NCIK
NATIONALT CENTER FOR IT-KRIMINALITET

POLITI

NCIK årsrapport 2023

En rapport om it-relateret økonomisk kriminalitet anmeldt i 2023

Indholdsfortegnelse

Indledning

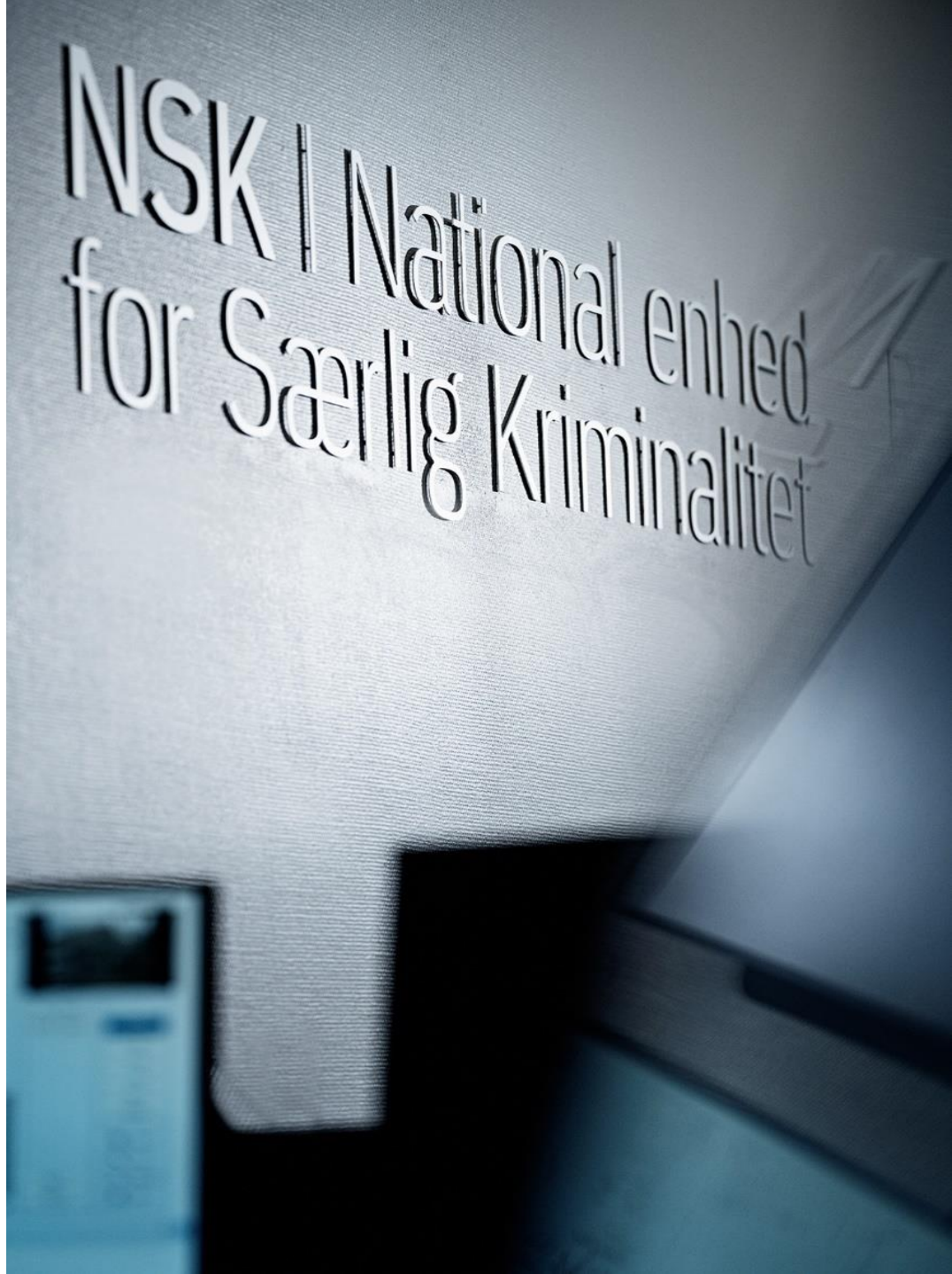
I denne rapport præsenterer vi anmeldelsesbilledet, som det så ud for it-relateret økonomisk kriminalitet i 2023. Årsrapporten indeholder de officielle tal fra Nationalt Center for It-Kriminalitet (NCIK) om it-relateret økonomisk kriminalitet og giver en oversigt over anmeldelserne på alle NCIKs sagsområder.

2023 har været præget af en markant stigning i antallet af anmeldelser om it-relateret økonomisk kriminalitet. Med den rekordstore stigning på 30 procent i forhold til 2022 står vi over for et anmeldelsesbillede, der kræver endnu større fokus på forebyggelse og analyse af it-relateret økonomisk kriminalitet samt på en effektiv og skarp prioritering, så vi hurtigt finder ud af, hvilke sager der skal efterforskes i politikredsene.

Indledningsvis beskriver vi kriminalitetsområdet og fremhæver nogle af de aspekter, der gør it-relateret økonomisk kriminalitet til en særligt udfordrende kriminalitetsform. Herefter præsenteres anmeldelsestallene fordelt på sagsområderne, og i den efterfølgende del af rapporten går vi i dybden med de enkelte kriminalitetsområder for at give en mere nuanceret forståelse af det nuværende trussels- og situationsbillede.

God læselyst.

Jesper Kracht, politiinspektør og 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 kortoplysninger, CEO-fraud 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.

Delmængde af den it-relaterede kriminalitet, der finder sted
Denne årsrapport opgør udelukkende den it-relaterede økonomiske kriminalitet, som NCIK har kendskab til i form af anmeldelser. Danmarks Statistik opgør i rapporten It-anvendelse i befolkningen 2023, at kun hver femte borger, der har været udsat for it-relateret økonomisk kriminalitet, kontakter politiet efterfølgende (Danmarks Statistisk, 2023:54). Det vidner om et stort mørketal på kriminalitetsområdet, og der er ingen tvivl om, at det faktiske omfang af denne type kriminalitet er større end opgjort i denne rapport.

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, NCIK modtager, er det beløb, den enkelte har mistet, begrænset. Til gengæld ses der ofte gerningspersoner, der udsætter en lang række borgere for samme type bedrageri og derved opnår et betydeligt udbytte. Her har NCIK 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 2023 fremgår det, at det kun er 47 procent af de adspurgte mænd, der i høj grad kan genkende svindel på nettet, mens det samme gør sig gældende for kun 36 procent af de adspurgte kvinder. Det er særligt de ældre aldersgrupper, der mener, at de ikke har nok viden om it-sikkerhed, da ca. 47 procent af de 80-89-årige mener, at de i mindre grad eller slet ikke har nok viden om it-sikkerhed (Danmarks Statistik, 2023:55).

Færre anmeldelser og stor skade
På nogle af de sagsområder, NCIK behandler, kan skaden for den enkelte borger eller virksomhed være stor.

Antallet af anmeldelser om kontaktbedrageri mod virksomheder er faldet med ca. 20 procent i forhold til 2022. Faldet skal formentlig ses i lyset af, at der har været stort forebyggelses- og mediemæssigt fokus på CEO fraud i løbet af 2023. Selvom anmeldelsestallet er faldet, og sagstallet er lavere end i mange andre af NCIKs sagsområder, er det vigtigt med et fortsat fokus på denne type kriminalitet, da det ofte er meget store beløb, virksomheder, foreninger og myndigheder bliver svindlet for.

Et andet eksempel på et område, som ikke fylder meget i anmeldelsesbilledet, men har store økonomiske og personlige konsekvenser for forurettede, er datingsvindel. Her er tale om organiserede kriminelle, der typisk måludpeger deres ofre via sociale medier. NCIK ser i ofte 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 **35.254** anmeldelser om it-relateret økonomisk kriminalitet i 2023.

Det er det højeste antal anmeldelser nogensinde

Det er en **stigning på 30 procent** i forhold til 2022

Samhandel er stadig NCIKs største sagsområde og udgør ca. **35 procent** af anmeldelserne

Der er samlet set sket en **stigning på 42 procent** i antal anmeldelser fra 2019 til 2023

Væsentlige konklusioner 2/2

Anmeldelser om misbrug af kortoplysninger er steget med **70 procent** fra 2022 til 2023

Fald på **20 procent** i sager om kontaktbedrageri mod virksomheder.

Markant fald på **40 procent** i antallet af anmeldelser om kreditbedrageri

Der er sket en **stigning i antallet af anmeldelser med sms som kontaktform på 130 procent** i forhold til 2022.

Stigningen skal ses som et resultat af det generelt stigende anmeldelsestal og en stor stigning i antal anmeldelser om bekendt i knibe, hvor forurettede modtager en besked fra gerningspersonen, der udgiver sig for at være forurettedes barn, der beder om penge

Sådan er sagstallene opgjort i årsrapporten

Når politiet modtager en anmeldelse om it-relateret økonomisk kriminalitet, beriges denne med en såkaldt søgenøgle. Det er en kategorisering, 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 sagsområder.

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 54 i rapporten.

Anmeldelser om it-relateret økonomisk kriminalitet i 2023

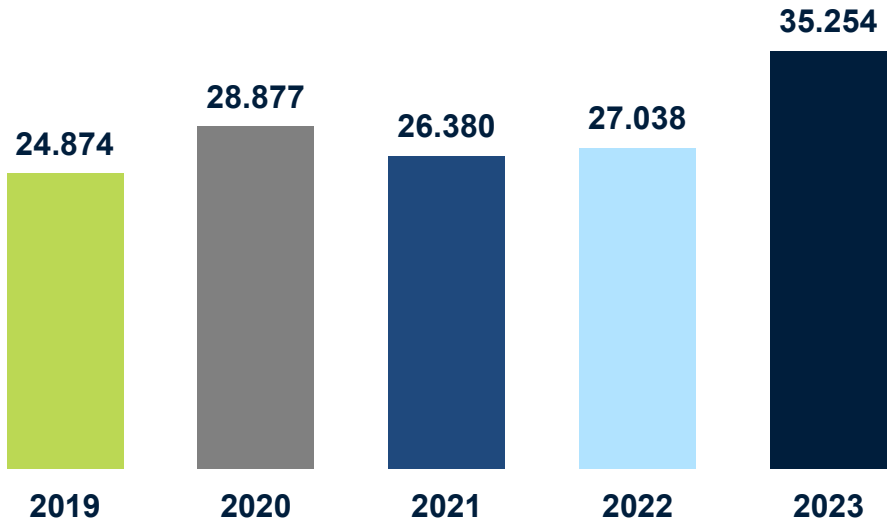
POLITI

35.254

I 2023 modtog NCIK 35.254 anmeldelser om it-relateret økonomisk kriminalitet. Dette tal udgør den primære base i årsrapporten*

*Se metodeafsnit på side 54 for mere information om datagrundlaget i denne rapport.

Rekordmange anmeldelser i 2023



Stor stigning i anmeldelsestal

NCIK modtog i 2023 35.258 anmeldelser om it-relateret økonomisk kriminalitet. Det er 8.220 flere anmeldelser end i 2022, hvilket svarer til en stigning på 30 procent.

Denne stigning skal ses i lyset af en samlet stigning i antal anmeldelser om it-relateret økonomisk kriminalitet siden 2019. Der er samlet sket en stigning i antal anmeldelser fra 2019 til 2023 på 42 procent.

Stigning på tværs af sagsområder

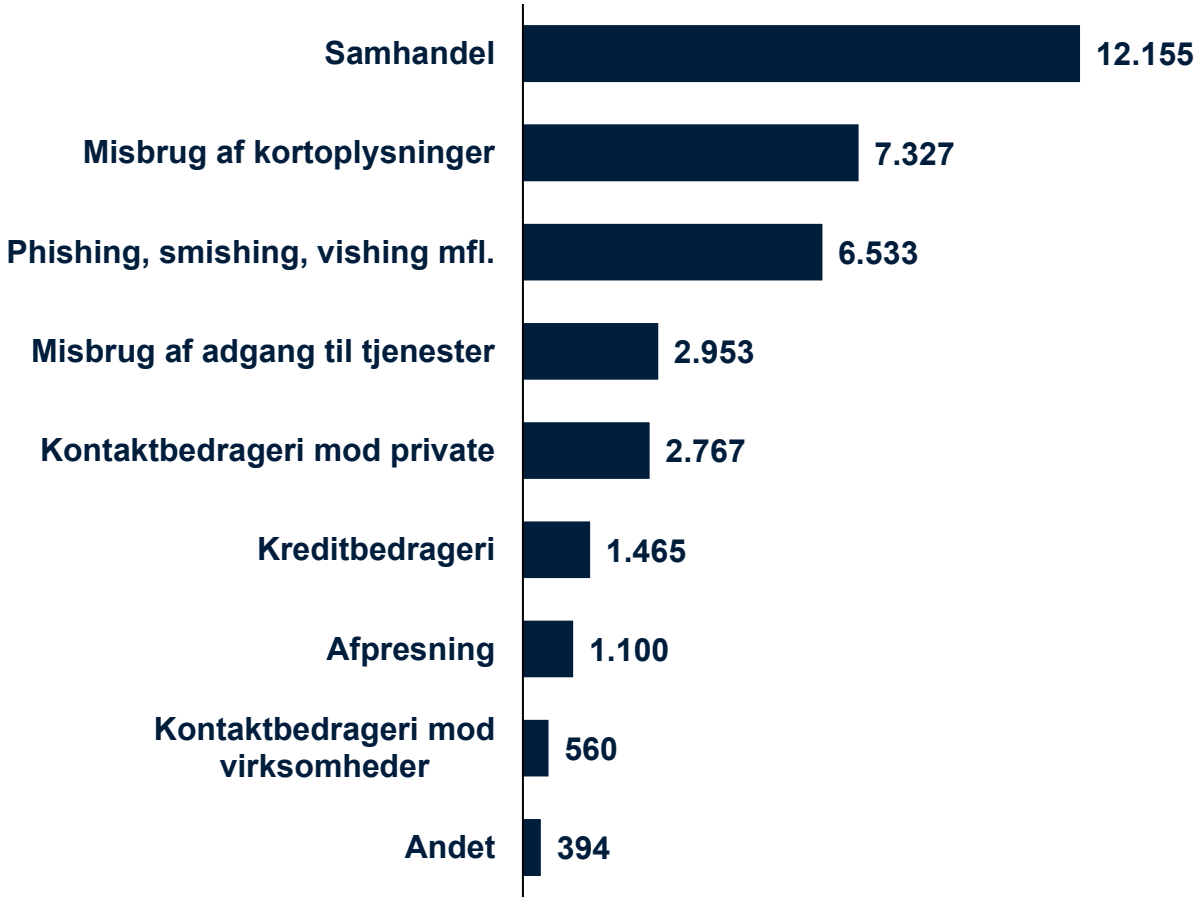
På seks ud af otte af NCIKs etablerede sagsområder er der sket en stigning i antal anmeldelser. Stigningen er særligt båret af anmeldelser om misbrug af kortoplysninger, misbrug af adgang til tjenester og en stigning i anmeldelser med smishing som kontaktmodus.

Dynamiske tal

Det totale anmeldelsestal for alle foregående år 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: (35.254) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos NCIK i år 2023.

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



Samhandel er stadig NCIKs største sagsområde

I 2023 modtog NCIK 12.155 anmeldelser om samhandelsbedrageri, hvilket udgør 35 procent af alle anmeldelser om it-relateret økonomisk kriminalitet i 2023. Det er en stigning på 15 procent i forhold til 2022. Stigningen skal ses i lyset af en stor samlet stigning i anmeldelser på tværs af de fleste af NCIKs sagsområder.

Stor stigning i misbrug af kortoplysninger

Der er sket en stigning på 70 procent i antallet af anmeldelser om misbrug af kortoplysninger fra 2022 til 2023. Stigningen kan skyldes, at implementering af tekniske løsninger for at beskytte danskere mod indbrud i netbank, gør, at kriminelle i stedet retter deres fokus mod misbrug af kortoplysninger.

Fald på to sagsområder

På sagsområderne kreditbedrageri og kontaktbedrageri mod virksomheder er der i begge kategorier sket et fald i antal anmeldelser fra 2022 til 2023.

Om kategorien Phishing, smishing, vishing mfl.

Denne kategori indeholder sager, hvor anmeldelsen er mangelfuld, eller hvor det ikke har været muligt at afgøre, hvad der er sket. I langt de fleste af sagerne er der ikke rapporteret et økonomisk tab.

Base: (35.254) Antal anmeldelser om it-relateret økonomisk kriminalitet modtaget hos NCIK i år 2023.

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

91 procent er private anmeldere

I 2023 modtog NCIK 32.163 anmeldelser fra private anmeldere svarende til 91 procent af alle anmeldelser.

9 procent er professionelle anmeldere

I 2023 modtog NCIK 3.115 anmeldelser fra professionelle anmeldere svarende til ni procent af alle anmeldelser.

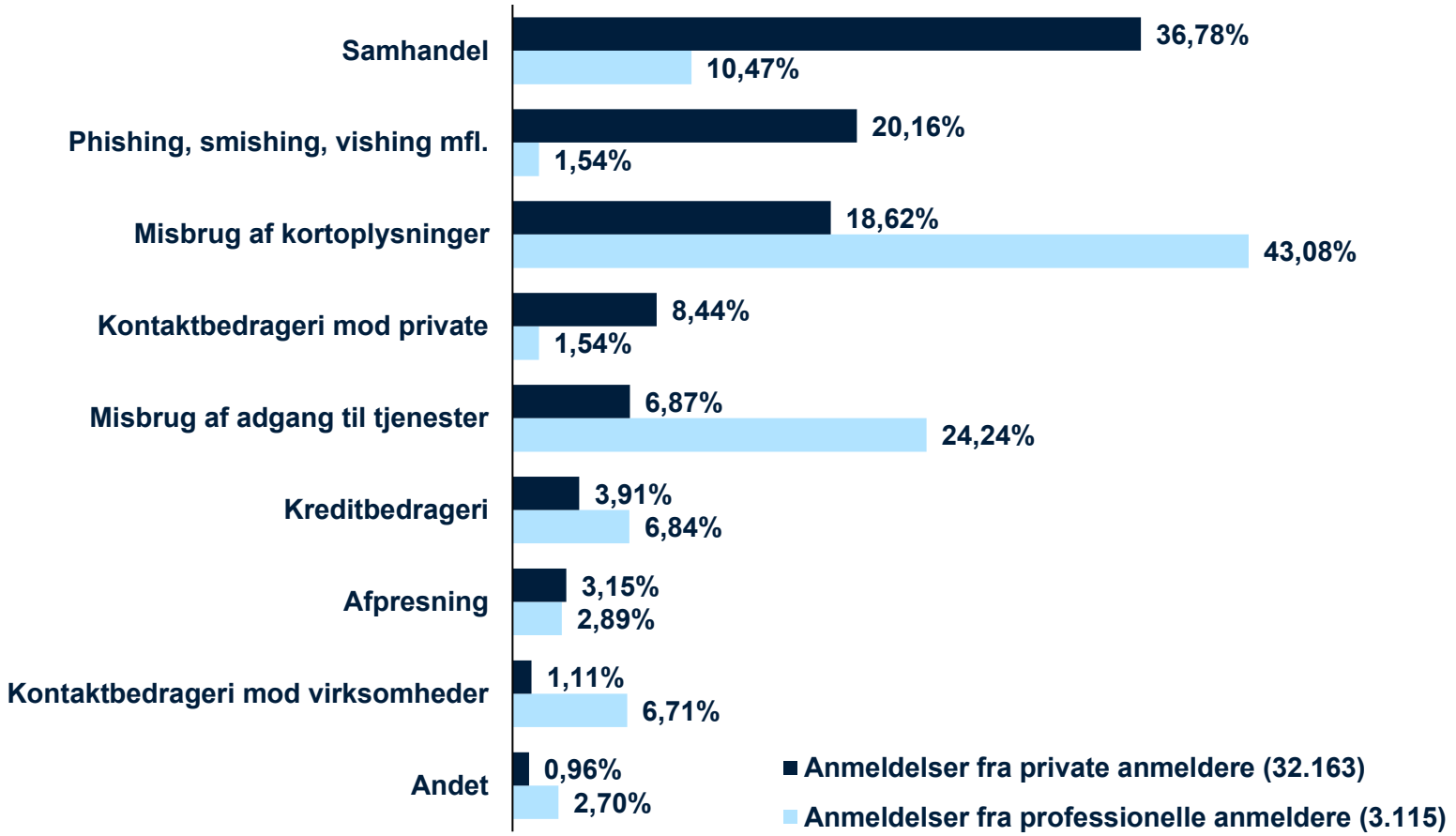
Anmeldere af it-relateret økonomisk kriminalitet opdeles i to grupper

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 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: (35.278) 32.163 anmeldelser er fra privatpersoner. 3.115 anmeldelser er fra professionelle. Nogle anmeldelser har både en privat og en professionel anmelder tilknyttet. Derfor overstiger basen i denne tabel (35.278) det samlede anmeldelsestal (35.254).

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



Private anmeldte i høj grad samhandelsbedrageri

37 procent af anmeldelserne fra private anmeldere handlede om samhandel. Det er et lille fald i forhold til 2022, hvor 42 procent af de private anmeldere anmeldte samhandel.

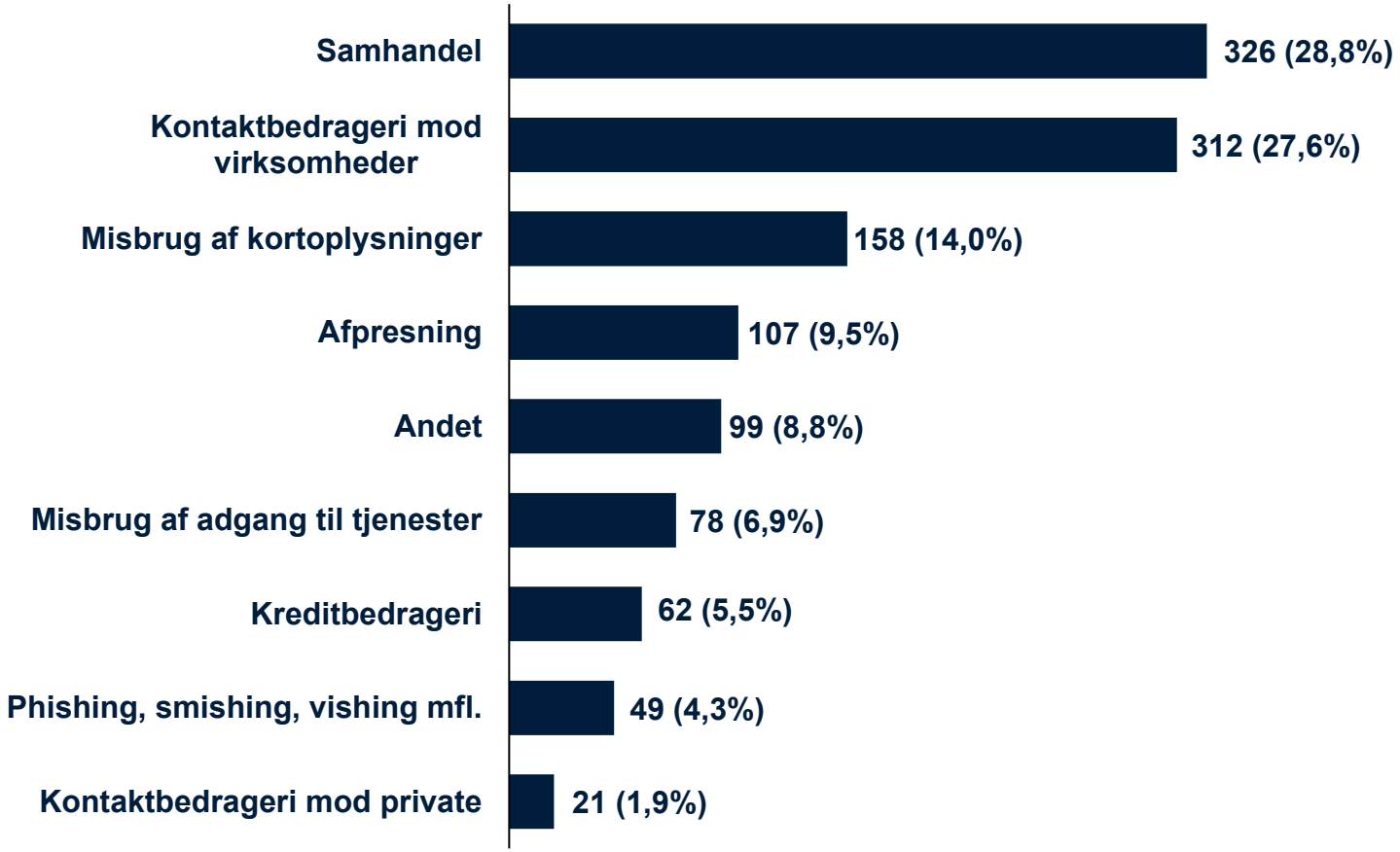
Anmeldelser fra professionelle anmeldere kom oftest fra banker

De professionelle anmeldelser handlede især om misbrug af kortoplysninger, misbrug af adgang til tjenester og samhandel.

Det er ikke overraskende, at netop disse sagsområder fylder meget i anmeldelser fra professionelle anmeldere. Langt størstedelen af de professionelle anmeldere er banker eller lånevirksomheder. Ca. halvdelen af anmeldelserne fra professionelle anmeldere kommer fra 40 forskellige virksomheder, organisationer eller myndigheder.

Base: (35.278) 32.163 anmeldelser er fra privatpersoner. 3.115 anmeldelser er fra professionelle. Nogle anmeldelser har både en privat og en professionel anmelder tilknyttet. Derfor overstiger basen i denne tabel (35.278) det samlede anmeldelsestal (35.254).

Halvdelen af de professionelle forurettede i 2023 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 i 2023.

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 sagsområde.

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

Base: (1.212) Antal unikke professionelle forurettede inden for hvert sagsområde i 2023.

Antal forurettede udsat for it-relateret økonomisk kriminalitet i 2023

32.829 forskellige personer

har været udsat for it-relateret økonomisk kriminalitet

1.128 forskellige professionelle

har været udsat for it-relateret økonomisk kriminalitet

Om de forurettede

I strafferetlige termer benævnes et offer for kriminalitet ofte som den forurettede part i sagen. Derfor bruges betegnelsen forurettede om ofrene for it-relateret økonomisk kriminalitet i årsrapporten.

Alder

Mange forurettede i fx samhandelsbedrageri er yngre personer og på dette sagsområde er gennemsnitsalderen 38 år, mens der på sagsområdet kontaktbedrageri mod private er en overrepræsentation af ældre personer, hvor gennemsnitsalderen er 55 år.

Køn

Kønsfordelingen på de forskellige sagsområder varierer meget fra område til område. I fx samhandelsbedrageri og kontaktbedrageri mod virksomheder er der en overrepræsentation af mandlige forurettede, men der er flest kvinder, der er forurettede i sager om kontaktbedrageri mod private. På tværs af alle sagsområder er der en fuldstændig ligelig fordeling mellem kønnene.

Antal anmeldelser fordelt på politikredse

Nordjyllands Politi
2.706 anmeldelser (**7,7%**)
Pr. 1.000 indbygger: **4,9**

Østjyllands Politi
3.349 anmeldelser (**9,6%**)
Pr. 1.000 indbygger: **5,3**

Midt- og Vestjyllands Politi
3.084 anmeldelser (**8,8%**)
Pr. 1.000 indbygger: **4,8**

Sydøstjyllands Politi
2.487 anmeldelser (**7,1%**)
Pr. 1.000 indbygger: **4,9**

Syd- og Sønderjyllands Politi
2.054 anmeldelser (**5,9%**)
Pr. 1.000 indbygger: **4,4**

Fyns Politi
2.870 anmeldelser (**8,2%**)
Pr. 1.000 indbygger: **5,3**

Sydsjælland og Lolland-Falsters Politi
2.188 anmeldelser (**6,3%**)
Pr. 1.000 indbygger: **5,5**

Midt- og Vestsjællands Politi
2.568 anmeldelser (**7,3%**)
Pr. 1.000 indbygger: **5,3**

Nordsjællands Politi
4.294 anmeldelser (**12,3%**)
Pr. 1.000 indbygger: **7,0**

Københavns Vestegns Politi
2.464 anmeldelser (**7,0%**)
Pr. 1.000 indbygger: **5,7**

Københavns Politi
6.728 anmeldelser (**19,2%**)
Pr. 1.000 indbygger: **6,6**

Bornholms Politi
180 anmeldelser (**0,5%**)
Pr. 1.000 indbygger: **4,6**

Base: (35.269) Kortet ovenfor viser 34.972 sager. I 15 sager er der to anmeldere tilknyttet, som er bosat i forskellige politikredse. Disse 15 sager tæller derfor dobbelt.
Herudover er der 297 anmeldelser, hvor bopælskredsen er ukendt. Vedrørende Københavns Politikreds, se metodeafsnit.

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. Det kan også dreje sig om sager, hvor sælger aldrig modtager penge for varen, selvom varen er sendt til køber.

Billetter
I sager om svindel med billetter er det typisk sager, hvor forurettede efterlyser billetter til udsolgte arrangementer.

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.

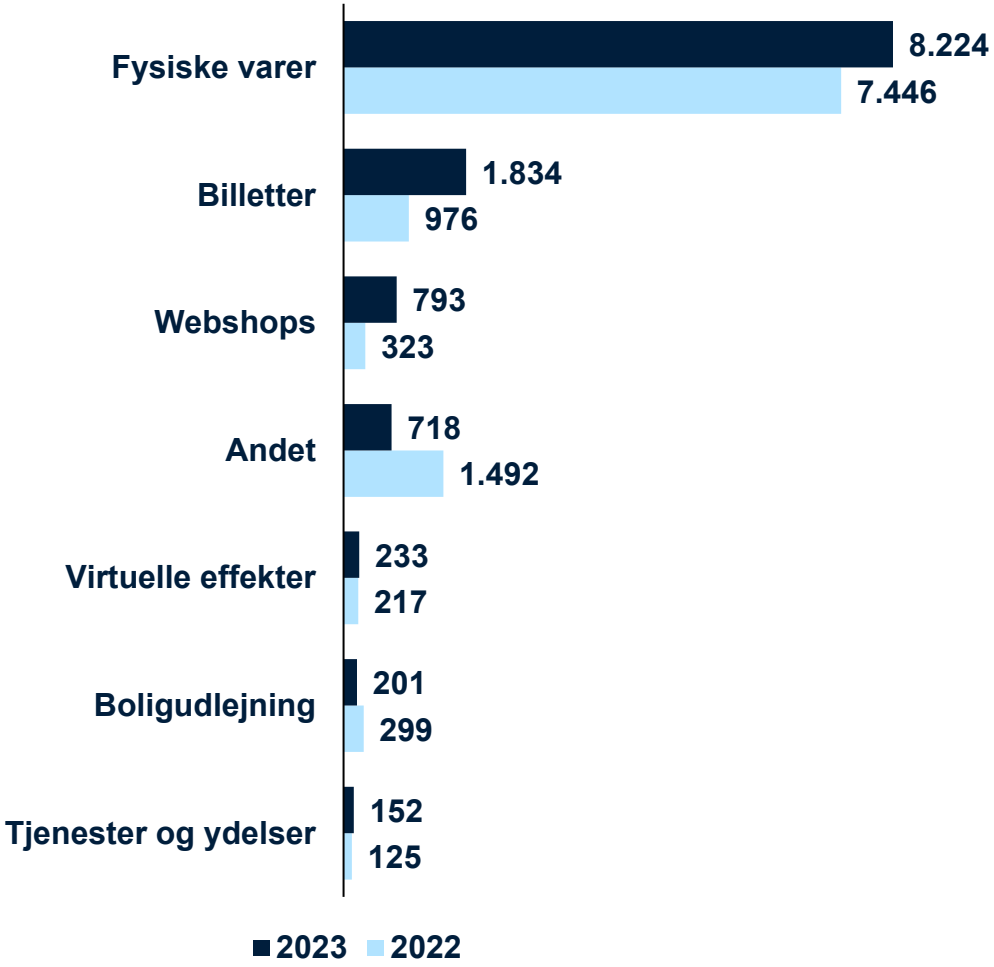
Boligudlejning
I sager om boligudlejning betaler forurettede typisk for leje af en feriebolig eller permanent bolig. Gerningspersonen udlejer fiktive boliger eller boliger, som personen ikke har råderet over.

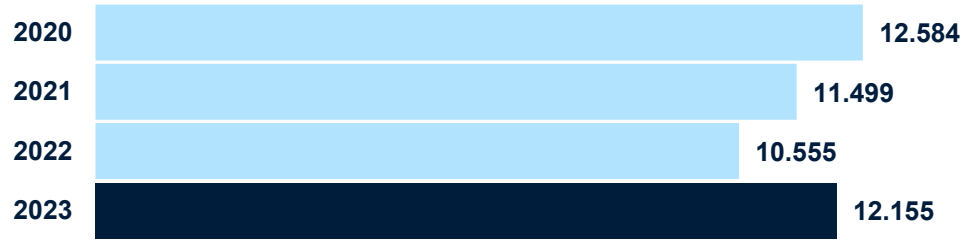
Tjenester og ydelser
I sager om svindel med tjenester og ydelser har to parter indgået en aftale om en ydelse, som forudbetales af den ene part, og som ikke leveres af den anden part. Det kan fx være forudbetaling af håndværkerarbejde, hjælp til skoleopgaver, hjælp til hjemmesider mv. eller ved køb af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

35% af alle anmeldelser i 2023





Flere sager i 2023 end i 2022 og 2021

Det samlede anmeldelsestal inden for samhandel er steget med ca. 15 procent fra 2022 til 2023 og med ca. seks procent fra 2021 til 2023. Stigningen skal formentlig ses som et resultat af en generel stigning i antallet af e-handlende borgere fra 2022 til 2023 (Danmarks Statistik, 2023; 18).

Stigning i sager om billetter

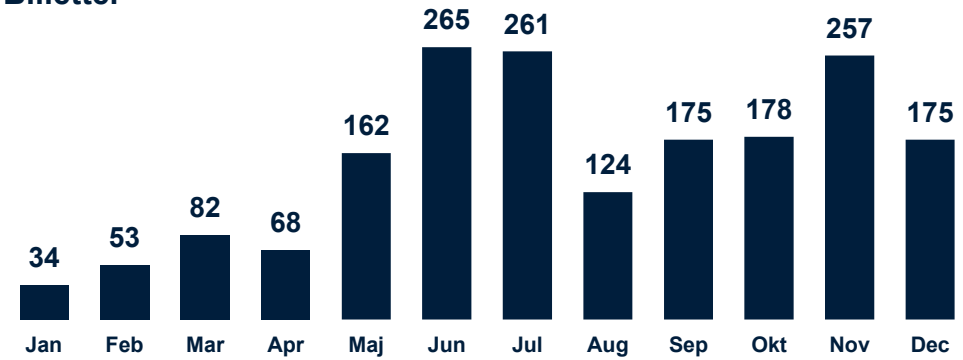
15 procent af alle sager om samhandelsbedrageri i 2023 omhandlede svindel med billetter, hvilket svarer til en stigning på ca. 90 procent i forhold til 2022. Stigningen skal formentlig ses i lyset af, at kulturlivet ikke længere er påvirket af covid-19 restriktioner, og at andelen af borgere, der køber billetter til koncerter, festivaler, fodboldkampe mv. således har været stigende siden 2021 (Danmarks Statistik, 2023; 20).

Mørketal i sager om virtuelle effekter

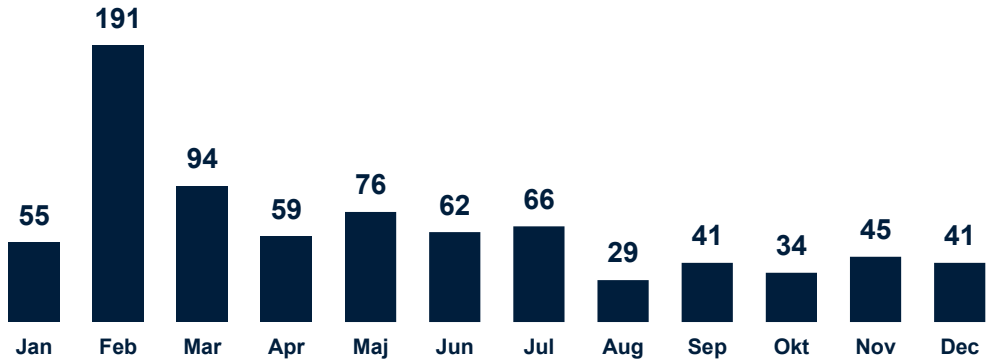
Fra 2022 til 2023 har der været en lille stigning i sager omhandlende virtuelle effekter på ca. syv procent. Virtuelle effekter har særligt værdi i online spilverdener, og den handlede vare er typisk skins eller virtuel valuta. Et dansk studie viser, at en tredjedel (35,8 procent) af unge danskere, der handler med virtuelle effekter, har været udsat for svindel i en online handelssituation (Nordic Journal of Criminology, 2023; 9), hvorfor der formodes at være et betydeligt mørketal på området.

Sæsonbetonede anmeldelser om samhandelsbedrageri

Billetter



Webshops



Sæsonvise udsving i anmeldelsesbilledet
På nogle sagsområder er det muligt at se i anmeldelsesbilledet, at store begivenheder eller sæsoner finder sted. Det kan fx være udsolgte koncerter, festivaler eller sportsbegivenheder.

Billetter
I 2023 modtog NCIK 1.834 anmeldelser om samhandelsbedrageri omhandlende svindel med billetter. Det er især i løbet af festivalsæsonen i juni og juli måned, hvor flest anmelder billetsvindel.

Der er hovedsageligt tale om sager, hvor forurettede har efterlyst billetter til en bestemt festival via sociale medier, og efterfølgende kontaktes af gerningspersonen. Der er ligeledes eksempel på sager, hvor svindlen har fundet sted i Facebookgrupper, hvor der formidles salg af falske billetter.

Stigningen i november måned skyldes store sportsbegivenheder som FC København, der spillede kampe i Champions League og EM-kvalifikationslandskamp mod Slovenien, der begge havde udsolgt.

Webshops
I 2023 modtog NCIK i alt 793 anmeldelser om samhandelsbedrageri omhandlende falske webshops. Det svarer til en stigning på 146 procent i forhold til 2022, og skal blandt andet ses i lyset af krigen i Ukraine og de heraf følgende stigende varmepriser. I februar 2023 så NCIK en markant stigning i sager om svindel ved køb og salg af brænde og træpiller på særligt én falsk webshop.

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 fx skal betales et mindre beløb i ekstra fragt for levering af en pakke. Andre gange kan forurettede modtage en falsk mail fra fx 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.

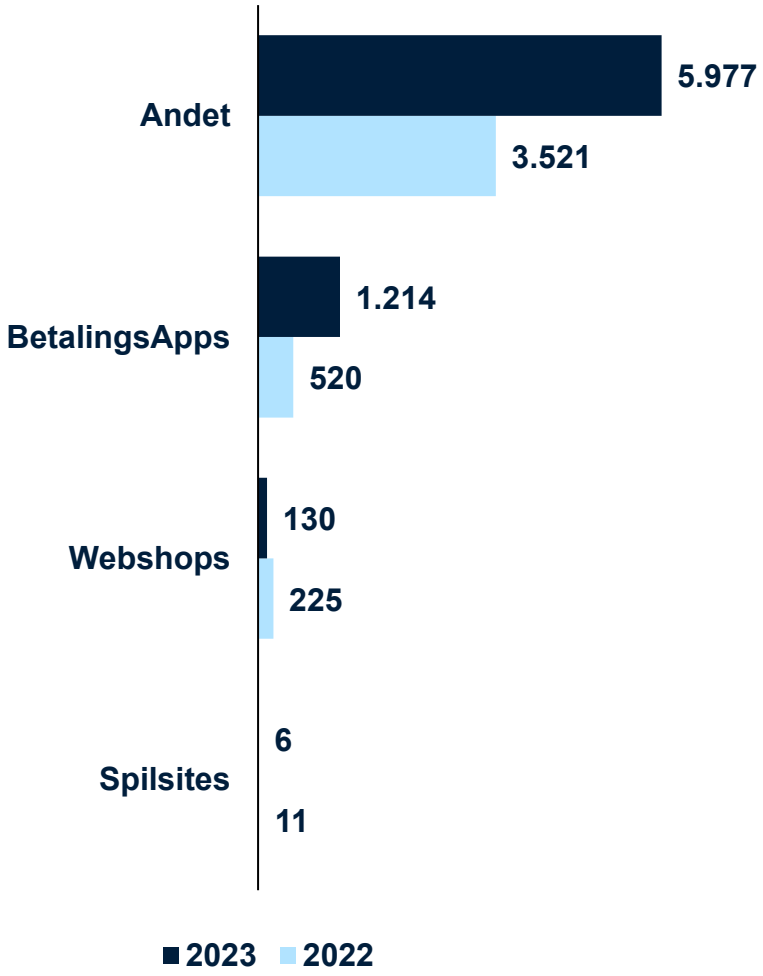
Webshops
Denne type svindel forekommer, når kortoplysninger uberettiget bliver brugt til at købe en vare eller ydelse på en webshop. Varen sendes ofte til et muldyr, til en postboks eller som elektronisk vare på e-mail.

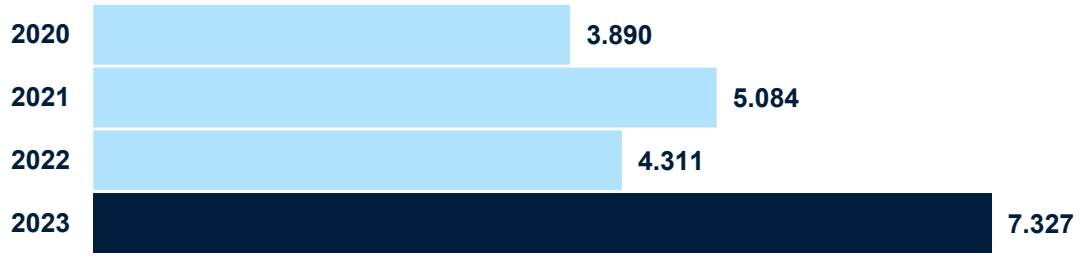
Betalingsapps
Der findes i dag flere betalingsløsninger, hvor brugere kobler deres kortoplysninger sammen med betalingsløsningen. Da man både kan foretage overførsler og køb i butikker gennem betalingstjenesterne, er de blevet et attraktivt middel for misbrug af kortoplysninger.

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

Misbrug af kortoplysninger

21% af alle anmeldelser i 2023





Flere anmeldte misbrug af kortoplysninger

Der er siden 2022 sket en stigning på 70 procent i antallet af anmeldelser om misbrug af kortoplysninger. Stigningen kan blandt andet ses i lyset af, at kriminelle nu formodes at rette deres fokus fra indbrud i netbank til misbrug af kortoplysninger pga. de forbedrede sikkerhedstekniske foranstaltninger, som bl.a. finansindustrien har indført i forbindelse med netbanksløsninger. Her er der eksempelvis indført to-faktorgodkendelse ved login og overførsler. Derudover er der også indført QR-koder ved brug af MitID, hvilket kan have betydning for, at kriminaliteten har flyttet sig over på misbrug af kortoplysninger.

Om kategorien Andet

Kategorien Andet fylder forholdsvis meget i opgørelsen. I denne kategori ligger sager om misbrug af kortoplysninger, der samtidig er registreret under Phishing, smishing, vishing mfl. for at klarlægge gerningspersonens fremgangsmåde til at misbruge forurettedes kortoplysninger.

Betalingsapps og webshops

Misbrug af kortoplysninger er også misbrug af betalingsapps som fx MobilePay og Apple Pay. I 2023 er sager, der er registreret under kategorien betalingsapps, steget med 133 procent i forhold til 2022, mens sager, der er registreret under webshops, er faldet med ca. 42 procent i samme periode.

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, 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.

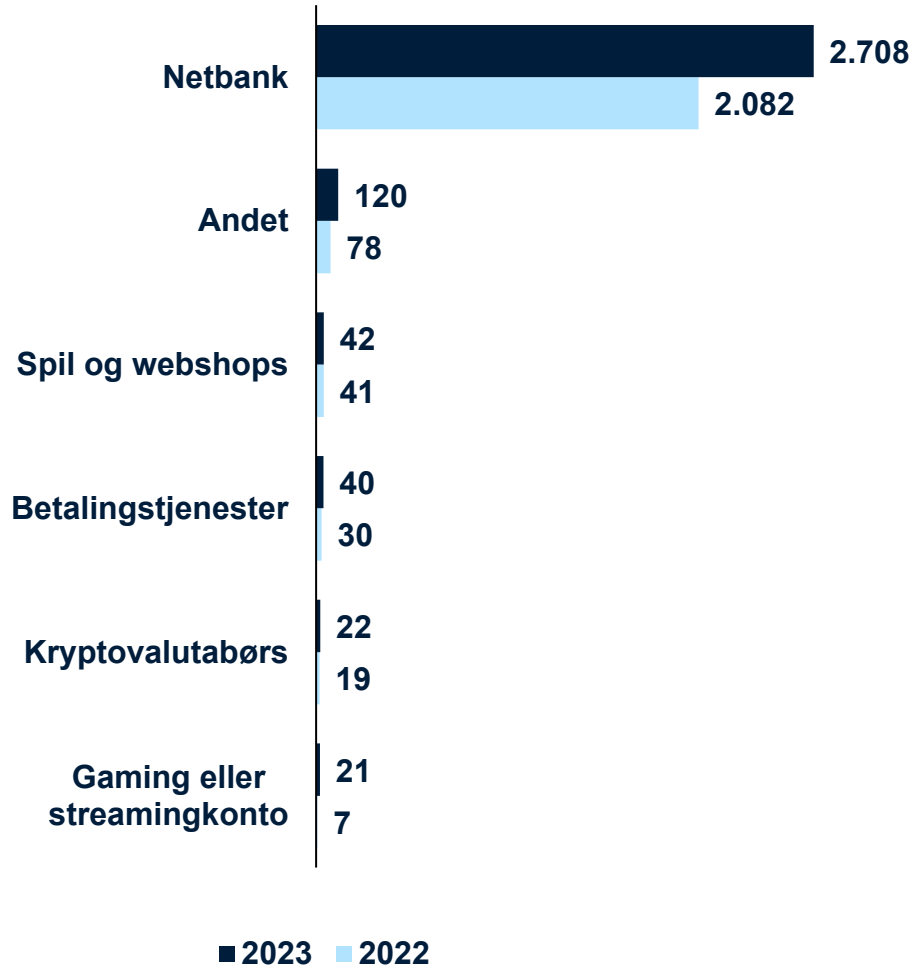
Betalingstjenester
Bonuskortordninger og andre former for konti med opsparede bonuspoint, fx hos flyselskaber, er ofte i gerningspersoners interesse. Gerningspersonerne skaffer sig adgang til kontoen, og bruger pointene til at købe varer, rejser og tjenesteydelser.

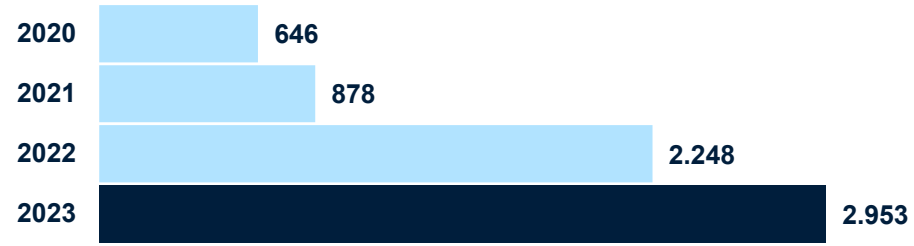
Gaming eller streamingkonto
I sager, hvor forurettede har fået misbrugt sin gaming eller streamingkonto, bliver der hævet penge, overført penge eller oprettet abonnementer på forurettedes streamingkonto. Der kan også blive stjålet virtuelle effekter.

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.

Misbrug af adgang til tjenester

8% af alle anmeldelser i 2023





Stigning i antallet af sager om misbrug af adgang til netbank

Antallet af anmeldelser om misbrug af adgang til netbank i 2023 er steget med ca. 29 procent i forhold til 2022.

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

Disse opkald foretages typisk ved hjælp af spoofing for at få opkaldet til at fremstå mere troværdigt og legitimt. Ved at spoofe et telefonnummer kan man ringe og udgive sig for et andet nummer end det, man ringer fra. Ofte kommer opkaldene fra numre, som forbindes med troværdighed. Eksempelvis pengeinstitutter, politiet eller andre offentlige myndigheder.

Stigning i antallet af sager om misbrug af adgang til tjenester siden 2020

Misbrug af adgang til tjenester er et område, der fortsat er i vækst, når der sammenlignes med anmeldelsestallet fra 2020, hvorfra der er sket en stigning på ca. 360 procent frem til 2023.

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 falske hjemmesider, 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 eller arv (såkaldt ”Nigeriabrev”). Forud for udbetaling af arven, bliver der stillet krav om betaling af arveafgift mv. af det lovede pengebeløb, som aldrig modtages. Anmeldelser om klassiske ”Nigeriabreve” ses sjældent.

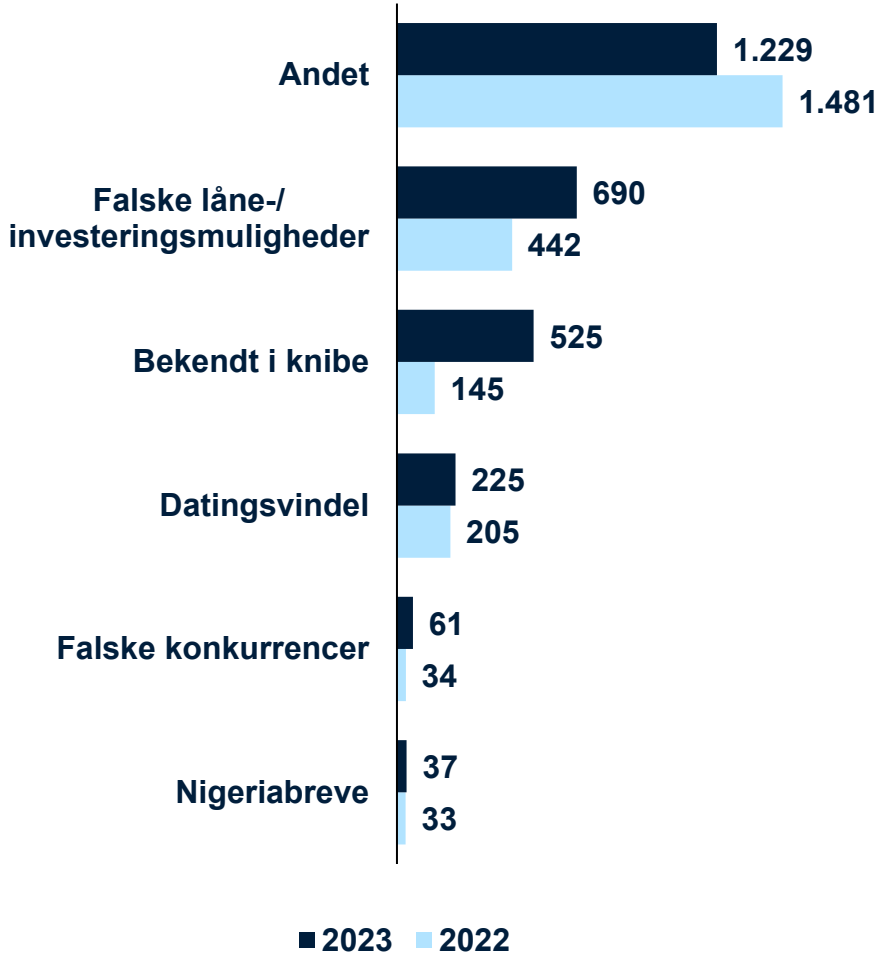
Bekendt i knibe
Denne type svindel sker ofte ved, at forurettede bliver kontaktet via e-mail, sms eller chat af en person, der udgiver sig for at være en bekendt eller nær relation. Historien udspiller sig typisk således, at der er opstået en nødsituation i udlandet, og den forurettede bliver derfor lokket til at foretage konto-til-kontooverførsler eller andre pengeoverførsler. Det kan også være sager, hvor forurettede låner penge ud i den tro, at det er en bekendt, der anmoder om lån. I realiteten er deres konto blevet overtaget af gerningspersonen.

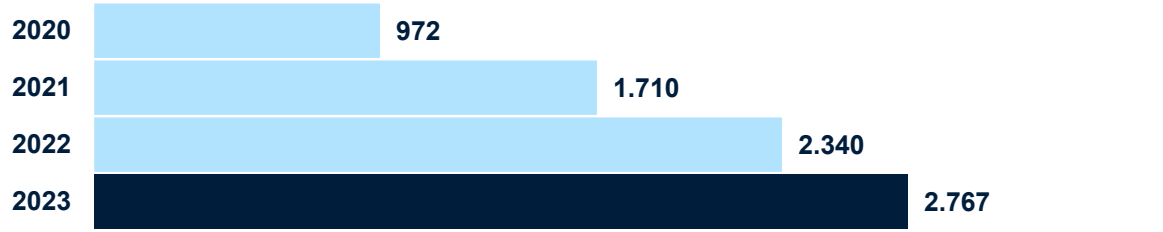
Datingsvindel
Datingsvindel tager udgangspunkt i, at en person etablerer en relation til en med falsk identitet via sociale medier. Gerningspersonen med den falske identitet udnytter forurettedes følelsesmæssige involvering og lokker penge ud af vedkommende ved kontooverførsler. Det ender typisk med, at den forurettede overfører store pengebeløb til gerningspersonen eller investerer på falske investeringssider.

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 er ofte blevet eksponeret for konkurrencen på sociale medier.

Kontaktbedrageri mod private

8% af alle anmeldelser i 2023





Flere anmeldelser om kontaktbedragerier mod private
Fra 2022 til 2023 steg antallet af anmeldelser om kontaktbedrageri mod private med ca. 18 procent. Den overordnede stigning i antallet af kontaktbedragerier er særligt båret af en stigning i sager omhandlende falske låne-/investeringsmuligheder og bekendt i knibe.

Stor andel af sager i kategorien Andet
I 2023 var der 1.229 anmeldelser registreret under Andet, og størstedelen af disse omhandler telefonsvindel mod ældre borgere. 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 konti er i fare.

Kategorien Andet dækker også over sager, hvor borgere er blevet ringet op af en engelsktalende robotstemme, der udgiver sig for at være fra politiet, under påskud af, at vedkommendes identitet var blevet misbrugt i forbindelse med alvorlig kriminalitet. Læs mere om telefonsvindel og robotstemmer på side 51.

Stor stigning i kategorien Bekendt i knibe
I 2023 var der 525 anmeldelser registreret under Bekendt i knibe, hvilket er en stigning på 262 procent i forhold til 2022. Den samlede stigning skyldes primært en stigning i antal anmeldelser vedrørende falske sms’er, hvor gerningspersoner udgiver sig for at være barn til forurettede. Under påskud af, at deres telefon er gået i stykker forsøger eller lykkes gerningsmanden med at franarre forurettede penge.

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 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 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.

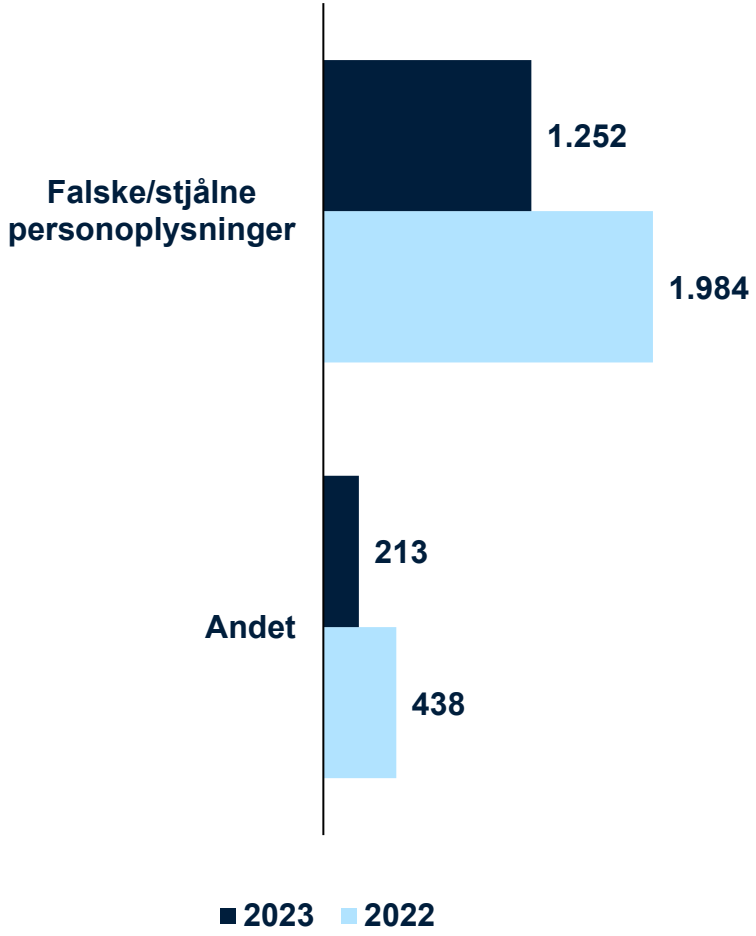
Falske/stjålne personoplysninger
Denne type svindel forekommer ved, at en gerningsperson har fået adgang til en borgers personoplysninger og derefter misbruger vedkommendes identitet til at oprette lån- eller leasingaftaler. Efterfølgende oplever virksomheden, at der ikke bliver betalt ydelse på kreditaftalen, og virksomheden forsøger at inddrive gælden hos den person, vis identitet er misbrugt.

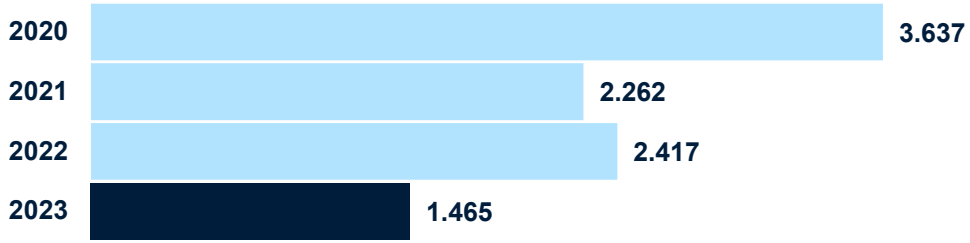
Flere virksomheder tilbyder i dag kunder at købe varer på afbetaling, hvoraf nogle virksomheder specialiserer sig i at tilbyde afbetalingsaftaler (kreditaftale) for varer købt hos andre virksomheder. Fx kan der i dag købes en ny smartphone hos virksomhed A, mens virksomhed B tilbyder at hjælpe forbrugeren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

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

Kreditbedrageri

4% af alle anmeldelser i 2023





Fald i antal anmeldelser om kreditbedrageri
Fra 2022 til 2023 var der et markant fald på ca. 40 procent i antallet af anmeldelser om kreditbedrageri. I de fleste anmeldelser om kreditbedrageri fra 2023 er der tale om en gerningsperson, der enten benytter falske eller stjålne identiteter til at optage kredit i en anden persons navn.

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

Politiet har derudover haft succes med at efterforske et større sagskompleks om kreditbedrageri begået af den samme gerningsperson, hvilket formentlig også kan være med til at forklare faldet i antallet af anmeldelser.

Om kategorien Andet
Denne kategori dækker over anmeldelser, der endnu ikke har fået en kategorisering.

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.

Også i 2023 så NCIK en 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.

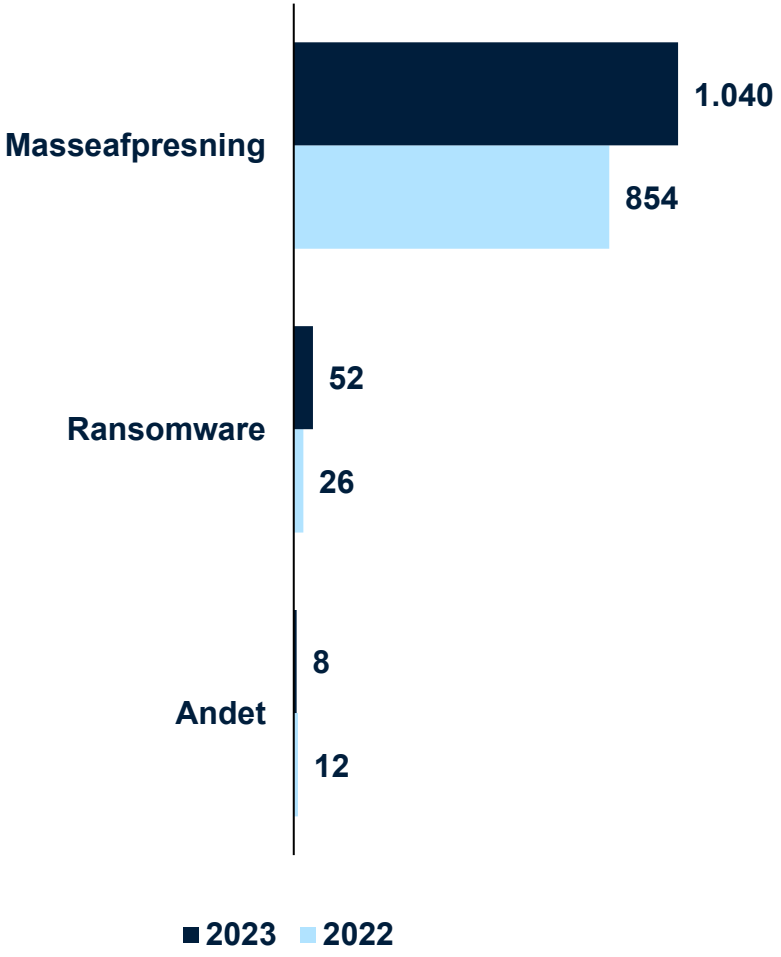
Masseafpresning
I masseafpresningssager sender gerningspersoner afpresningsmails til mange tilfældige personer i håb om, at nogle reagerer og betaler en løsesum. Gerningspersonen målretter ofte mailindholdet med henvisning til forurettedes tidligere anvendte passwords. Masseafpresningsmails bliver sendt i bølger, hvorfor NCIK også ofte modtager anmeldelserne i bølger.

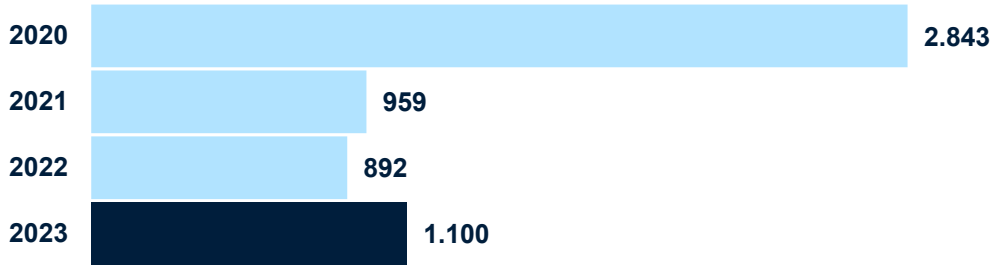
Ransomware
Ransomware rammer både borgere og virksomheder, men der er en overvægt af anmeldelser fra virksomheder. NCIK har blandt andet set eksempler på ransomware, hvor én eller flere medarbejdere i en virksomhed modtog e-mails med skjulte links til download af filer fra antageligt VPS (virtuel privat 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.

Ransomware er begyndt at bevæge sig i retning af ikke blot kryptering af data, men også tilegnelse af virksomhedskritisk eller personfølsomt materiale, der trues offentliggjort eller udbudt til salg på internettet.

Afpresning

3% af alle anmeldelser i 2023





Antallet af anmeldelser om afpresning

I 2023 modtog NCIK 1.042 anmeldelser om afpresning, hvilket er en stigning på ca. 23 procent sammenlignet med 2022. Faldet kan bero på borgernes øgede bevidsthed om digitale trusler samt bedre teknologisk beskyttelse i form af spamfiltre, der begrænser mængden af fx uønskede mails.

Masseafpresning driver udviklingen inden for sagsområdet

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 mindre grad ligner enten danske eller udenlandske politimyndigheder.

Få anmeldelser om afpresning med ransomware

I 2023 modtog NCIK 52 anmeldelser om afpresning med ransomware, hvilket er en stigning på 100 procent fra 2022.

I en trusselsvurdering fra 2023 vurderer Center for Cybersikkerhed, at truslen fra økonomisk motiveret cyberkriminalitet, herunder ransomwareangreb, er meget høj, og at veletablerede ransomwaregrupper går efter alle dele af samfundet (CFCS, 2023: 10).

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 eller formanden, 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, hvor adgangen 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 det legitime e-maildomæne, 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 2023 så NCIK flere sager, hvor en virksomhed eller forening modtog e-mails, der udgav sig for at være direktøren eller formanden 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 eller foreningens konto.

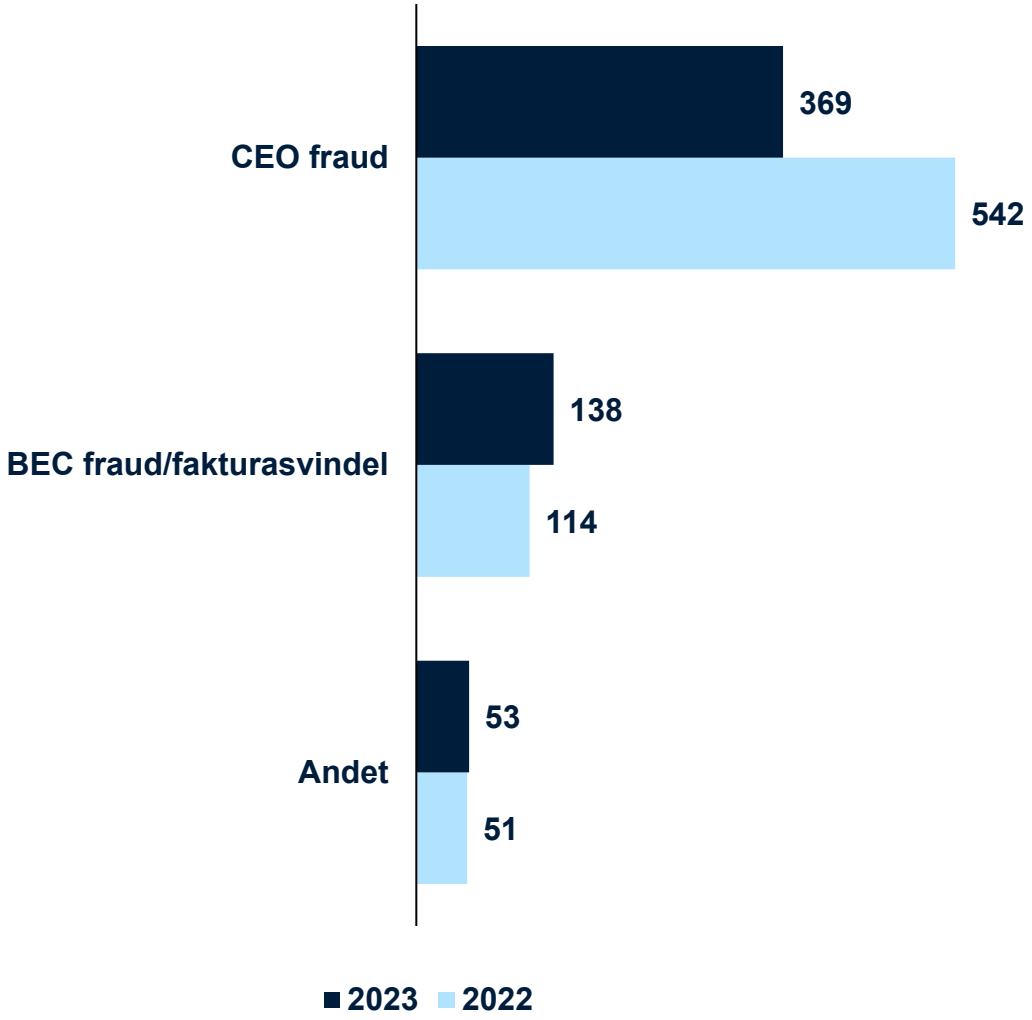
BEC/fakturasvindel

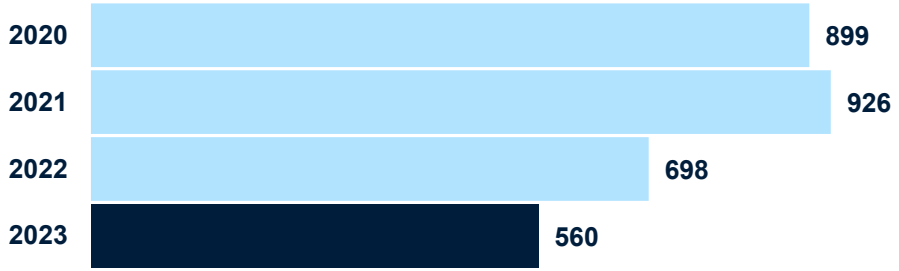
BEC/fakturasvindel minder på mange måder om CEO fraud, idet gerningspersonen prøver at vildlede en økonomimedarbejder i en virksomhed eller kasserer i en foreningen til at betale en falsk faktura. Det sker typisk ved, at firmaet modtager en faktura fra gerningspersonen på e-mail, hvor modtagerkontoen 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% af alle anmeldelser i 2023





Fald i anmeldelser om kontaktbedrageri mod virksomheder
Der blev i 2023 anmeldt ca. 20 procent færre sager om kontaktbedrageri mod virksomheder i forhold til 2022. Mere end halvdelen af anmeldelserne – 66 procent – omhandlede CEO fraud, hvor svindlere udgiver sig for at være direktør eller formand i en virksomhed eller forening for på den måde at franarre virksomheden penge.

Fokus på foreninger
I størstedelen af sagerne om CEO fraud kom anmeldelsen fra en forening, og der tegner sig dermed et billede af, at svindlerne i højere grad går målrettet efter foreninger fremfor virksomheder og offentlige myndigheder. I den forbindelse blev der i 2023 iværksat flere forebyggelsesindsatser målrettet foreninger, hvilket også førte til et stort mediemæssigt fokus på denne type kriminalitet.

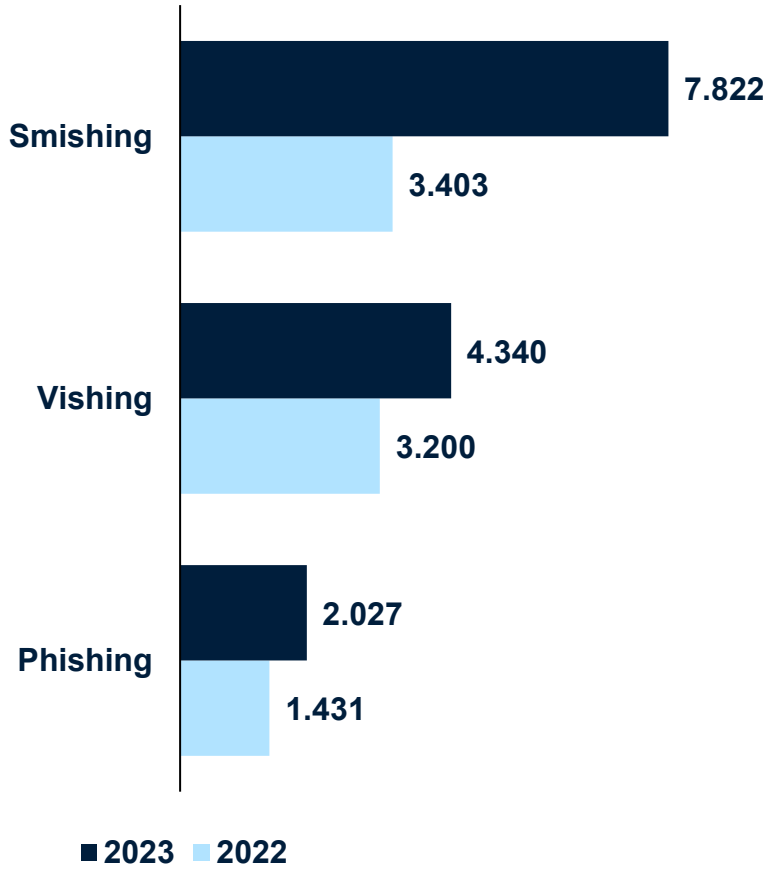
I sager om CEO fraud bliver forurettede ofte svindlet til at indkøbe gavekort til Itunes, da disse kan videresælges eller veksles til Appleprodukter eller kryptovaluta.

På trods af det samlede fald i antal anmeldelser om kontaktbedrageri mod virksomheder, ses en stigning på ca. 20 procent i antallet af anmeldelser om BEC fraud fra 2022 til 2023.

Anmeldelser og kontaktmodus

POLITI

Kontaktmodi smishing, phishing og vishing



Gerningspersonens kontaktmåde
Politiet modtager også anmeldelser, hvor gerningsindholdet ikke altid kan belyses. Dette er ofte i sager, hvor borgeren anmelder, at de har modtaget en besked (smishing), et telefonopkald (vishing) eller en e-mail (phishing), men hvor borgeren ikke trykker på linket i beskeden eller besvarer mailen. Disse henvendelser kategoriseres i langt de fleste tilfælde udelukkende efter gerningspersonens kontaktmåde – altså smishing, vishing eller phishing - og får dermed ikke andre kategorier.

På nogle sagsområder vil kontaktmodus altid være den samme – fx i samhandelsbedrageri, hvor svindlen altid foregår på samhandelsplatformen, mens det på andre sagsområder vil variere, hvad kontaktmodus er.

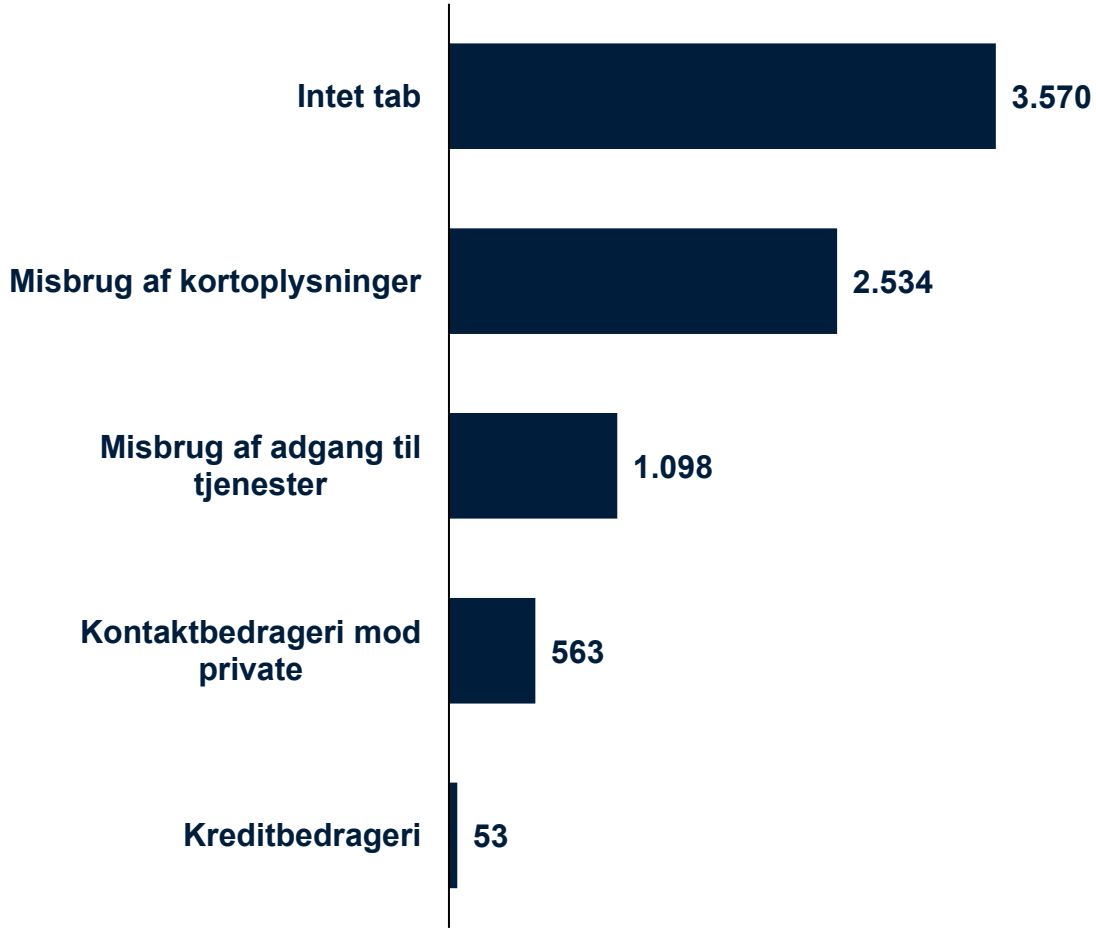
39 procent af alle anmeldelser i 2023 indeholder et eller flere kontaktmodi
Hvis en anmeldelse har flere kontaktmodi indgår den i opgørelsen under alle de modi, den har. Anmeldelser, der indeholder flere modi kan fx være sager, hvor gerningspersonen har benyttet sig af både smishing og vishing til at få adgang til forurettedes MitID.

Stigning i smishing, vishing og phishing
Anmeldelser med smishing som kontaktmodus er steget markant med ca. 130 procent i forhold til 2022. Det vil sige, at gerningspersoner i højere grad bruger sms'er i forsøget på at svindle borgere.

Læs mere om smishing som kontaktmodus på side 50.

Base: (13.632) 13.077 af anmeldelserne indeholder ét af de tre kontaktmodi. 553 anmeldelser indeholder to kontaktmodi og to anmeldelser indeholder tre kontaktmodi.

Smishing: Svindel via sms-beskeder



I 48% af anmeldelserne er der ikke rapporteret tab

I 52% af anmeldelserne er der rapporteret tab

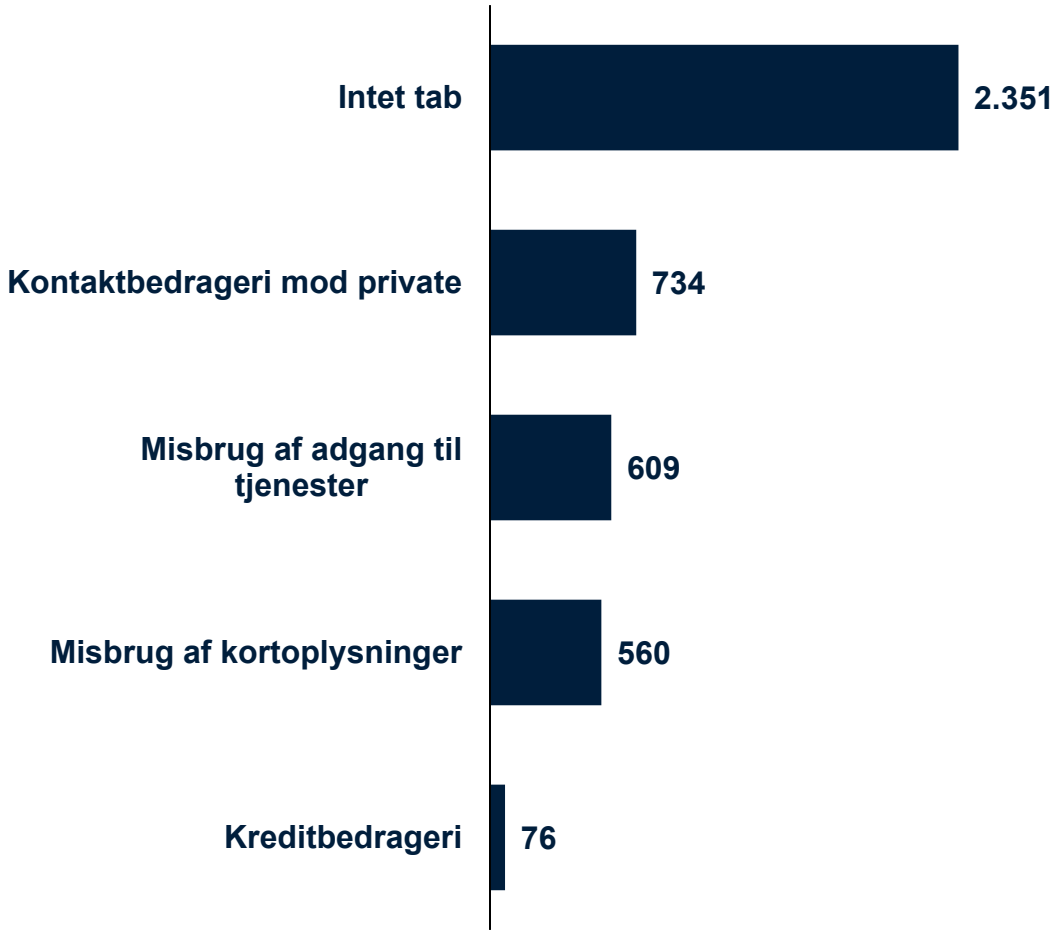
Smishinganmeldelser uden tab
I alt er 3.570 anmeldelser i 2023 udelukkende blevet kategoriseret som smishing uden tab. I denne kategori indgår sager, hvor det ikke har været muligt at fastslå gerningspersonens specifikke mål med beskeden, og hvor forurettede ikke har lidt økonomisk tab som følge af modtagelsen.

Kontakt til den forurettede
Ved smishing som kontaktmodus modtager forurettede en besked fra gerningspersonen, der typisk indeholder links til en falsk webside. På denne side prøver gerningspersonen at lokke kortoplysninger og MitID-oplysninger ud af forurettede.

Anmeldelser i andre kategorier
Anmeldelser med smishing som kontaktmodus, hvor forurettede har lidt et tab indgår i opgørelserne på NCIKs øvrige sagsområder.
Der er ca. 360 sager fordelt på de fire angivne sagsområder, hvor det har været tydeligt, at formålet med smishing eksempelvis har været at misbruge forurettedes kortoplysninger, men hvor forurettede ikke har haft et økonomisk tab.

Læs mere om smishing som modus på side 50.

Vishing: Svindel via telefonopkald



I **45%** af anmeldelserne er der ikke rapporteret tab

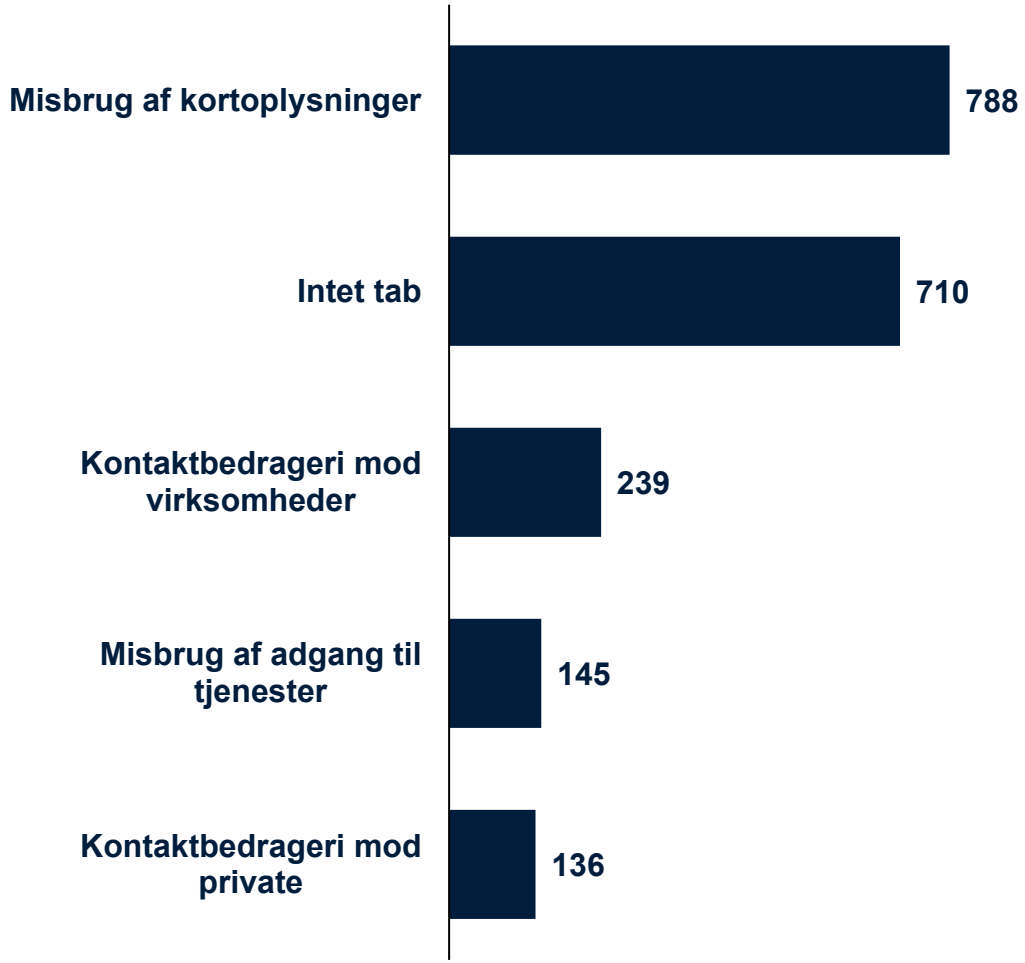
I **55%** af anmeldelserne er der rapporteret tab

Vishinganmeldelser uden rapporteret tab
I alt er 2.351 anmeldelser i 2023 udelukkende blevet kategoriseret som vishing uden tab. I denne kategori indgår sager, hvor det ikke har været muligt at fastslå gerningspersonens specifikke mål med opkaldet, og hvor forurettede ikke har lidt økonomisk tab som følge af opkaldet.

Kontakt til den forurettede
Ved vishing som kontaktmodus modtager forurettede et opkald fra gerningspersonen, der typisk vil være fra et spoofet nummer. På denne måde prøver gerningspersonen fx at lokke forurettede til at logge ind i netbank og flytte penge fra kontoen til en ”sikker” konto, som gerningspersonen råder over.

Anmeldelser i kategorier
Anmeldelser med vishing som kontaktmodus, hvor forurettede har lidt et tab indgår i opgørelserne på NCIKs sagsområder.
Der er ca. 130 sager fordelt på de fire angivne sagsområder, hvor det har været tydeligt, at formålet med opkaldet fx har været at få adgang til forurettedes netbank, men hvor forurettede har afbrudt opkaldet og dermed ikke lidt et økonomisk tab.

Phishing: Svindel via e-mails



I **58%** af anmeldelserne er der ikke rapporteret tab

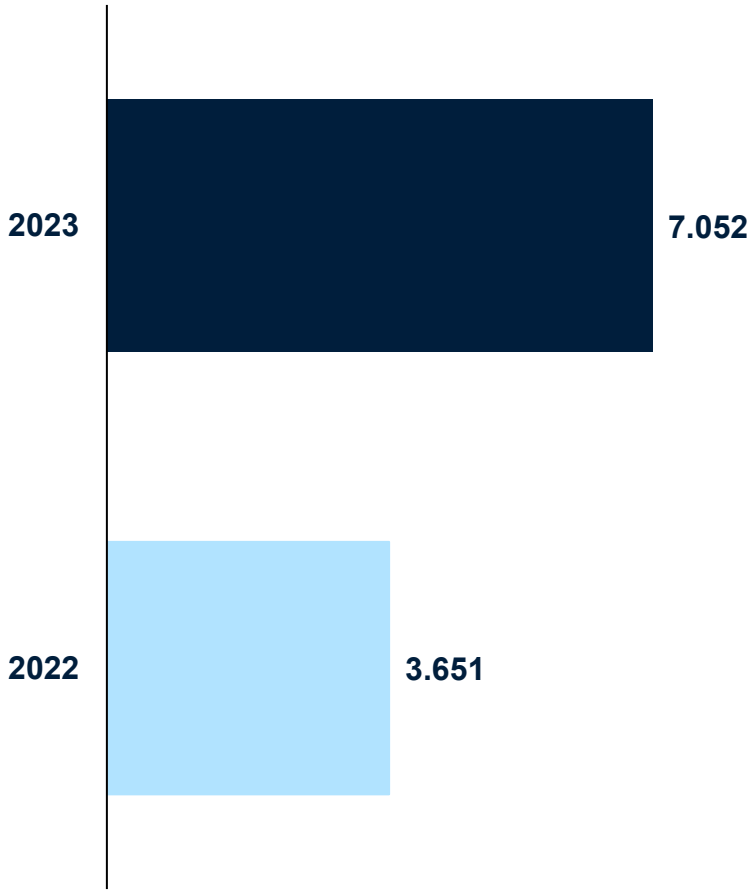
I **42%** af anmeldelserne er der rapporteret tab

Phishinganmeldelser uden rapporteret tab
I alt er 710 anmeldelser udelukkende blevet kategoriseret som phishing uden tab. I denne kategori indgår sager, hvor det ikke har været muligt at fastslå gerningspersonens specifikke mål med e-mailen, og hvor forurettede ikke har lidt økonomisk tab som følge af henvendelsen.

Kontakt til den forurettede
Ved vishing som kontaktmodus modtager forurettede en e-mail fra gerningspersonen, der typisk vil bære præg af at være sendt til mange mennesker på samme tid. På denne måde prøver gerningspersonen fx at lokke forurettede til at tro, at de skal have en refusion fra fx Skat eller Sygesikring Danmark, hvorefter forurettede logger ind på en falsk side og afgiver MitID- eller kortoplysninger.

Anmeldelser i andre kategorier
Anmeldelser med phishing som kontaktmodus, hvor forurettede har lidt et tab indgår i opgørelserne på NCIKs sagsområder.
Der er ca. 180 sager fordelt på de fire angivne sagsområder, hvor det har været tydeligt, at formålet med e-mailen fx har været at få forurettede til at afgive kortoplysninger med henblik på at misbruge disse oplysninger, men hvor der ikke er lidt et økonomisk tab.

Misbrug af MitID



20 procent af alle anmeldelser i 2023 indeholder MitID
I 2023 udgør anmeldelser, der involverer MitID 20 procent af det samlede anmeldelsestal. Dog vurderer NCIK, at dette tal er langt højere end registreret.

Mangelfulde anmeldelsesdata gør det ofte svært at identificere, om der har været misbrugt et MitID-login i sagen, men da det er næsten umuligt at begå indbrud i netbank, misbruge adgang til tjenester eller udføre kontaktbedrageri mod private uden brug af MitID-login, er det NCIKs vurdering, at alle disse sager indeholder elementer af misbrug af MitID.

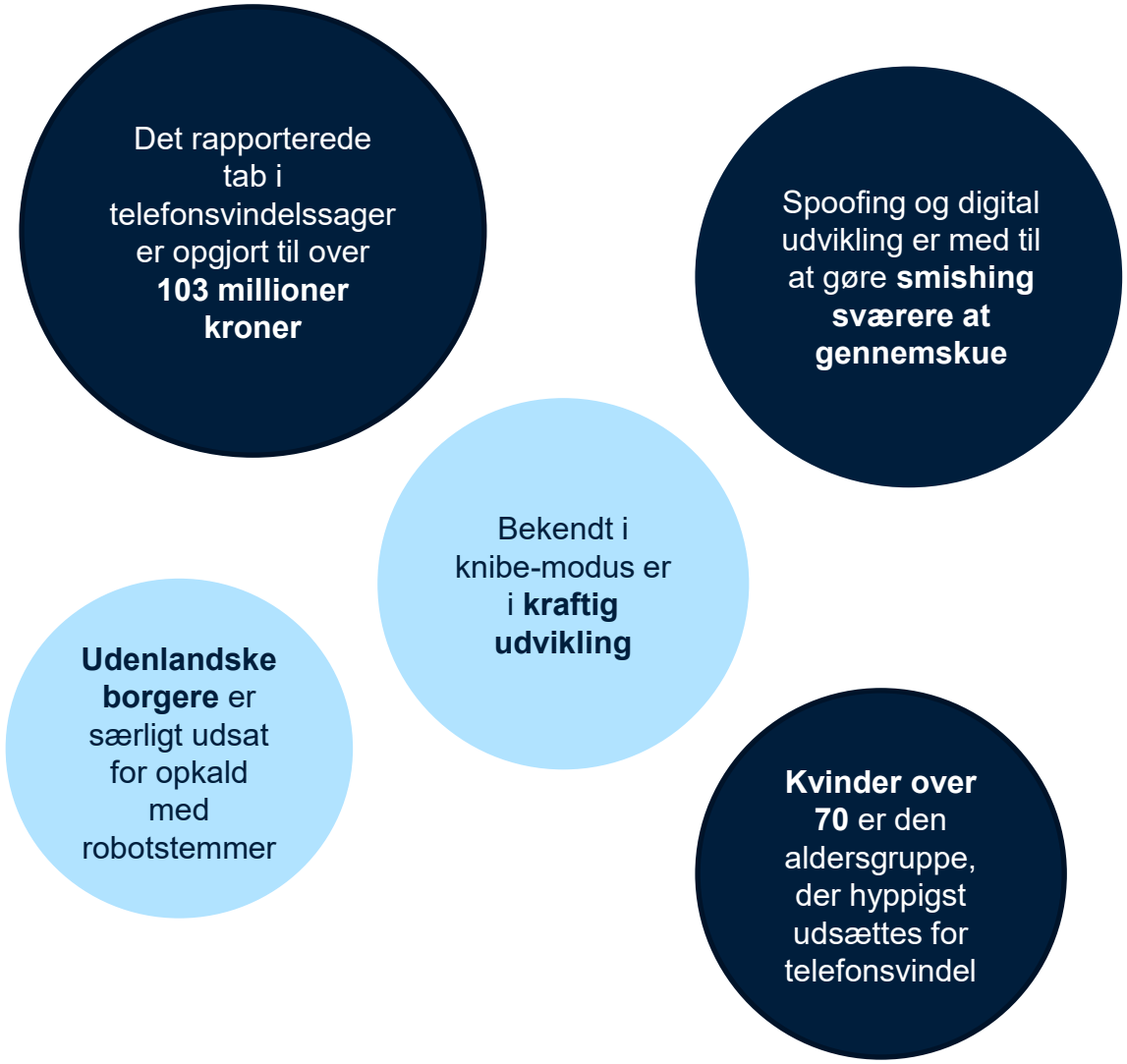
Stigning på 93 procent i forhold til 2022
Det er i forhold til 2022 sket en stigning i antal anmeldelser, der er registreret med kategorien MitID på 93 procent. Stigningen er både et resultat af stigningen i antal anmeldelser om indbrud i netbank, misbrug af adgang til tjenester og kontaktbedrageri mod private og en ændring i NCIKs registreringspraksis.

Base: (35.254) Tabellen er beregnet på forekomsten af ordene MitID og/eller NemID i sagernes resuméfelter og sager registreret under kategorien Phishing, smishing, vishing mfl..

Nedslag i kriminalitetsområdet

POLITI

Nedslag i kriminalitetsområdet



Uddybende perspektiver på kriminalitetsområdet
I årsrapporten foretager NCIK udvalgte nedslag i kriminalitetsområdet, hvor der dykkes dybere ned i specifikke sagsområder, hvorunder der har været en særlig udvikling eller stigninger i anmeldelsestallet.

Disse nedslag giver NCIK mulighed for at formidle nuancer og tendenser inden for bestemte sagsområder, hvilket kan give en forståelse for de dynamikker, der præger situationsbilledet inden for it-relateret økonomisk kriminalitet.

Smishing: Svindel via sms-beskeder

Misbrug af kortoplysninger og indbrud i netbank
Misbrug af kortoplysninger og indbrud i netbank, hvor gerningspersonen har brugt en sms-besked som redskab til at lokke oplysninger ud af den forurettede, udgør en stor del af anmeldelserne, der er registreret med smishing som kontaktmodus. Dette modus foregår typisk ved, at en sms-besked afsendes af gerningspersonen for at lokke forurettede til at afgive kortoplysninger og/eller MitID-oplysninger. Det kan også være oplysninger, der ikke direkte kan bruges til fx at misbruge forurettedes kort, men som senere kan bruges ved telefonsvindel. Det kan fx være oplysninger om forurettedes bankforhold eller navn på forurettedes bankrådgiver. Disse sms-beskeder sendes ofte fra et spoofet telefonnummer, der dermed foregiver at komme fra en troværdig kilde. Derfor lægger svindelbeskederne sig ind i en allerede eksisterende beskedtråd fra eksempelvis en myndighed, et fragtfirma eller forurettedes pengeinstitut.

Et andet udbredt modus er, når svindlere byder på varer på private handelsplatforme og aftaler med sælgeren, at de vil købe varen. Derefter sender gerningspersonen et link til et fragtfirma. Linket leder typisk forurettede til en side, der er designet til at ligne fragtfirmaets eller MitID's loginside, hvorpå forurettede afgiver oplysninger i troen på, at de arrangerer forsendelse eller modtager betaling fra gerningspersonen. Den digitale udvikling har gjort disse beskeder mere overbevisende med færre grammatikfejl og et mere professionelt udseende.

Et modus i kraftig udvikling er bekendt i knibe-scenariet, hvor forurettede modtager en sms-besked fra gerningspersonen, der udgiver sig for at være forurettedes barn og præsenterer en form for krise. Dette kan typisk være, at de har tabt eller fået stjålet deres telefon, og derfor har fået nyt nummer. Efterfølgende anmoder gerningspersonen ofte om penge til at betale for den nye telefon.

Mange bliver ramt
Falske sms-beskeder kan sendes ud til mange borgere på en gang, hvilket øger svindlernes rækkevidde, og chancen for at narre borgerne i et øjebliks uopmærksomhed stiger med hver besked. Aldersfordelingen blandt forurettede i smishinganmeldelserne fordeler sig jævnt mellem 20-70-årige, hvilket betyder, at personer i alle aldersgrupper er sårbare over for svindlen.

Selvom politi, myndigheder og interesseorganisationer løbende informerer om ikke at klikke på links, afspejles disse tiltag tilsyneladende ikke i anmeldelsesstatistikken. NCIK vurderer, at der fortsat er stort behov for strukturel forebyggelse og implementering af tekniske tiltag for at gøre svindel via smishing meget vanskeligere.

Telefonsvindel 1/2

Social engineering-metoder
Telefonsvindel er en form for bedrageri, hvor gerningspersoner tager telefonisk kontakt til forurettede med det formål at manipulere vedkommende til at udlevere personlige oplysninger og kodeord eller overføre større pengebeløb. I sager om telefonsvindel ses ofte brug af social engineering, hvor kriminelle ved hjælp af overtalelsesteknikker forsøger at omgå de sikkerhedsforanstaltninger, der i stigende grad implementeres på nettet.

Social engineering ses blandt andet ved, at gerningspersonen udgiver sig for at være fra forurettedes bank, politiet eller andre myndigheder, som forurettede forventes at have stor tillid til. Herefter vil gerningspersonen eksempelvis fortælle, at forurettedes bankkonto er udsat for et hackerangreb, og at forurettede derfor skal skynde sig at overføre sine penge til en ”sikker” konto, som gerningspersonen råder over.

Gerningspersonerne fremstår imødekommende og hjælpsomme i telefonen, og de har ofte sat sig ind i offerets personlige og økonomiske profil, blandt andet via sociale medier eller onlinetelefonbøger. Opkaldenes troværdighed styrkes endvidere af, at gerningspersonerne i mange tilfælde benytter spoofede telefonnumre, så det i visningen er identisk med eksempelvis forurettedes banks eget telefonnummer.

Store økonomiske og personlige tab
Det totale rapporterede tab i sager med telefonsvindel som modus i 2023 er opgjort til over 103 millioner kroner.

Forurettede er i overvejende grad kvinder i aldersgruppen 70-79 år, og blandt dem er en stor del enker og/eller aleneboende. NCIKs erfaring er, at denne befolkningsgruppe er i større risiko for at lide tab ved telefonsvindel, da de ofte mangler viden om it-sikkerhed samt gatekeepers i form af eksempelvis familiemedlemmer, der kan træde til og rådgive og advare dem om risikoen for telefonsvindel og andre former for it-kriminalitet.

I en kortlægning af kriminalitetsformen ses flest sager med forurettede bosat i Nordsjællands politikreds, og NCIK formoder, det er fordi, de kriminelle går målrettet efter dem, de tror, har flest ressourcer.

Det kan have alvorlige omkostninger at blive udsat for telefonsvindel, økonomisk såvel som personligt. Forurettede fortæller ofte om en følelse af skyld og skam, dels fordi de er blevet udsat for kriminalitet og dels fordi de mener, at de burde have gennemskuet svindlen og manipulationen. Det er vigtigt at pointere, at gerningspersonerne i disse sager ofte er organiserede kriminelle, som er specialiserede i denne type kriminalitet.

Telefonsvindel 2/2

En kriminalitetsform med alvorlige samfundskonsekvenser

Telefonsvindel udgør ligeledes en udfordring i vores skandinaviske nabolande. I Sverige er telefonsvindel udpeget som den største trussel inden for it-relateret kriminalitet med udgangspunkt i den negative effekt, denne kriminalitetsform forventes at have på borgernes generelle tillid til samfundet og dets institutioner (Brå, 2023: 8).

Befolkningens tillid til både andre medborgere og myndigheder er i Danmark kendetegnet ved at være høj. Det er i udpræget grad denne tillid, svindlerne udnytter, ikke mindst når det kommer til den ældre del af befolkningen. Forebyggelse af kontaktbedrageri, der involverer social manipulation gennem social engineering-metoder, vanskeliggøres således af, at vi som mennesker grundlæggende har en antagelse om, at de parter, vi kommunikerer med, fortæller os sandheden (Journal of Language and Social Psychology, 2014: 10).

NCIK betragter ligeledes telefonsvindel som en alvorlig kriminalitetsform og har fortsat et stort forebyggelses- og efterforskningsmæssigt fokus på området.

Et fortsat behov for at styrke borgernes digitale robusthed

En central del af forebyggelse af telefonsvindel er en styrkelse af borgernes kendskab til digital sikkerhed. Dette gør sig især gældende for den gruppe borgere, der betragtes som digitalt udsatte, og derfor er overrepræsenterede i sager om telefonsvindel og andre former for kontaktbedrageri med tab til følge. Blandt den gruppe borgere, der anses som digitalt udsatte, udgør kvinder ca. 60 procent (Algoritmer, Data og Demokrati, 2023). En undersøgelse foretaget af Epinion i februar 2023 for Ældre Sagen viser desuden, at ældre borgere især føler sig utrygge, når digitale handlinger har med penge at gøre (Epinion, 2023:46).

Mangelfuld kendskab til digital sikkerhed er et fællestræk for denne gruppe, og derfor er det nødvendigt med målrettede forebyggelsesindsatser, der kan klæde målgruppen på med relevante og nødvendige redskaber til at undgå digital svindel. Dette indebærer blandt andet en større indsigt i gerningspersonernes metoder - fx brug af social engineering, samt beskyttelse af personlige oplysninger, passwords, etc.

NCIK ser fortsat et behov for forebyggelsesindsatser, men også et behov for at beskytte borgere mod it-relateret økonomisk kriminalitet på et strukturelt niveau, fx ved hjælp af lovændringer eller implementeringer af tekniske løsninger, der hæver den digitale sikkerhed og dermed gør det sværere for kriminelle at få succes.

Robotstemmer

Robotstemme som led i telefonsvindel

NCIK modtog især henover sommeren 2023 en række anmeldelser om telefonsvindel, hvor brugen af robotstemmer var et gennemgående modus. Typisk blev forurettede ringet op af en robotstemme, som udgav sig for at være eksempelvis dansk politi eller Europol. Robotstemmen talte engelsk og fortalte blandt andet, at forurettede var mistænkt i en sag om hvidvask eller lignende, eller at vedkommendes personlige oplysninger var blevet misbrugt. Herefter bad robotstemmen forurettede om at taste 1. Hvis forurettede gjorde dette, blev de enten mødt af en gerningsperson, der udgav sig for at være politibetjent, eller yderligere en robotstemme, som bad forurettede om at indtastede eksempelvis cpr-nummer eller kortoplysninger.

I langt de fleste tilfælde førte svindlen ikke til økonomisk tab eller udlevering af oplysninger. En udfordring ved brugen af robotstemmer er dog blandt andet, at det giver mulighed for at nå ud til mange borgere og hurtigt sortere de fra, som er i stand til at gennemskue svindlen. Derved får gerningspersonen kun direkte kontakt med de borgere, der allerede har tastet 1, og dermed er et trin tættere på at blive svindlet.

Udenlandske borgere er udsatte

I telefonsvindelssager med robotstemme som modus er størstedelen af forurettede mellem 20-40 år, og anmeldelserne fordeler sig forholdsvist ligeligt mellem kønnene. Alder og køn på forurettede adskiller sig således fra andre former for telefonsvindel, hvor særligt ældre kvinder er overrepræsenterede i anmeldelsestallene.

Langt de fleste sager om telefonsvindel med robotstemmer som modus er anmeldt uden tab, og forurettede har derfor ikke afgivet oplysninger eller haft økonomisk tab. I de sager, hvor der er sket et tab, eller hvor forurettede har afgivet personoplysninger, er det primært udenlandske borgere bosat i Danmark, der har anmeldt. Dette kan bero på, at man som ikke-dansktalende i landet ikke har samme forudsætninger for at vide, hvordan politiet i Danmark arbejder.

Denne form for automatisering af telefonopkald har også ramt andre europæiske lande i bølger.

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 2019-2023. Data er frosset 1. januar 2024, 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

Anmeldelser og kontaktmodus

Phishing, smishing, vishing og MitID bliver behandlet som selvstændige modi, der går på tværs af sagsområderne under kategorien ”Phishing, smishing, vishing mfl.”. Det betyder, at forskellige anmeldelser på tværs af alle NCIKs sagsområder kan indeholde én eller flere af disse modi. Nogle sager kan være vanskelige at placere i et sagsområde pga. manglende anmeldelsesinformation, hvorfor sagen udelukkende er kategoriseret under denne kategori.

Under opgørelsen af kontaktmodi phishing, smishing og vishing på side 42 indgår derfor både sager, der udelukkende har denne kategori samt de sager, der også er kategoriseret under et af NCIKs andre sagsområder.

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 2024, men fordi data er dynamiske, betyder det, at data trukket den 1. januar 2024 ikke vil være de samme, som data trukket den 1. januar 2023. 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. Der er tale om et meget begrænset antal sager, hvorfor årsrapportens datagrundlag er begrænset til at omhandle sager med et specifik NCIK-journalnummer.

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 politikredsene og får derved ikke et NCIK-journalnummer. Det betyder, at en sag med mange underforhold kan tælle som 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 2023. 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 over 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 mv..

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 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 2023*

Nordic Journal of Criminology (2023) *Victimization in online gaming-related trade scams: A study among young Danes*

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

Brottsförebyggande Rådet (2023) *Bedrägerier mot privatpersoner: De förebyggande åtgärdernas träffsäkerhet*

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

Epinion (2023) *Befolkningens oplevelser og udfordringer i et digitalt samfund – med fokus på ældre*

Algoritmer, Data og Demokrati (2023) *Algoritmer.org/befolkningsundersoegelse/forside/2023-2/borgernes-digitale-kompetencer/*

NCIK
NATIONALT CENTER FOR IT-KRIMINALITET

POLITI

NCIK årsrapport 2023