheders hjemmesider (B2B).

I sager om samhandel benytter gerningspersonerne sig ofte af muldyr eller udnytter andre personers identitet. Et muldyr er en person, der modtager penge af en gerningsperson for at sløre pengesporet, eller på anden vis stiller sin konto til rådighed for kriminelle. Derved medvirker muldyret til hvidvask.

Fysiske varer
I en sag om svindel med fysiske varer, er der ofte tale om elektronik, tøj, tasker og tilbehør. Typisk sætter gerningspersonen en vare til salg, som aldrig sendes til køber.

Billetter
I sager om svindel med billetter er det typisk billetter til populære eller udsolgte koncerter, festivaler, sportsarrangementer mv. der er omdrejningspunkt for sagen.

Virtuelle effekter
Samhandelsbedrageri omhandler også virtuelle effekter, som særligt har værdi i online spilverdener eller på spilplatforme. Den handlede vare er typisk skins eller virtuel valuta.

Boligudlejning
I sager om boligudlejning betaler forurettede typisk for leje af en feriebolig eller permanent bolig. Gerningspersonen udlejer fiktive boliger eller boliger, som personen ikke har råderet over.

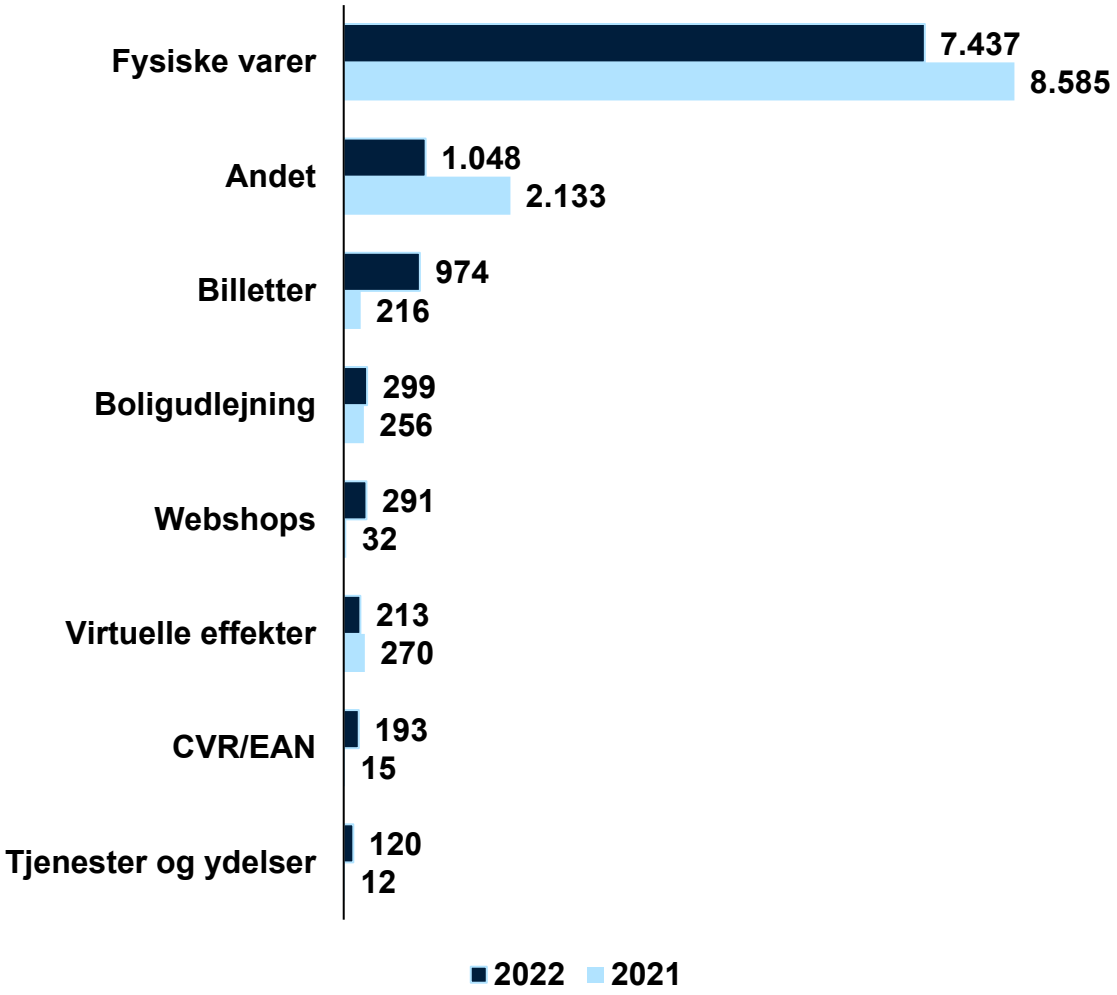
CVR og EAN
Virksomheders CVR og EAN-nummer misbruges til at indkøbe varer. En virksomhed kan fx risikere at få misbrugt sit CVR-nummer, som gerningspersonen bruger til at oprette en firmakonto til indkøb af materialer, værktøj mv.

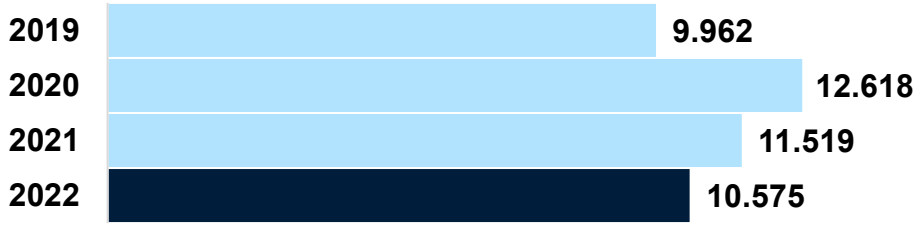
Tjenester og ydelser
I sager om svindel med tjenester og ydelser har to parter indgået en aftale om en ydelse, som forudbetales af den ene part, og som ikke leveres af den anden part. Det kan fx være forudbetaling af håndværkerarbejde, hjælp til skoleopgaver, hjælp til hjemmesider mv. eller ved køb af en seksuel ydelse.

Webshops
Samhandelsbedrageri dækker også over sager på webshops, hvor køber foretager et køb på en falsk webshop og aldrig modtager varen, da webshoppen ikke eksisterer.

Samhandel

39% af alle anmeldelser





Samhandelsbedrageri foregår på forskellige platforme

I 2022 omhandlede ca. 70 procent af alle sager om samhandel fysiske varer. 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.

Færre sager i 2022 end i 2021 og 2020

Det samlede anmeldelsestal inden for samhandel er faldet med ca. otte procent fra 2021 til 2022 og med 16 procent fra 2020 til 2022. Det høje anmeldelsestal i 2020 er formentlig et resultat af nedlukningen i forbindelse med covid-19, som generelt fik e-handlen til at vokse.

Faldet af antal anmeldelser fra 2021 til 2022 skal formentlig ses som et resultat af et fald i antallet af personer, der har handlet nye eller brugte varer af en anden privatperson via handelsplatformene. Samtidig kan genåbningen efter covid-19 formentlig være årsag til faldet, da en del af handlen er overgået til de fysiske butikker igen (Danmark Statistik, 2023:24).

Stor stigning i sager om billetter

Ca. ni procent af alle samhandelssager handlede i 2022 om billetter, hvilket er en stigning i anmeldelsestallet på ca. 350 procent i forhold til 2021. Denne stigning skal formentlig forklares med, at 2022 var det første hele år siden 2019, hvor kulturlivet ikke var påvirket af covid-19-restriktioner.

Misbrug af kortoplysninger

POLITI

Beskrivelse af misbrug af kortoplysninger

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, da det er webshoppen, der lider det økonomiske tab.

Gerningspersonerne får ofte adgang til de forurettedes betalingskort ved at fremsende en mail eller en sms, hvor der skal betales et mindre beløb i ekstra fragt for levering af en pakke. Andre gange kan forurettede modtage en falsk mail fra deres energiselskab eller Skat om, at de skal have tilbagebetalt et beløb.

I helt andre tilfælde har forurettede udleveret oplysninger til en gerningsperson via forskellige social engineering-metoder. Det kan være opkald fra personer, der udgiver sig for at være fra vedkommendes bank, Skat eller anden myndighed, eller det kan være sms'er eller e-mails, som får personen til at afgive betalingskortoplysninger.

En nyere form for misbrug af kortoplysninger består af, at gerningspersoner 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.

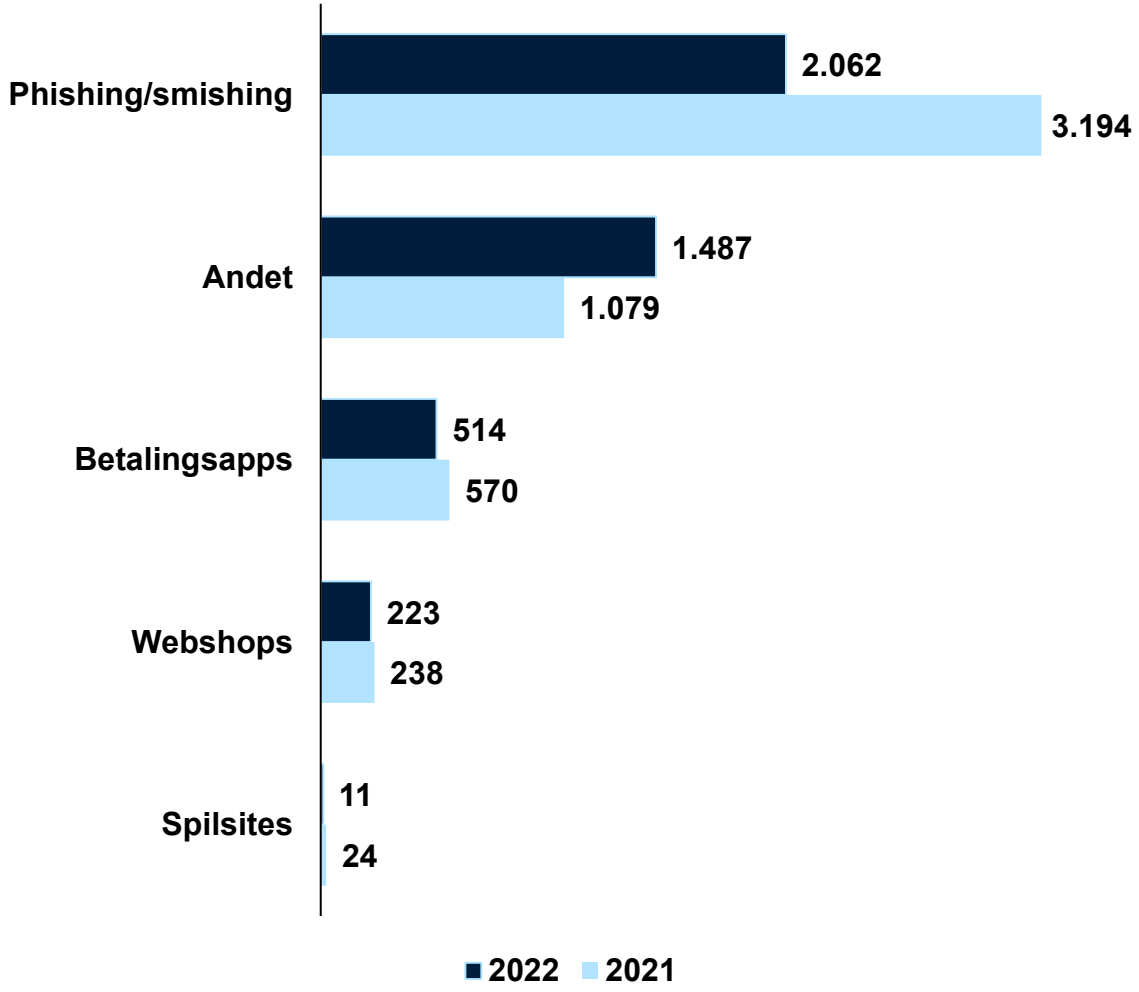
Webshops
Denne type svindel forekommer, når kortoplysninger uberettiget bliver brugt til at købe en vare eller ydelse på en webshop. Varen sendes ofte til et muldyr, til en postboks eller som elektronisk vare på e-mail.

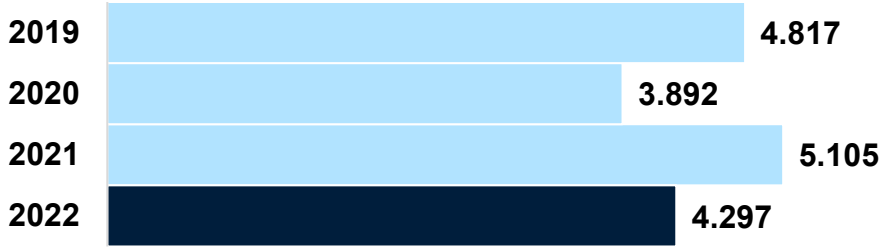
Betalingsapps
Der findes i dag flere betalingsløsninger, hvor brugere kobler deres kortoplysninger sammen med betalingsløsningen. Da man både kan foretage overførsler og køb i butikker gennem betalingstjenesterne, er de blevet et attraktivt middel for misbrug af kortoplysninger.

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.

Misbrug af kortoplysninger

15,9% af alle anmeldelser





Ikke et reelt fald i antallet af sager om misbrug af kortoplysninger

Antallet af anmeldelser registreret som misbrug af kortoplysninger er faldet med ca. 16 procent fra 2021 til 2022. Faldet skyldes, at vi pr. 1. januar 2022 har oprettet nye og mere retvisende kategorier for denne type sager. Før 1. januar 2022 blev alle sager, hvor forurettede blev franarret oplysninger, registreret som misbrug af kortoplysninger. Med den nye registreringspraksis kan vi opgøre mere præcist, om det er MitID, NemID eller andre oplysninger, der er sagens omdrejningspunkt.

Det betyder, at en del af de sager, der tidligere lå registreret under misbrug af kortoplysninger nu registreres under tværgående tema.

Betalingsapps og webshops

Misbrug af kortoplysninger er også misbrug af betalingsapps som fx MobilePay og Apple Pay. I 2022 er sager, registreret under kategorien betalingsapps, faldet med ca. 10 procent i forhold til 2021, og sager, der er registreret under webshops, er faldet med ca. seks procent i samme periode.

Om 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 den forurettede 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 offentlige 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. Gerningspersonen kan også have ændret Nemkonto, så ydelserne tilfalder en konto, som gerningspersonen har valgt.

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

Falske/stjålne personoplysninger
Denne type svindel forekommer ved, at 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, vis identitet er misbrugt.

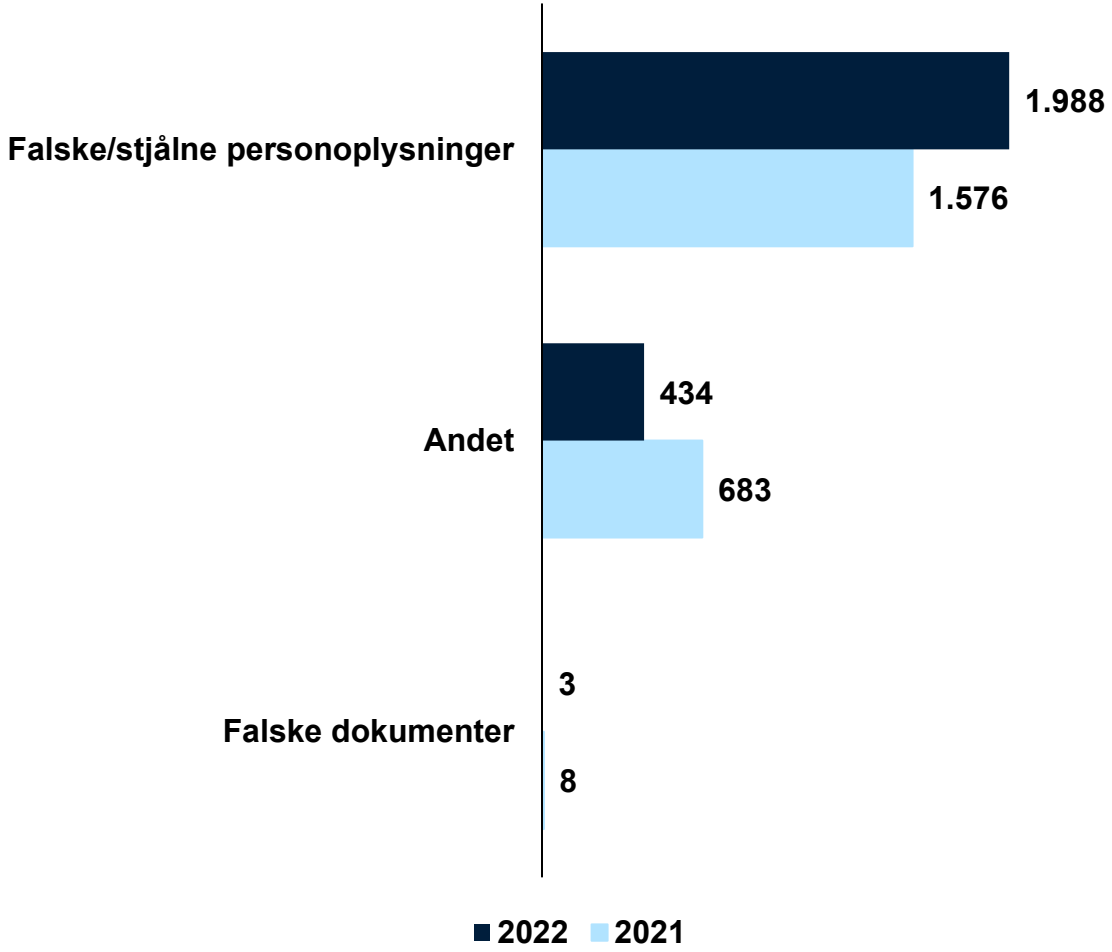
Flere virksomheder tilbyder i dag kunder at købe varer på afbetaling, hvoraf nogle virksomheder specialiserer sig i at tilbyde afbetalingsaftaler (kreditaftale) for varer købt hos andre virksomheder. Fx kan der i dag købes en ny smartphone hos virksomhed A, mens virksomhed B tilbyder at hjælpe forbrugeren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

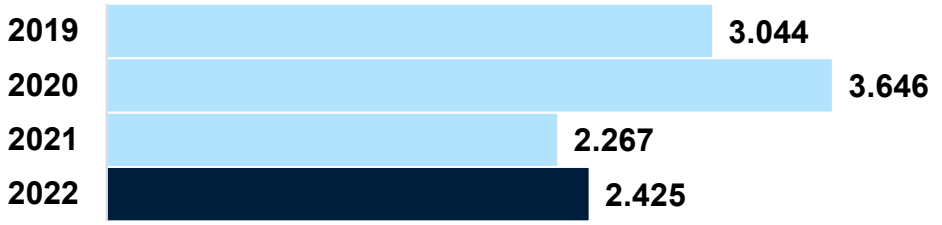
NCIK ser sager, hvor den forurettedes identitet bliver misbrugt til at bestille varer hos udenlandske virksomheder, som skal leveres i pakkeshops.

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

Kreditbedrageri

9% af alle anmeldelser





Antallet af anmeldeler om kreditbedrageri

Fra 2021 til 2022 var der en stigning på ca. syv procent i antallet af anmeldelser om kreditbedrageri. Dog er anmeldelsestallet i både 2021 og 2022 faldet markant, når der sammenlignes med 2019 og 2020.

Der oprustes løbende med sikkerhedsforanstaltninger i sektoren, og det er formentlig med til at forklare udviklingen i faldet af anmeldelser. Dog ser NCIK også, at kriminelle løbende forsøger at omgå to-faktorverifikation ved at misbruge identitetsoplysninger, som er franarret forurettede via telefon, e-mail eller sms.

Kreditbedrageri med falsk eller stjålen identitet

I de fleste anmeldelser om kreditbedrageri fra 2022 er der tale om en gerningsperson, der enten benytter falske eller stjålne identiteter til at optage kredit i en anden persons navn.

Om kategorien Andet

Denne kategori dækker over sager, der endnu ikke har fået en kategorisering.

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 forurettede med henblik på at begå bedrageri og franarre vedkommende penge eller andre 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, på sociale medier via chattjenester 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.

Låne/investeringssvindel
De forurettede reagerer ofte på annoncer på legitime websites (nyhedsmedier, sociale medier mv.) og på fuphjemmesider, der til forveksling ligner legitime, danske nyhedsmedier. Nogle forurettede lider mindre tab i et forsøg på at opnå private lån på sociale medier, mens andre lider væsentligt større tab som følge af annonceindhold, hvor der på forskellige måder er blevet fortalt om lukrative investeringsmuligheder – ofte ved investering i kryptovaluta.

Store pengebeløb i udlandet
Denne type svindel handler om, at forurettede typisk via e-mail bliver kontaktet af en person i udlandet, der tilbyder adgang til et større pengeløb (såkaldt ”Nigeriabrev”). Det drejer 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.

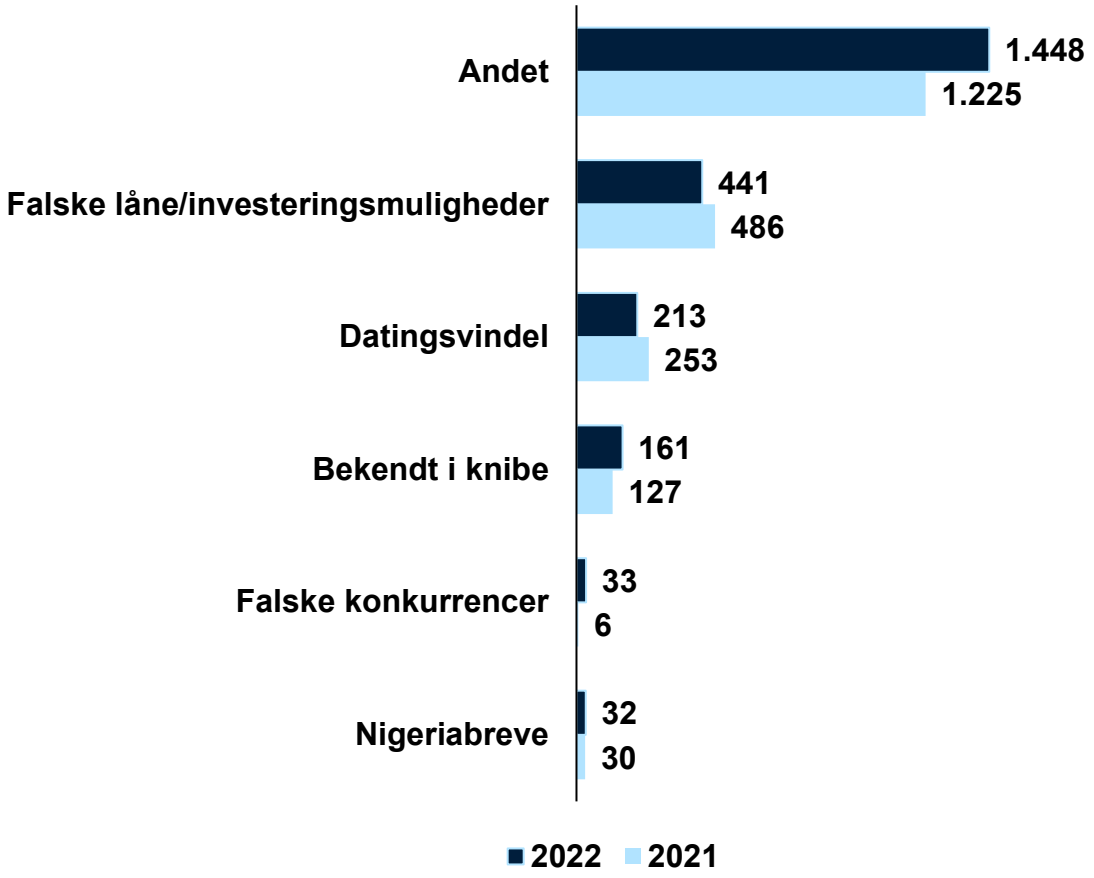
Bekendt i knibe
Denne type svindel sker ofte ved, at forurettede bliver kontaktet via e-mail, sms eller chat af en person, der udgiver sig for at være en bekendt eller nær relation. Historien udspiller sig typisk således, at der er opstået en nødsituation i udlandet, og den forurettede bliver derfor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

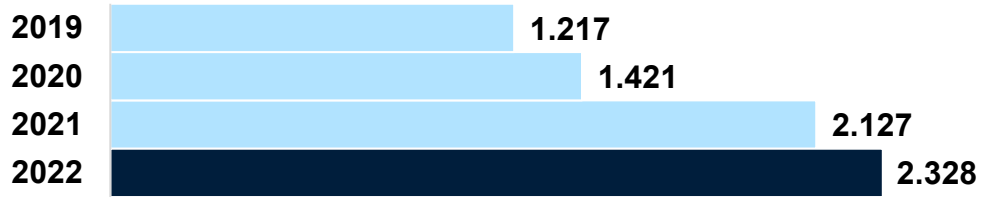
Datingsvindel
Datingsvindel tager udgangspunkt i, at en person etablerer en relation til en med falsk identitet via sociale medier. Gerningspersonen med den falske identitet udnytter forurettedes følelsesmæssige involvering og lokker penge ud af vedkommende ved kontooverførsler. Datingsvindel er karakteriseret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

Falske konkurrencer
I denne type sager er forurettede blevet lokket til at betale for at være med i en konkurrence, men konkurrencen er fiktiv, og der er ikke nogle reelle vinderchancer. Forurettede kan være blevet eksponeret for konkurrencen på sociale medier.

Kontaktbedrageri mod private

8,6% af alle anmeldelser





Flere anmeldelser om kontaktbedragerier mod private

Fra 2021 til 2022 steg anmeldelsestallet for kontaktbedrageri mod private med ca. ni procent. Den overordnede stigning i antallet af kontaktbedragerier er særligt båret af, at NCIK siden 1. januar 2022 har kategoriseret investeringssvindel under kontaktbedrageri mod private. Anmeldelser i kategorien investeringssvindel udgør ca. 19 procent af alle anmeldelser om kontaktbedrageri mod private i 2022.

Stor andel af sager i kategorien Andet

I 2022 var der 1.448 anmeldelser registreret under Andet, og ca. 750 af disse omhandler vishing, herunder telefonsvindel mod ældre borgere. I 2021 var tallet ca. 200. Det er eksempelvis sager, hvor gerningspersonen kontakter forurettede telefonisk og udgiver sig for at være fra bank eller politi, og dermed 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 sager om bekendt i knibe er steget lidt i 2022. Disse sager handler ofte om, at en person tager kontakt til forurettede via sociale medier og udgiver sig for at være et familiemedlem eller anden nær relation med det formål at lokke forurettede til at overføre penge til gerningspersonen.

Misbrug af adgang til tjenester

POLITI

Beskrivelse af misbrug af adgang til tjenester

Om misbrug af adgang til tjenester

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.

Netbank
Indbrud i netbank bliver ofte begået efter forudgående kontakt, hvor gerningspersonen typisk ringer til en borger og udgiver sig for at være fra en bank, en offentlig myndighed eller lignende. Gerningspersonen fortæller, at der er ved at blive gennemført en uretmæssig transaktion, og på den måde bliver forurettede overtalt til at udlevere personoplysninger, NemID/MitID og eventuelle sms-verificeringskoder. Oplysningerne bliver ofte misbrugt allerede under samtalen. Kriminalitetsformen omfatter ofte et større netværk af muldyr, der hvidvasker de penge, som er blevet overført fra den forurettedes konti. I mange tilfælde laver gerningspersonerne flere overførsler svarende til det beløb, mange bankkunder dagligt kan hæve i pengeautomater. Der er forskel på, hvor store økonomiske tab, de forurettede lider, men der kan være tale om særdeles høje beløb.

Spil og webshops
Gerningspersonen skaffer sig adgang til eksisterende brugerkonti på spilplatforme, streamingtjenester og lignende, hvorefter vedkommende foretager køb og/eller overfører virtuelle effekter såsom skins, skjolde, våben mv. videre til andre konti. NCIK ser også anmeldelser, hvor gerningspersonen køber film, streamer sportsevents mv., hvor forurettede lider økonomisk tab svarende til værdien af det købte.

Betalingstjenester
Bonuskortordninger og andre former for konti med opsparede bonuspoint, fx hos flyselskaber, er ofte i gerningspersoners interesse. Gerningspersonerne skaffer sig adgang til kontoen, og bruger pointene til at købe varer, rejser og tjenesteydelser.

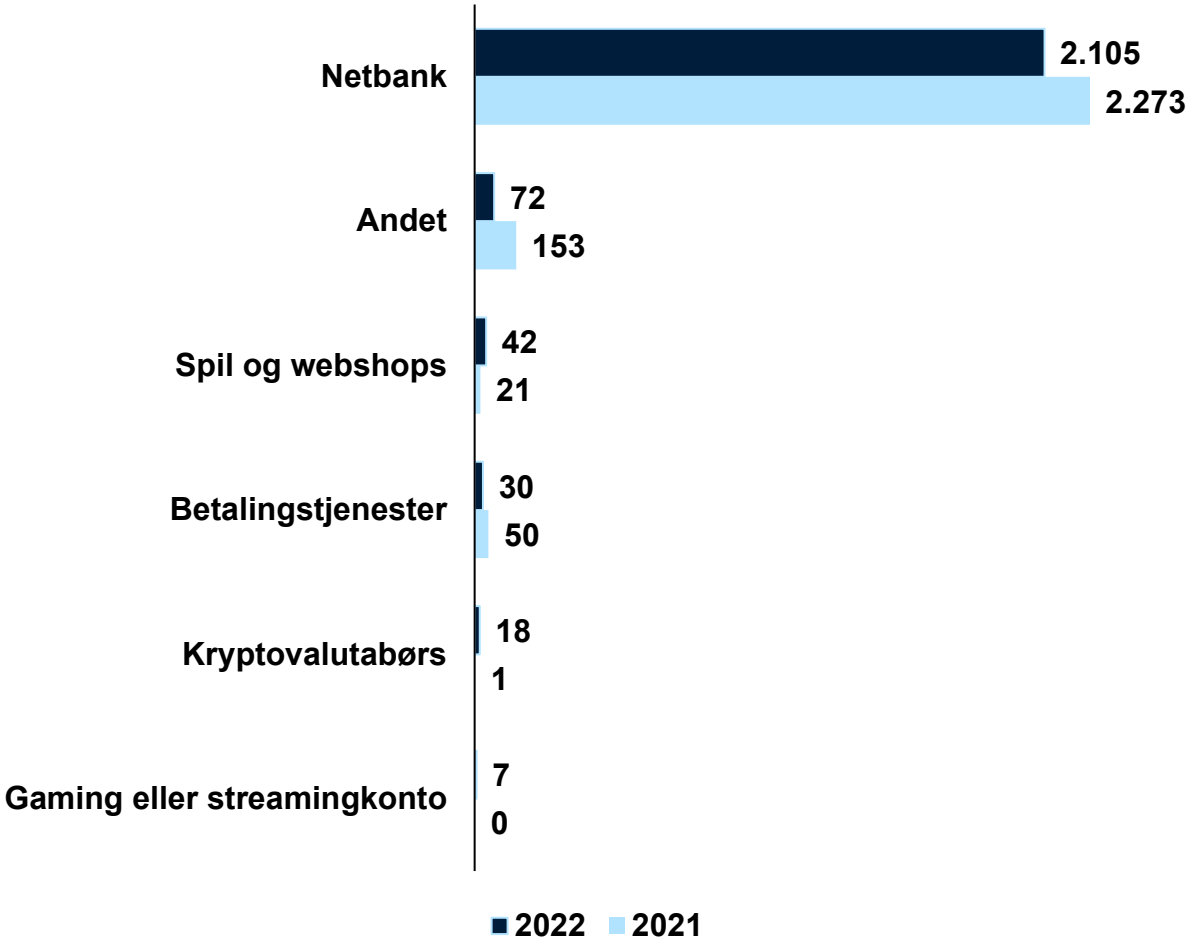
Gaming eller streamingkonto
I sager, hvor forurettede har fået misbrugt sin gaming eller streamingkonto, bliver der hævet penge, overført penge eller oprettet abonnementer på forurettedes streamingkonto eller stjålet virtuelle effekter.

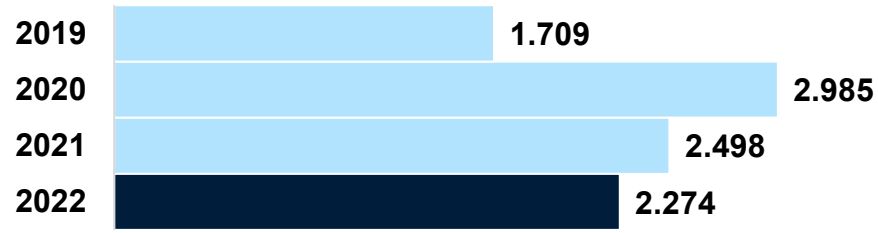
Kryptovalutabørs
Der bliver hævet eller overført penge via forurettedes kryptovalutabørs, som forurettede har i forvejen eller får oprettet i sit navn. Herefter investerer gerningspersonen forurettedes penge i kryptovaluta.

Keylogger og andet spyware
I denne type sag får forurettede stjålet sin kode til en betalingstjeneste via udstyr, som er installeret på en offentlig maskine/computer af en gerningsperson. Det kan fx være en betalingsautomat i en butik eller en computer på et bibliotek.

Misbrug af adgang til tjenester

8,4% af alle anmeldelser





Fald i antallet af sager om misbrug af adgang til netbank

Antallet af anmeldelser om misbrug af adgang til netbank i 2022 er faldet med ca. syv procent i forhold til 2021.

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.

Stigning i antallet af sager om misbrug af adgang til tjenester siden 2019

Selvom der er sket et lille fald i anmeldelsestallet fra 2021 til 2022, er det et område, der fortsat er i vækst, når der sammenlignes med sagstallet fra 2019, hvorfra der er en stigning på 33 procent frem til 2022.

Stigning i sager om spil og webshops

Antallet af sager om spil og webshops steg fra 2021 til 2022 med 100 procent.

Misbrug af adgang til tjenester dækker også over sager, hvor forurettedes konti på hjemmesider, hvor de har tilknyttet et betalingskort for hurtig betaling, bliver misbrugt. Det dækker også over sager, hvor forurettedes Steamkonto bliver misbrugt.

Afpresning

POLITI

Beskrivelse af afpresning

Om afpresning

Afpresningssager inden for it-relateret økonomisk kriminalitet dækker blandt andet over sager, hvor e-mails med trusler af forskelligartet karakter bliver sendt til forurettede. Teksten er ofte på engelsk, men forekommer også på gebrokkent 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.

NCIK modtager et stort antal anmeldelser om afpresning, hvor afsenderen tilkendegiver at have tilegnet sig adgang til 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.

I 2022 så NCIK en ny variant af masseafpresning, hvor gerningspersoner foregav at være fra dansk eller udenlandsk politimyndighed. I disse sager forsøgte gerningspersonerne at få forurettede til at reagere på en e-mail, der angav at have oplysninger om, at forurettede var under mistanke for seksualforbrydelser.

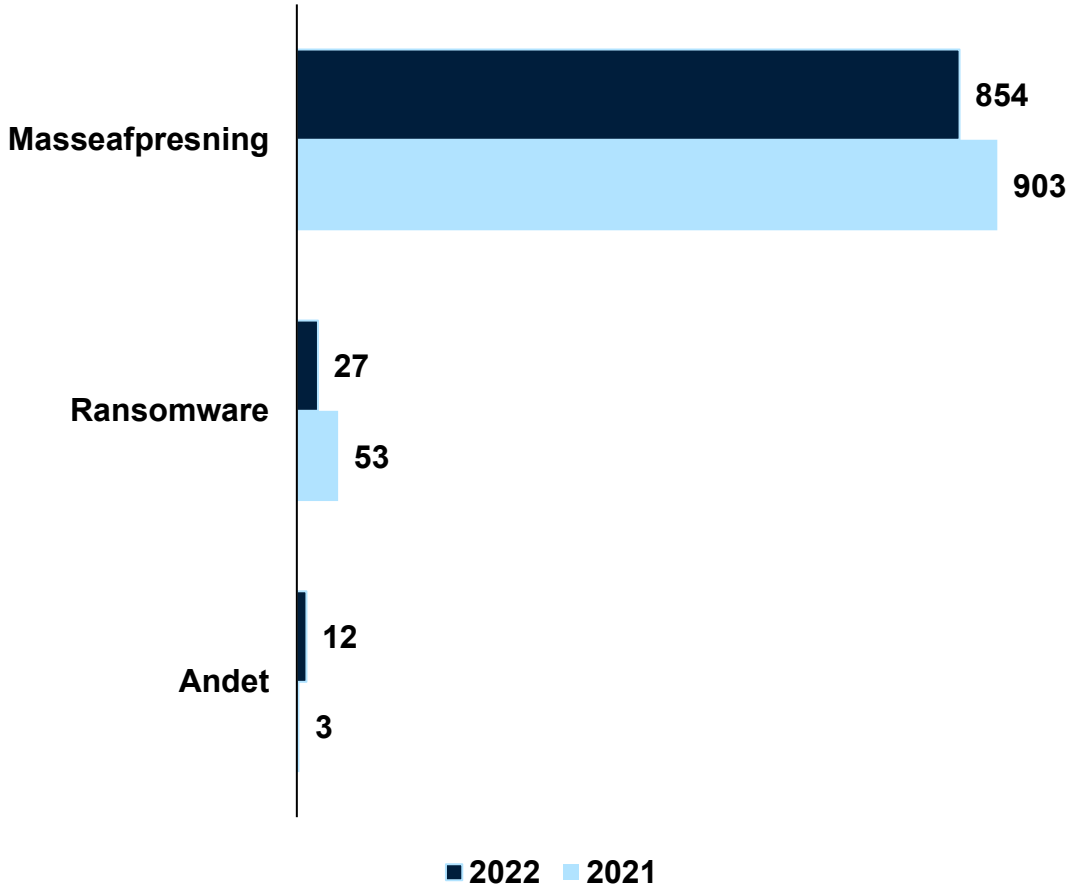
En anden form for afpresning foregår ved ransomware. Ransomware (afpresningssoftware) er betegnelsen for en type malware (skadelig software), som begrænser eller fuldstændig blokerer adgangen til den computer, server eller it-infrastruktur, der inficeres. Formålet er at få forurettede til at betale en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

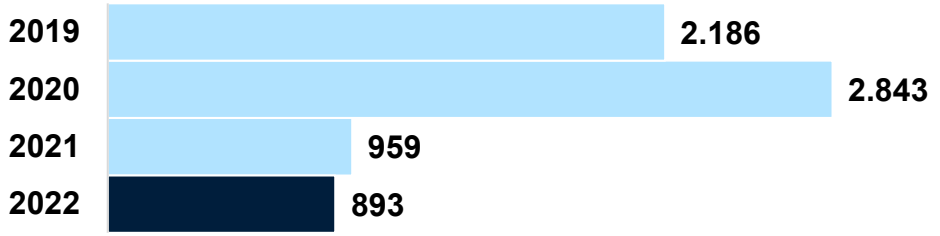
Masseafpresning
I masseafpresningssager sender gerningspersoner afpresningsmails til mange tilfældige personer i håb om, at nogle reagerer og betaler en løsesum. E-mailen bærer præg af at være sendt til mange vilkårlige modtagere på én gang. Masseafpresningsmails bliver sendt i bølger, så typisk modtager NCIK også anmeldelserne i bølger.

Ransomware
Ransomware rammer både borgere og virksomheder, men der er en overvægt af anmeldelser fra virksomheder. 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.

Afpresning

3,3% af alle anmeldelser





Stort fald i antallet af sager om afpresning siden 2020

I 2022 modtog NCIK 893 anmeldelser om afpresning, hvilket er et lille fald fra 2021. NCIK ser dog et markant fald i antallet af sager om afpresning sammenlignet med 2019 og 2020.

Fra 2020 til 2022 ses et fald på ca. 69 procent i antallet af sager om afpresning. Faldet kan bero på, at borgerne er blevet bedre til at spotte denne type svindel og i takt med dette også har fået bedre spamfiltre, der begrænser mængden af uønskede mails og spam.

Masseafpresning driver udviklingen inden for 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. Et eksempel på dette er de såkaldte Europol-mails, hvor der i mailen fremgår trusler om offentliggørelse af intime billeder, og hvor afsenderen i højere eller lavere grad ligner enten danske eller udenlandske politimyndigheder.

Få anmeldelser om afpresning med ransomware

I 2022 modtog NCIK relativt få anmeldelser om afpresning med ransomware. Dog vurderer Center for Cybersikkerhed i 2023, at truslen på området er høj, og at organiserede ransomwaregrupper fortsat retter angreb mod alle dele af samfundet (CFCS, 2023:4).

Kontaktbedrageri mod virksomheder

POLITI

Beskrivelse af kontaktbedragerier mod virksomheder

Om kontaktbedrageri mod virksomheder

Kontaktbedragerier mod virksomheder, myndigheder, foreninger eller andre organisationer sker ofte i form af CEO/BEC fraud.

CEO fraud kaldes i Danmark også for direktørsvindel. Ved CEO fraud anvender gerningspersoner 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.

BEC er en forkortelse for den engelske term Business E-mail Compromise, og er i udgangspunktet en mere avanceret form for CEO fraud. BEC fraud sker typisk ved, at en gerningsperson kompromitterer adgangen til en eller flere e-mailkonti, hvis adgang herefter benyttes til at sende nye betalingsoplysninger til forurettede. Ofte ser NCIK anvendelse af typosquatting, hvor gerningspersonen sørger for at registrere et e-maildomæne, 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.

CEO fraud

I 2022 var der flere sager, hvor en virksomhed eller forening modtog e-mails, der udgav sig for at være direktøren eller chefen for selvsamme virksomhed. Af de fremsendte e-mails fremgik det, at der hurtigst muligt skulle overføres større eller mindre beløb til en udenlandsk konto eller indkøbes forskellige former for forudbetalt kredit. Før selve betalingsanmodningen spurgte gerningspersonen i flere tilfælde, hvor mange penge, der var til rådighed på virksomhedens konto.

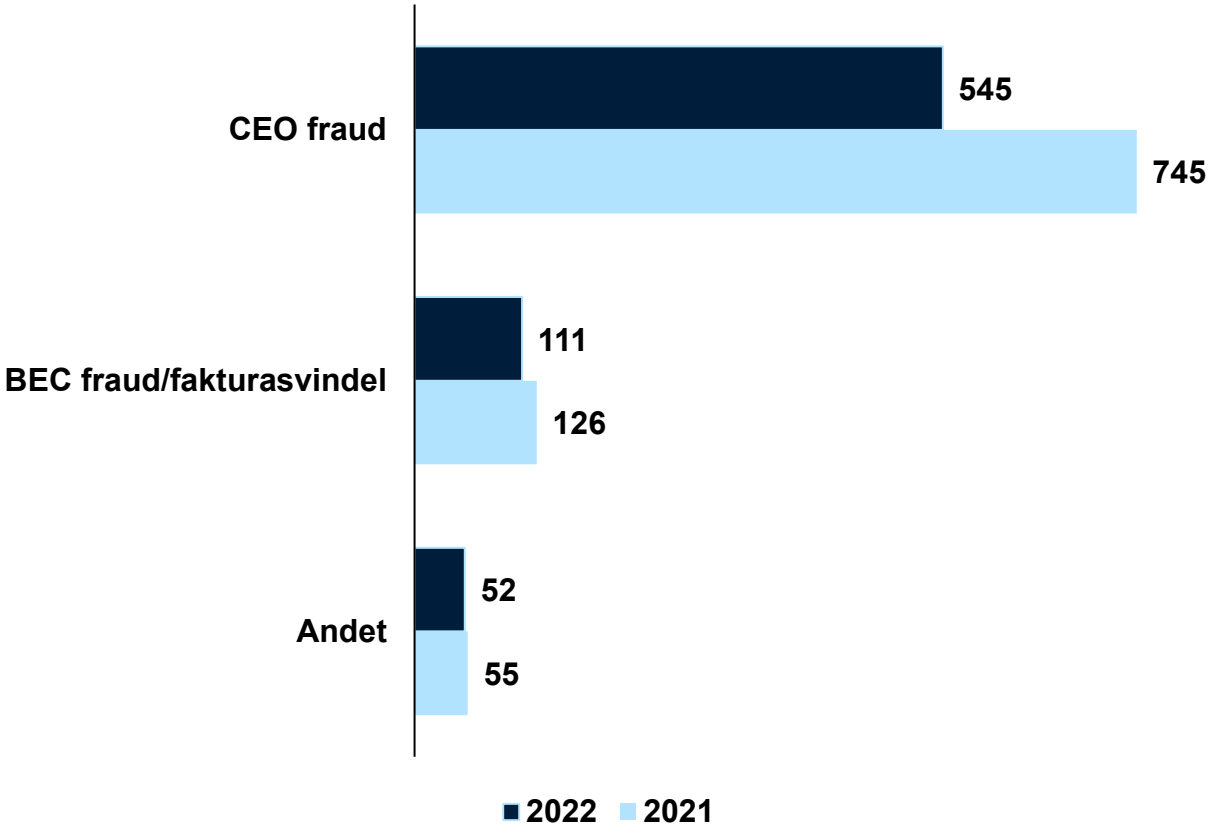
BEC/fakturasvindel

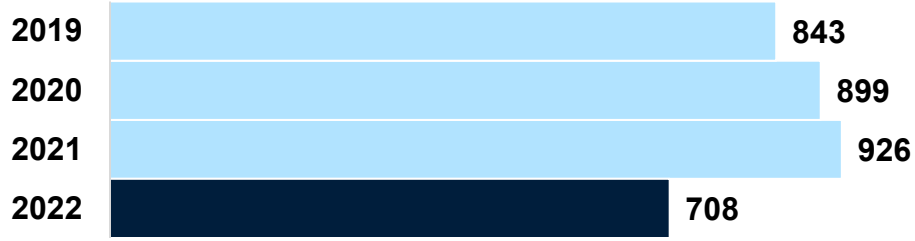
BEC/fakturasvindel minder på mange måder om CEO fraud, idet gerningspersonen prøver at vildlede den økonomiansvarlige i en organisation til at betale en falsk faktura. Det sker typisk ved, at firmaet modtager en faktura fra gerningspersonen på e-mail, hvor modtagerkontoen er kontrolleret af gerningspersonen. BEC fraud sker typisk ved, at en gerningsperson skaffer sig adgang til en e-mailkonto og derefter giver falske instruktioner om kommende betalinger for reelle ydelser eller varer.

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.

Kontaktbedrageri mod virksomheder

2,6% af alle anmeldelser





Færre anmeldelser om kontaktbedrageri mod virksomheder
I 2022 blev der anmeldt ca. 24 procent færre sager om kontaktbedrageri mod virksomheder i forhold til 2021. Ca. 77 procent af anmeldelserne om kontaktbedrageri mod virksomheder var i form af CEO fraud. Kontaktbedrageri mod virksomheder dækker også over foreninger og myndigheder.

CEO fraud fylder mest

De fleste anmeldelser i kategorien kontaktbedrageri mod virksomheder handler om CEO fraud. Fra 2021 til 2022 har vi dog set et fald i antal anmeldelser på ca. 27 procent, mens antallet af anmeldelser om BEC fraud/fakturasvindel er faldet med ca. 12 procent fra 2021 til 2022.

I 2022 var der 545 anmeldelser om CEO fraud og 111 anmeldelser om BEC fraud/fakturasvindel. Hertil kommer 52 sager, der endnu ikke er kategoriseret.

Forurettede i sager om it-relateret økonomisk kriminalitet

POLITI

Antal forurettede udsat for it-relateret økonomisk kriminalitet i 2022

24.343 forskellige personer

har været udsat for it-relateret økonomisk kriminalitet

1.056 forskellige professionelle

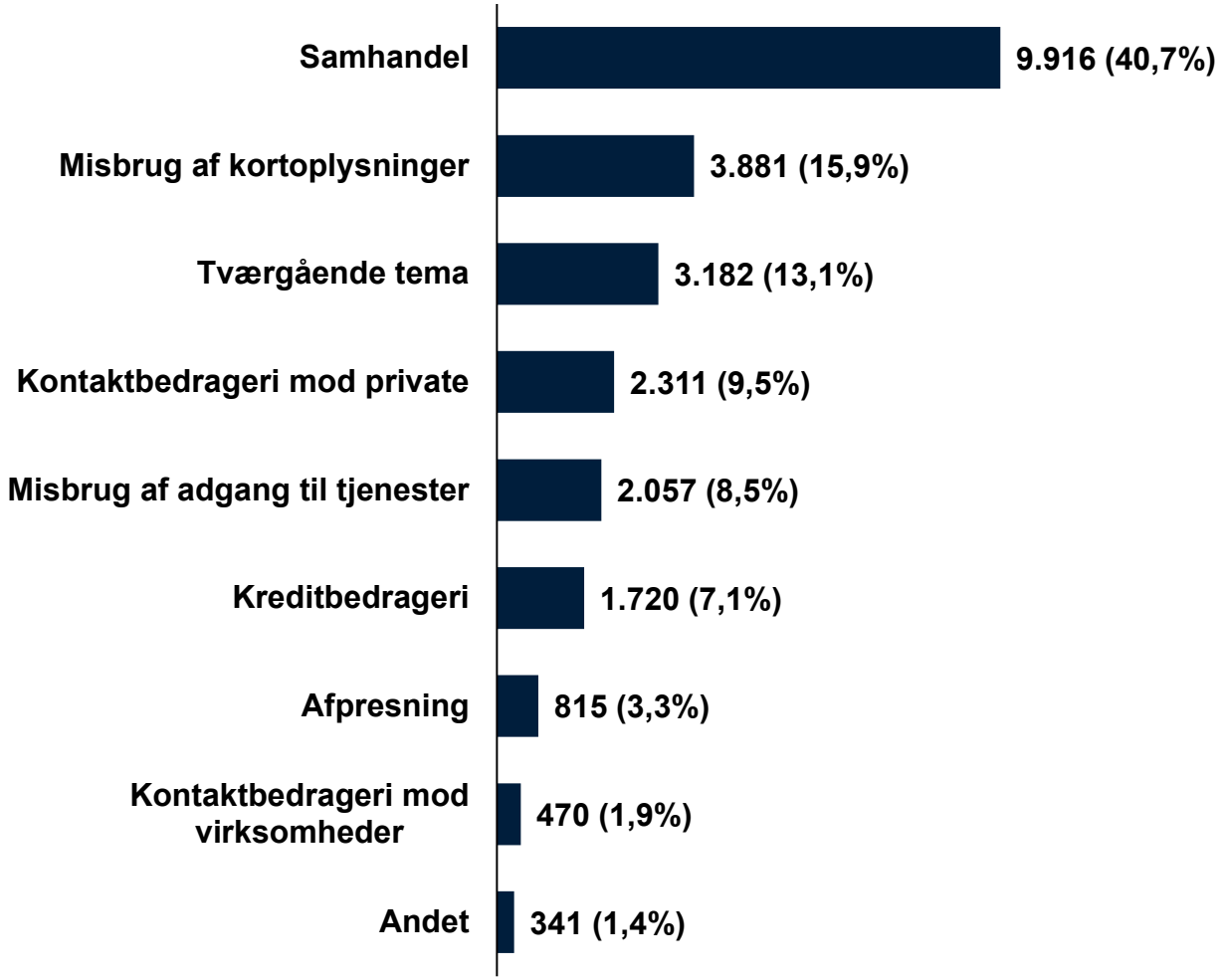
har været udsat for it-relateret økonomisk kriminalitet

Om de forurettede

Denne del af rapporten tager udgangspunkt i de personer og virksomheder, som har været ofre for it-relateret økonomisk kriminalitet i 2022. 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: (24.343) Antal unikke private forurettede inden for hvert sagsområde i 2022.

Antallet af unikke forurettede per sagsområde

Diagrammet 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. Lidt over 40 procent af de personer, der anmeldte til NCIK i 2022, var udsat for samhandelsbedrageri og knap 16 procent for misbrug af kortoplysninger.

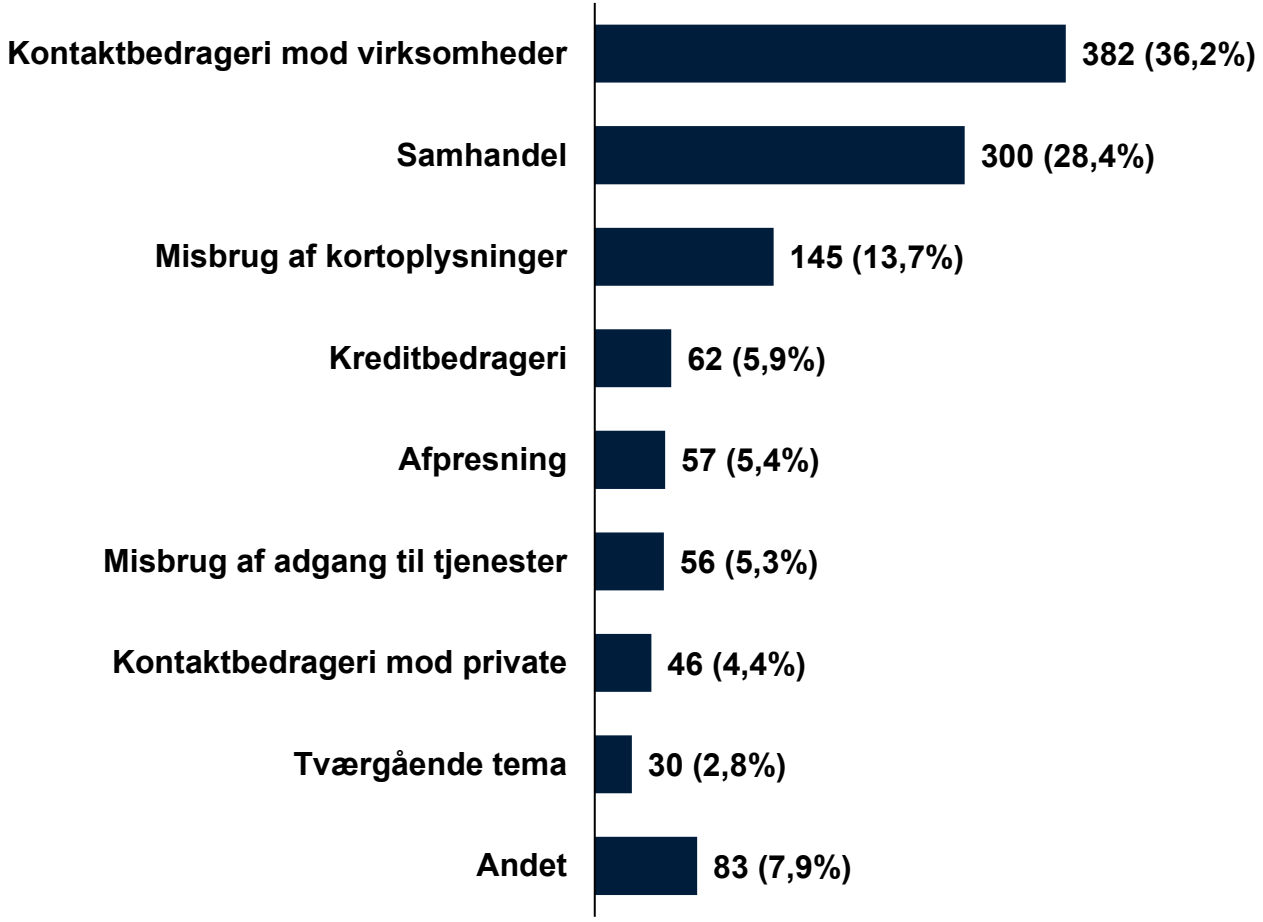
Ca. 57 procent af privatpersonerne har tilsammen anmeldt sager vedrørende de to hyppigste anmeldelseskategorier.

Der kan være stor forskel på det tab, forurettede har. Misbrug af identitet og efterfølgende lånoptagelse kan eksempelvis løbe op i 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.

65 procent af de professionelle forurettede i 2022 blev udsat for kontaktbedrageri eller samhandel



Fordeling af professionelle forurettede på NCIKs sagsområder

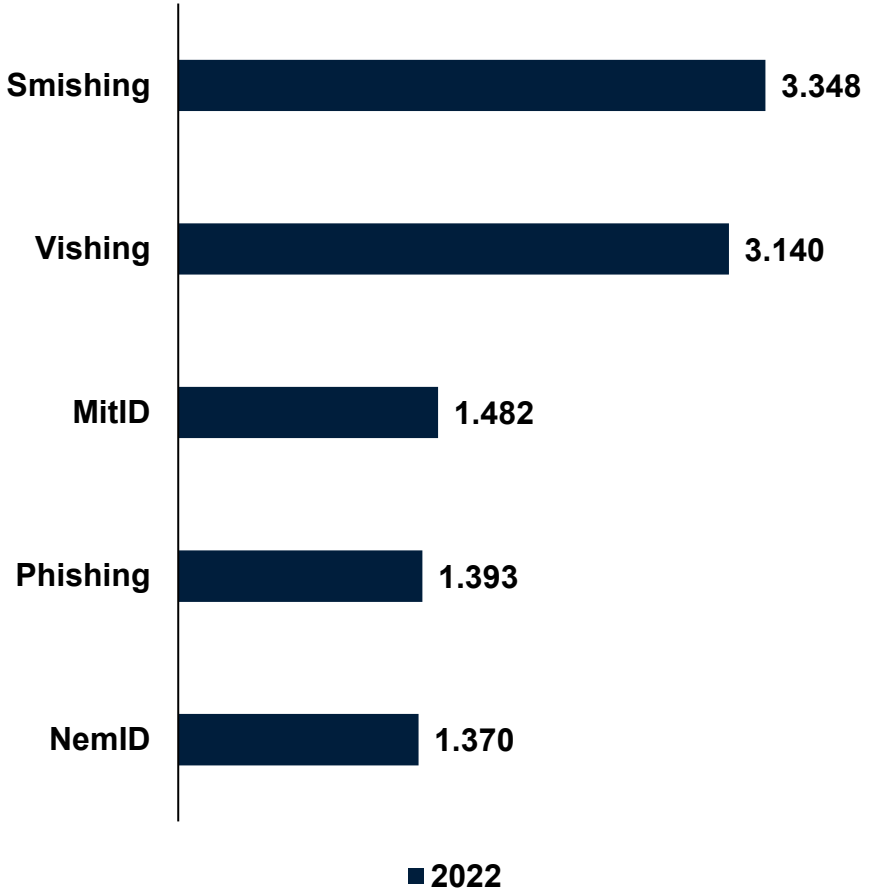
I diagrammet er NCIKs sagsområder opgjort på baggrund af antallet af unikke professionelle forurettede. Denne gruppe består af de virksomheder, myndigheder, foreninger mv., der blev udsat for it-relateret økonomisk kriminalitet anmeldt i 2022.

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/MitID i oprettelsen, vil anmeldelsen tælle som en privat anmeldelse. En virksomhed kan tælle én gang for hvert sagsområde.

Base: (1.056) Antal unikke professionelle forurettede inden for hvert sagsområde i 2022.

Sager på tværs af kriminalitetsområder



Ny registreringsmetode
Som noget nyt er anmeldelserne fra 2022 ikke kun registreret på kriminalitetsområder. En del af anmeldelserne har temaer, der går på tværs af de forskellige kriminalitetsområder. Diagrammet viser, hvor mange anmeldelser, der indeholder elementer af hvert tema. Temaet beskriver oftest et modus, der kan bruges som kategori på de fleste af NCIKs sagsområder.

29 procent af alle anmeldelser i 2022 indeholder et eller flere temaer
Hvis en anmeldelse har flere temaer indgår den i opgørelsen under alle de temaer, den har. Anmeldelser, der indeholder flere temaer kan fx være sager, hvor gerningspersonen har benyttet sig af både smishing og vishing til at få adgang til forurettedes MitID.

Stigning i vishing og smishing
Da denne opgørelsesmetode blev indført i januar 2022, kan der ikke laves en direkte sammenligning med de tidligere år. Det er dog ikke nyt, at gerningspersoner benytter sig af smishing, vishing og phishing. Det vurderes, at en del af stigningen i antallet af anmeldelser fra 2021 til 2022 skyldes en stigning i anmeldelser, hvor der benyttes vishing og smishing som modus.

Gerningspersoner benytter ofte disse fremgangsmåder i forbindelse med misbrug af kortoplysninger, misbrug af adgang til tjenester eller kontaktbedrageri mod private. Derfor optræder en del af anmeldelserne i denne opgørelse også i opgørelserne af kriminalitetsområderne.

Base: (7.885) 5.536 af anmeldelserne indeholder ét af de tværgående temaer. 1896 anmeldelser indeholder to tværgående temaer, 408 anmeldelser indeholder tre tværgående temaer, 44 anmeldelser indeholder fire tværgående temaer, mens én anmeldelse indeholder alle fem tværgående temaer.

Opmærksomhedspunkter

POLITI

Muldyr 1/2

En forudsætning for it-relateret økonomisk kriminalitet

Et muldyr er en person, der stiller sin konto til rådighed for kriminelle, som dermed kan sløre de finansielle spor fra en kriminel handling. Nogle muldyr får betaling for at fungere som mellemled, mens andre måske ikke er klar over, at de medvirker til hvidvask. Betegnelsen muldyr benyttes både når muldyret bevidst, ubevidst eller under pres foretager hvidvask.

Muldyrene gør det muligt at flytte penge fra økonomisk kriminalitet uden at efterlade digitale spor, der peger tilbage på den kriminelle bagmand. De er derfor et nødvendigt led i at få vasket pengene rene. Muldyret medvirker til hvidvask fx ved at få overført et beløb direkte fra forurettedes konto og derefter videreføre det til en anden muldyrkonto, eller ved at hæve og overdrage beløbet til bagmanden i kontanter. Muldyret kan også deltage ved at udlåne sin identitet, spilkonto eller kontokort til en kriminel transaktion.

Udfordrede efterforskninger

Der er visse udfordringer forbundet med at efterforske hvidvasksager, hvor der indgår muldyr, fordi muldyrkonstruktioner vanskeliggør mulighederne for at identificere den egentlige bagmand i sagerne. Pengesporet sløres hurtigt, og pengene videreføres ofte helt eller delvist til andre konti og i nogle tilfælde til muldyr i andet og tredje led. I andre tilfælde bliver der foretaget kontanthævninger, hvorefter pengene overdrages til bagmanden eller medgerningspersoner til førforbrydelsen.

Forebyggelse vigtigt

Muldyrsaktivitet er et omfattende problem, og i takt med, at it-relateret økonomisk kriminalitet bliver ved med at stige, sker det samme med muldyr, fordi brugen af muldyr er en forudsætning for dette kriminalitetsområde. Derfor er det vigtigt med forebyggelse, så man undgår, at særligt unge ikke medvirker til denne type kriminalitet. Mange unge ved nemlig ikke, at det er ulovligt at stille sin konto til rådighed for kriminelle. Ifølge en undersøgelse fra Finans Danmark har mange unge ikke kendskab til, hvad det vil sige at være muldyr. I en spørgeundersøgelse svarede 48 procent af de adspurgte unge mellem 18 og 30 år, at de ikke kendte til begrebet (Finans Danmark, 2021:66).

Muldyr 2/2

Landsdækkende aktion målrettet muldyr

Den 5. januar 2023 iværksatte NSK en omfattende, landsdækkende aktion og anholdt 140 personer på tværs af alle landets politikredse. 600 politifolk deltog i aktionen, der er den største nogensinde i dansk politi. Aktionen blev sat i værk med det formål at komme en del af muldyraktiviteterne til livs, fordi de er et vigtigt og nødvendigt led for de organiserede kriminelle, når de skal hvidvaske de penge, de har svindlet sig til. Med aktionen har dansk politi forsøgt at sætte en stopper for det, og forhåbentlig også afholdt andre fra at fungere som muldyr. Nogle af de anholdte blev fremstillet i grundlovsforhør og varetægtsfængslet, mens de fleste blev sigtet, afhørt og efterfølgende løsladt. Hovedparten af sagerne afventer afgørelse ved domstolene, og der arbejdes stadig på at identificere bagmænd i sagerne.

Stammer fra kontaktbedragerier

De hvidvaskede penge i aktionen stammer fra kontaktbedragerier, hvor især ældre borgere er blevet kontaktet af gerningsmænd, der udgiver sig for at komme fra fx Nets, banken eller politiet for at franarre ofrene personoplysninger eller penge. Herefter har gerningsmændene ofte tømt forurettedes konto under påskud af, at ville beskytte kontoen mod hackerangreb. I nogle tilfælde er de forurettede blevet manipuleret til at selv at overføre pengene.

Paragrafferne

Straffelovens § 290 og 290a: Hæleri og hvidvask kan straffes med bøde eller fængsel op til 1 år og 6 måneder. Derudover risikerer man at få en plet på straffeattesten, hvilket kan have jobmæssige konsekvenser langt ud i fremtiden.

Telefonsvindel

Manipulation af forurettede
Telefonsvindel er en form for kontaktbedrageri, hvor gerningspersoner ringer til mere eller mindre tilfældigt udvalgte personer med henblik på at få dem til at udlevere fortrolig data eller overføre større pengebeløb. I en række tilfælde har gerningspersonerne ved hjælp af social engineering-metoder manipuleret forurettede til at overføre store pengebeløb under påskud af, at de ringer fra enten forurettedes bank, anden myndighed eller politiet. Svindlen målrettes ofte ældre borgere ved hjælp af søgninger i online telefonbøger. Telefonsvindel handler i høj grad om, at kriminelle bruger mange forskellige overtalelsesmetoder til at omgå de sikkerhedsforanstaltninger, man i stigende grad implementerer på nettet.

Stigning i antal sager i 2022
I 2022 er mange borgere blevet svindlet eller forsøgt svindlet for næsten 100 mio. kroner ved kontaktbedrageri over telefonen. At være forurettet i disse sager kan være omkostningstungt – både økonomisk, men også på det menneskelige plan. Ofte har forurettede en følelse af selvbebrejdelse, fordi de mener, at de burde have gennemskuet manipulationen, og at de er blevet narret af en svindler. I den forbindelse er det vigtigt at tilføje, at gerningspersonerne i disse sager kan være organiserede kriminelle.

Forebyggelse og adfærdsændring er vigtigt
Forebyggelsen af denne type social engineering, hvor gerningspersonen manipulerer forurettede, besværliggøres af, at vi som mennesker er prædisponerede til at antage, at de parter, vi kommunikerer med, fortæller sandheden (Journal of Language and Social Psychology, 2014:10). Det er derfor ikke tilfældigt, at det ofte er banker, politi eller andre myndigheder, som gerningspersoner i disse sager udgiver sig for. Det er typisk institutioner, som befolkningen anser for at have en høj troværdighed.

Forebyggelse i disse tilfælde handler derfor ikke blot om oplysning, men om at ændre adfærd hos befolkningen. Det handler også om at klæde særligt udsatte dele af befolkningen bedre på til at beskytte sig selv digitalt. Det gælder om at ruste dem til at søge og forstå viden om de tekniske foranstaltninger, man kan implementere for at forebygge, at gerningspersoner kan opnå kontakt og få held med at manipulere forurettede.

Kunstig intelligens, store sprogmodeller og deep fakes

Hvad er kunstig intelligens?

Kunstig intelligens såsom talegenkendelse, maskinoversættelse og chatbots har længe været bredt funderet i samfundet, men for nylig har udbredelsen af store sprogmodeller såsom ChatGPT og andre kunstig intelligensmodeller, der fx kan skabe falske billeder og videoer (deep fakes), for alvor slået igennem i hele verden.

Fremtidens it-kriminalitet

NCIK har endnu ikke modtaget anmeldelser, hvor kunstig intelligens er identificeret som modus, men i andre lande har man allerede set de første sager, hvor kunstig intelligens i form af sprogmodeller eller deep fakes bliver brugt til at svindle folk. Det handler i særlig grad om kontaktbedrageri, hvor kriminelle har brugt kunstig intelligens til at efterligne pårørendes stemmer, så forurettede har overført penge direkte til gerningspersonen i den tro, at deres familiemedlem har været i knibe. Dette modus er også set i sager om CEO-fraud, hvor gerningspersoner har kontakt til medarbejdere i en virksomhed, der har overført store pengesummer til gerningspersonerne i den tro, at de har talt med direktøren for virksomheden. I virkeligheden er direktørens stemme blevet gengivet ved hjælp af kunstig intelligens.

Helt nye krav til modstandskraften

Kunstig intelligens stiller nye krav til forebyggelsen af it-relateret økonomisk kriminalitet. Hvor man tidligere har kunne identificere phishingforsøg ved, at ordlyden og sproget oftest har båret præg af at være ubehjælpeligt oversat, kan sprogmodeller i dag og i fremtiden kvalificere sproget i en sådan grad, at det ikke længere vil være til at gennemskue. Sprogmodeller kan desuden tage højde for den typiske sprogbrug fra fx en organisation eller virksomhed og dermed i højere grad fremstå troværdig. Derudover kan sprogmodeller også masseproducere phishingmails i langt højere grad, end vi ser allerede i dag. Denne udvikling stiller større krav til befolkningen og deres evner til at gennemskue it-kriminalitet. Det bliver i højere og højere grad nødvendigt for befolkningen at udvikle evner til at kunne genkende videoer, lyd og billeder genereret ved hjælp af kunstig intelligens, spotte kontekster og finde strukturelle sprogfejl, der kan bære præg af kunstig intelligens.

Metode

POLITI

Metode

Rapporten bygger på data fra politiets sagsstyringssytem 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 sagsstyringssytem Polsas. Data er behandlet i Qlikview-rapporten NCIK Forebyggelse (Årsrapport).

- Data dækker kalenderårene 2019-2022. Data er frosset 1. januar 2023, hvilket betyder, at registreringer foretaget efterfølgende ikke er med.
- 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

Tværgående tema

I 2022 ændredes registreringspraksis i NCIK. Den betyder, at sager, der indeholder phishing og smishing ikke længere kun kategoriseres under sagsområdet misbrug af kortoplysninger. I stedet er phishing, smishing og vishing samt NemID og MitID introduceret som selvstændige temaer, der går på tværs af sagsområderne. De fleste af sagerne med disse temaer er tilknyttet et sagsområde, og derfor optræder sagerne også i gennemgangen af sagsområderne. En del af sagerne er dog ikke tilknyttet et sagsområde, da temaet beskriver sagens indhold tilstrækkeligt.

Derfor indeholder denne rapport en samlet opgørelse af, hvor mange af anmeldelserne fra 2022, der kan relateres til de forskellige temaer. I denne opgørelse er prioriteringsnøglen ikke brugt. Det betyder, at hvis en sag indeholder flere temaer, vil den optræde flere gange i opgørelsen.

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 mv. Data til denne rapport er låst den 1. januar 2023, men fordi data er dynamiske, betyder det, at data trukket den 1. januar 2023 ikke vil være de samme, som data trukket den 1. januar 2022. Dette 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

Kategorisering af personer

Årsrapporten tager udgangspunkt i de personer, der er tilknyttet anmeldelser modtaget i 2022. 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 CVR-nummer, mens private personer har et CPR-nummer. Professionelle anmeldere består af virksomheder, myndigheder, foreninger m.v..

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/MitID 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, registreres deres hovedsædes adresse, som ofte ligger i København. Det er en del af grunden til, at så mange af anmeldelserne placeres i Københavns politikreds.

Kildehenvisninger

Danmarks Statistik (2023) *It-anvendelse i befolkningen 2022*

Federal Bureau of Investigation (2023) *Internet Crime Report 2022*

Center for Cybersikkerhed, Forsvarets Efterretningstjeneste (2023) *Cybertruslen mod Danmark 2023*

Finans Danmark (2021) *Unge. Gæld, forbrug og opsparing*

Journal of Language and Social Psychology (2014) *Truth-Default Theory (TDT): A Theory of Human Deception and Deception Detection*

NCIK
NATIONALT CENTER FOR IT-KRIMINALITET

POLITI

NCIK årsrapport 2022