DIGITALISERINGSSTYRELSEN

Omfang af identitetstyveri af NemID og svindel med NemKonto afledt heraf

Juni 2022

2022

Indhold

Indledning

1. Indledning

Indledningsvist introduceres rapportens formål og metodiske tilgang. Der gives også et resumé af rapportens hovedbudskaber.

1.1 Introduktion og formål

Folketinget har i forbindelse med behandling af spørgsmål om identitetstyveri af NemID og svindel med NemKonto efterspurgt bedre og bredere viden om omfanget af svindel med disse to digitale løsninger.

Denne rapport har til formål at formidle den viden vi i dag har om omfanget af identitetstyveri af NemID og svindel med NemKonto afledt heraf. Da denne type svindel ofte indgår i en kompleks sammenhæng med andre svindelformer og –metoder, søger rapporten af give et nuanceret indblik i området på tværs af centrale aktører. Der tilstræbes også at formidle viden, som kan bidrage til at minimere svindel på området yderligere. Derfor er fokus både rettet mod omfang, men også forskellige svindelformer, observerede ændringer i svindelmetoder samt sikkerhedstiltag der kan minimere svindel på området yderligere.

1.2 Afgrænsning og metode

Afgrænsning

Rapporten fokuserer på identitetstyveri af NemID og svindel med NemKonto afledt heraf. Da MitID først blev lanceret i oktober 2021, og fortsat er under implementering ved udarbejdelsen af denne rapport, indgår information om eventuel identitetstyveri af MitID ikke i rapporten. Opgørelser, der refereres til undervejs, indeholder ligeledes ikke data om MitID. Dataindsamling til rapporten er foretaget i perioden december 2021 til februar 2022.

Kapitel 4, som vedrører tiltag, der kan bidrage til at minimere svindel på området yderligere, dækker perioden frem til udgangen af maj. Dette for at favne de tiltag, der er blevet iværksat efter rapportens dataindsamlingsperiode.

Metode

Der findes ikke ensartede og fyldestgørende opgørelser og information, som er velegnet til at beskrive omfanget af identitetstyveri med NemID og svindel med NemKonto. Det skyldes, at områdets aktører har forskellige opgørelsesmetoder og opgørelsesenheder på grund af forskellige forretningsbehov, som blandt andet udspringer af forskellige juridiske indberetningspligter.

Hertil bør det nævnes, at det hidtil ikke har været alle former for identitetstyveri, som er strafbart efter straffeloven (Justitsministeriet (A) 2021). Dette har blandt andet gjort det vanskeligt for politiet at kortlægge det fulde omfang. Folketinget

har dog for nyligt besluttet at kriminalisere alle former for identitetstyveri (Folketinget 2021-22). Derudover har politiet pr. 1. januar 2022 indført to nye søgenøgler på NemID og MitID. Disse kan på sigt bidrage til bedre at kunne kortlægge omfanget af identitetstyveri, da politiet via disse søgenøgler kan udtrække relevante anmeldelser fra sagsbehandlingssystemet.

Det er desuden ikke muligt at adskille identitetstyveri af NemID og svindel med NemKonto fuldstændigt fra andre former for it-relateret kriminalitet. For at favne kompleksiteten på området, og samtidig opnå bedst mulig viden om svindel med de to specifikke digitale løsninger, er der dels indsamlet viden fra et samarbejde med Finans Danmark, Finans & Leasing og Rigspolitiet og dels gennemgået relevante undersøgelser og rapporter på området. En stor del af rapportens fund baserer sig desuden på opgørelser af politianmeldelser fra Nationalt Center for It-Kriminalitet og seneste offerundersøgelse fra Justitsministeriet. Disse kilder supplerer hinanden ved, at den ene bidrager med potentielt relevante politianmeldelser på området og den anden befolkningens oplevelse af potentielt relevant it-kriminalitet, som ikke nødvendigvis er blevet anmeldt.

Den metodiske tilgang er derfor baseret på research i eksisterende undersøgelser og rapporter - kombineret med kvalitativ viden og kvantitative øjebliksbilleder af deskriptiv karakter fra omtalte samarbejde. Metode er uddybet yderligere i bilag 1.

Finans Danmark, Finans & Leasing og Rigspolitiet/National enhed for Særlig Kriminalitet har valideret rapportens indhold undervejs.

1.3 Resumé af hovedkonklusioner

Det er ikke muligt at give et nøjagtigt estimat for omfanget af identitetstyveri af NemID og svindel med NemKonto på grund af forskellig registreringspraksis og metodiske usikkerheder ved sammenligning af eksisterende data.

Det samlede overblik tilvejebragt i rapporten peger dog på, at en meget lille andel, af de millioner som anvender NemID og NemKonto, rammes af identitetstyveri af NemID - og endnu færre udsættes også for svindel med NemKonto. Det kan dog have store konsekvenser, for de som rammes, hvorfor alle tilfælde tages meget alvorligt. Digitaliseringsstyrelsens Hotline ved identitetstyveri yder i den forbindelse døgnrådgivning og vejledning, og et lovforslag om en kompensationsordningen ved svindel med NemKonto er pt. under behandling i Folketinget for at sikre, at ofre for svindel med NemKonto ikke risikerer at hæfte økonomisk.

Derudover har Digitaliseringsstyrelsen i april 2021 indført et fysisk aktiveringsbrev ved forsøg på at ændre NemKonto i selvbetjeningsløsningen. Dette opleves at have mindsket svindel med NemKonto. Ydermere undersøges potentielle tiltag for at begrænse muligheden for at anvise NemKonto til en tredjemand. Endeligt forbedres sikkerheden med MitID på flere parametre, som skal beskytte borgerne endnu bedre mod identitetstyveri.

Indførsel af kravet om to-faktor autentifikation ved elektroniske betalinger fra januar 2021 har gjort det sværere at misbruge betalingskortoplysninger. Misbrug med danske betalingskort er reduceret med ca. 44 pct. siden 2016. Kravet har dog også skabt et øget behov blandt kriminelle for at erhverve sig borgeres NemID til at omgå to-faktor autentifikationen, men det er affødt af en positiv udvikling med mindre kriminalitet på andre områder.

Det øgede behov for at benytte sig af NemID til at begå identitetstyveri har muligvis ført til en udvikling i forskellige svindelmetoder. Der opleves især en udvikling inden for tilgangen "social engineering", hvor svindlere via e-mail, sms eller telefonopkald udgiver sig for at være eksempelvis en myndighed, som offeret har tillid til. I mange svindeltilfælde foretages ikke decideret identitetstyveri af NemID. I stedet manipuleres ofre eksempelvis til selv at logge ind i netbank og godkende en transaktion til svindleren med sit NemID. I andre tilfælde narres borgere til at udlevere person- og NemID loginoplysninger, hvorefter svindleren ved decideret identitetstyveri eksempelvis opretter forbrugslån i offerets identitet. I visse tilfælde benyttes identitetstyveriet også til at omdirigere offerets NemKonto til en tredjemands bankkonto.

Handlingsanvisende informationskampagner er vigtige, da svindlen ikke skyldes tekniske mangler ved NemID systemet, men kortvarig uopmærksomhed eller manglende viden om eksempelvis aldrig at udlevere sine NemID oplysninger via e-mail, sms eller over telefonen. Derudover er det vigtigt, at centrale aktører samarbejder på området, for dels at få bedre viden om omfanget løbende samt for at kunne vidensdele og bekæmpe konkrete svindeltendenser sammen.

Digitalisering i udvik-
ling

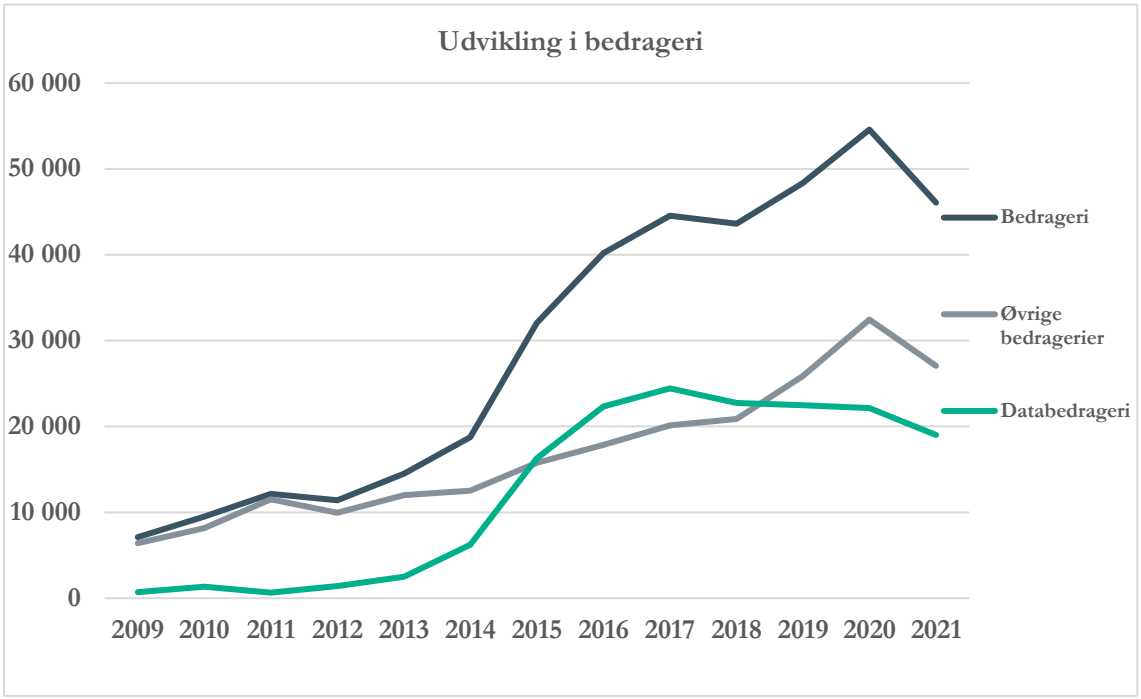
2. Digitalisering i udvikling

Kapitlet beskriver udviklingen i borgernes digitale adfærd og it-relateret kriminalitet. Kapitlet skal bidrage til at forstå grundlaget for potentielt identitetstyveri af NemID og svindel med NemKonto.

2.1 Digital handel i vækst

Digitale bookingsystemer, flytteanmeldelser, internethandel og meget mere har i dag gjort vores hverdag lettere og mere digital. Tre ud af fire danskere havde i 2019 handlet på internettet inden for de seneste tre måneder. I årtiet fra 2009 til 2019 steg andelen af danskere med dette handelsmønster fra 50 pct. til 74 pct. (Danmarks Statistik (A) 2019). Seneste opgørelse fra Eurostat viser desuden, at Danmark i 2019 var det næstmest internethandlende land i EU – kun overgået af Irland (Eurostat 2021). Samtidig med at flere handler online, køber vi også flere forskellige produkter online, hvilket bidrager yderligere til væksten i internethandlen (Danmarks Statistik (A) 2019). Ydermere har det ændrede adfærdsmønster under Covid-19 nedlukning bidraget til yderligere vækst i internethandlen i 2020 (Digitaliseringsstyrelsen et al., 2020, s. 5, Dansk Erhverv, 2020). Endeligt slår Danmark også europæisk rekord i brug af internettet blandt de 65-74-årige (Danmarks Statistik (B) 2019). Ligeledes er det blandt de 75-89-årige, at der ses den største vækst i forhold til flest nye online købere - med tre gange så mange som i 2011 (Danmarks Statistik (C) 2020, s. 18).

Der er store fordele ved, at Danmark er frontløber inden for internethandel og ikke mindst offentlig digitalisering. Udviklingen medfører dog også, at flere er i risiko for at opleve it-relateret kriminalitet. Siden 2009 er der generelt set en stigning i databedrageri, som blandt andet omfatter svindel på internettet med stjålne kortoplysninger (Danmarks Statistik (D) 2020). Dette er umiddelbart naturligt i lyset af, at der i samme periode er sket en markant vækst i internethandlen. Dog viser nyeste tal i nedenstående kurve, at der siden 2017 har været en let faldende tendens inden for databedrageri (Danmarks Statistik (E) 2022). Denne udvikling skal sammenholdes med en fortsat vækst i internethandlen i perioden (Danmarks Statistik (C) 2020, s. 18).



Figur 1. Udvikling i bedrageri. Kilde: Danmarks Statistik (E) 2022.

De fleste forsøg på svindel mislykkes

De fleste har på trods af spamfiltre prøvet af åbne en mistænkelig mail, eller åbnet en svigagtig mail uden at opdage det, men de færreste er heldigvis blevet narret af det. Ifølge en undersøgelse af Megafon A/S i 2020 oplevede og opdagede 64 pct. af danskerne i alderen 18-74 år at blive udsat for forsøg på phishing via enten e-mail, sms (smishing) eller telefon (vishing) inden for det seneste år. Heldigvis havde kun 2 pct. af respondenterne udleveret de efterspurgte oplysninger (Digitaliseringsstyrelsen et al. 2020, s. 12-13). Denne ageren tyder på, at borgerne er forholdsvis vant til at modtage forsøg på phishing, og at størstedelen af forsøgene gennemskues (ibid.).

Det store spænd mellem antallet der oplever forsøg på phishing, smishing eller vishing, og antallet der har udleveret oplysninger, indikerer desuden, at svindlere ofte benytter en strategi, hvor de sigter efter mange for blot at ramme få (ibid.). Nationalt Center for It-Kriminalitet (fremover NCIK[1]) bemærker dog, at dette primært er strategien bag phishing og smishing. Ved vishing vurderer de, at der typisk er en mere målrettet tilgang mod udvalgte individer, såsom ældre borgere, og politiet vurderer, at der er større risiko for at svindlen lykkes her end via e-mail og sms.

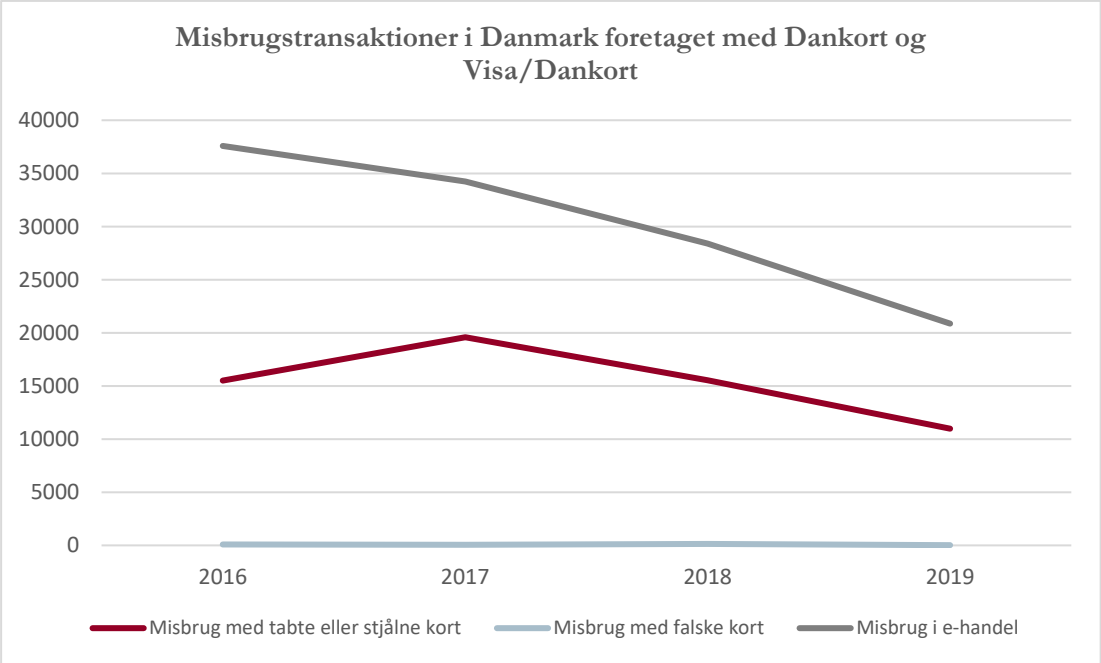
[1] Fremgår dog af flere kilderhenvisninger som LCIK på grund af nylig navneændring fra Landsdækkende Center for It-relateret økonomisk Kriminalitet til Nationalt Center for It-Kriminalitet.

2.2 Mindre svindel med betalingskort

I lyset af den omfattende vækst i internet-handel er det en forholdsvis lille andel, som oplever misbrug af deres kredit- eller dankort. For hver million transaktioner med Dankort og Visa/Dankort, i danske internetforretninger i 2019, er der registreret 103 misbrugstransaktioner – svarende til 0,1 promille (Konkurrence- og Forbrugerstyrelsen 2020, s. 35). Flere kilder peger desuden entydigt på en markant nedgang i svindel med betalingskort. En analyse fra Danmarks Nationalbank finder, at misbrug med danske betalingskort er reduceret med 44 pct. siden første opgørelse i 2016 (Danmarks Nationalbank 2020, s. 1 & Finans Danmark (D) 2022). Derudover har Dankort og Visa/Dankort sammenlignet med internationale kreditkort færrest misbrugstransaktioner (Konkurrence- og Forbrugerstyrelsen 2020, s. 36-37).

Tilfælde af misbrugstransaktioner forekommer i højere grad ved internethandel end ved fysisk handel (ibid.). Konkurrence- og Forbrugerstyrelsen vurderer, at det blandt andet skyldes, at det kan afskrække den kriminelle at være fysisk til stede og risikere at blive set, samt at indførslen af kontaktløs betaling har gjort det vanskeligt at aflure borgeres pinkoder (ibid. s. 34, 39). Uden pinkode er det meget begrænsede beløb, der kan svindles for pr. betaling med fysiske betalingskort.

Nedenstående figur 2 illustrerer, at antallet af misbrugstransaktioner i Danmark foretaget med Dankort og Visa/Dankort er faldet fra 2016 til 2019. Misbruget i internet-handlen er faldet mest



Figur 2. Misbrugstransaktioner i Danmark foretaget med Dankort og Visa/Dankort. Kilde: Konkurrence- og forbrugerstyrelsen 2020, s. 35

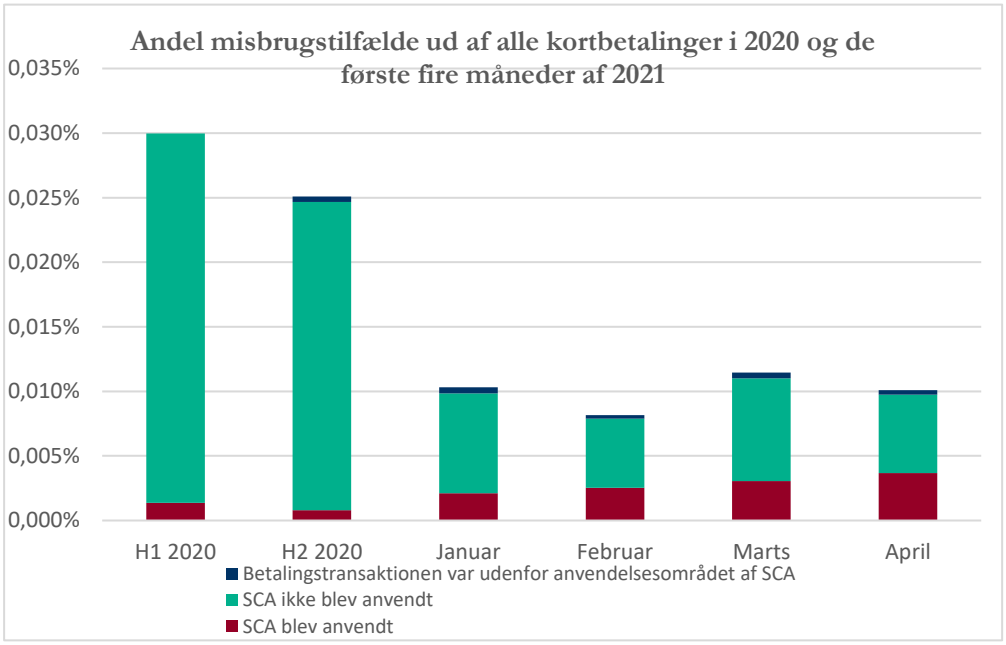
Der ses således en positiv udvikling med mindre misbrug af betalingskortoplysninger over de seneste år.

To-faktor autentifikation bidrager til mindre svindel, men øget pres på svindel med NemID
Flere faktorer har gjort det sværere at misbruge fysiske betalingskort og kortoplysninger til internethandel. De faktorer, som skønnes at have haft størst indflydelse herpå, er:

- **Indførsel af to-faktor autentifikation**
  Det reviderede betalingstjenestedirektiv (PSD2) har indført krav om stærk kundeautentifikation (SCA), også kaldet to-faktor autentifikation, ved alle elektroniske betalinger i forbindelse med både fysisk og online handel. Kravet trådte i kraft i september 2019 med en forlænget implementeringsperiode frem til januar 2021 - og skønnes af Finanstilsynet først at være blevet bredt implementeret fra januar 2021. SCA indebærer, at betaleren skal benytte mindst to faktorer til at godkende en betaling. Typisk i kombinationen med noget vedkommende ved, eksempelvis et password, samt noget vedkommende har, eksempelvis en mobil, der kan modtage en smskode eller en NemID-nøgleapp/-nøgleviser, eller noget vedkommende er - såsom et fingeraftryk (Finanstilsynet 2021, s. 3). Finanstilsynet anslår, at der i ca. 95 pct. af tilfældene anvendes NemID i verifikationsprocessen. Den resterende del er udført med et password og en sms engangskode (ibid. s. 8).
- **Kontaktløse betalingskort**
  Den markante nedgang siden 2016 formodes også at være relateret til implementeringen af kontaktløs betaling (Danmarks Nationalbank 2020, s. 11). Det har tidligere været udbredt blandt kriminelle at aflure pinkode og efterfølgende stjæle betalingskortet, hvorfor betaling uden indtastning af pinkode har medført en markant nedgang i dankort-tyveri (Nets 2019). Derudover er der ved kontaktløs betaling en beløbsgrænse på 350 kr., som begrænser beløbet, der kan svindles med, inden der er behov for at kende pinkoden (Danmarks Nationalbank 2020, s. 11).
- **Alarmeringssystemer**
  Flere banker har indført alarmeringssystemer, så et betalingskort automatisk lukkes, hvis der registreres usædvanlige transaktionsmønstre. Dette bidrager ligeledes til at forhindre misbrug af betalingskort (Finans Danmark (D) 2022). Brug af risikodata udbredes mere og mere, og ses blandt andet også som et af de sikkerhedstiltag, der indgår i MitID.

Der er således blevet sværere at svindle med både fysiske dankort og i internethandel med betalingskortoplysninger alene. Der formodes dermed at være et øget behov blandt kriminelle for at erhverve sig borgernes NemID, men det er affødt af en positiv udvikling i sikkerhedstiltag, som overordnet bidrager til mindre kriminalitet.

Finanstilsynet har undersøgt effekten af to-faktor autentifikation (SCA) ved kortbetalinger i internethandlen i perioden efter fuld implementering fra den 11. januar til den 30. april 2021. Udviklingen fremgår af nedenstående søjlediagram.



Figur 3: Misbrugstilfælde ud af alle kortbetalinger. Kilde: Finanstilsynet 2021, s. 5

Sammenlignet med første halvår af 2020 er tilfælde med misbrug af betalingskort faldet med ca. to tredjedele i den udvalgte stikprøve for 2021 (Finanstilsynet 2021, s. 5-6). Det ses i figur 3, da andelen af misbrugstilfælde med kortbetalinger i første halvår af 2020 udgør ca. 0,03 pct. af alle kortbetalinger, hvorimod det tilsvarende niveau de første fire måneder af 2021 ligger på ca. 0,01 pct. Det ses samtidigt, at andelen af svindeltilfælde, hvor to-faktor autentifikation er benyttet, er steget i 2021 - om end denne andel fortsat udgør mindre en 0,005 pct. af alle kortbetalinger. Det skyldes formentlig, at det i mindre grad er muligt at handle uden to-faktor autentifikation, hvorfor misbrugstilfælde alt andet lige oftere vil involvere dette, samt at svindlere er nødsaget til at udvikle nye metoder til at omgå to-faktor autentifikationen, da det er blevet sværere at svindle på anden vis (ibid.)

Der er således samlet set tale om en positiv udvikling med mindre svindel, men på bekostning af, at flere kriminelle vil have interesse i at tilegne sig borgernes NemID oplysninger – eller andre muligheder for at omgå to-faktor autentifikationen.

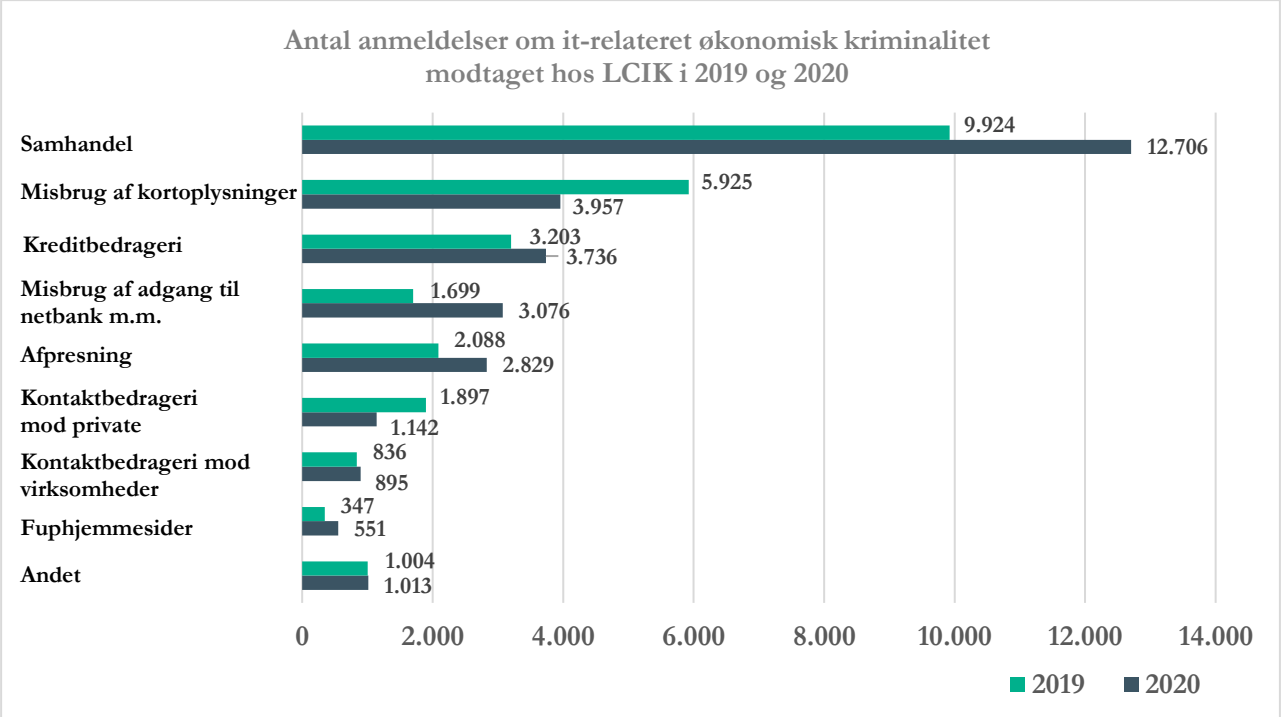
Det bemærkes desuden fra Finanstilsynets opgørelser, at svindel med betalingskort kun i meget lille grad knyttes til situationer med social engineering. Dette uddybes i afsnit 3.6.

2.3 Fordeling af it-relateret kriminalitet

I dette afsnit udfoldes kilder fra henholdsvis Rigspolitiet og Justitsministeriet. Disse supplerer hinanden med viden om forhold, der potentielt kan være relateret til identitetstyveri af NemID og svindel med NemKonto. De kan ikke sammenlignes direkte, da politiets tal tager udgangspunkt i politianmeldelser – som både kan være relateret til reelt misbrug/kriminalitet, men også til mislykkede forsøg herpå. Derimod belyser Justitsministeriets offerundersøgelse befolkningens

oplevelse af at have været være udsat for it-relateret kriminalitet, eksklusiv forsøg herpå. Flere af disse oplevelser vil ikke være politianmeldte. Samtidigt er det dog naturligt at formode, at oplevelser, som vedrører identitetstyveri af NemID og svindel med NemKonto, betragtes som så alvorlige, at de typisk anmeldes til politiet. Begge kilder indeholder desuden anmeldelser eller oplevelser, som ikke er relateret til identitetstyveri af NemID og svindel med NemKonto. Der er foretaget en kvalitativ vurdering af de potientielt mest relevante datakategorier sammen med henholdsvis National enhed for Særlig Kriminalitet og forfatterne bag Justitisministeriets offerundersøgelse – dette uddybes løbende.

Viden fra Rigspolitiet om it-relateret økonomisk kriminalitet
NCIK modtog i 2020 29.905 anmeldelser om it-relateret økonomisk kriminalitet, fordelt på 23.764 unikke forurettede borgere, hvilket svarer til ca. 0,4 pct. af befolkningen (LCIK 2021, s. 62, 67). Nedenstående søjlediagram viser en prioriteret fordeling efter antal anmeldelser i 2019 og 2020. Det bemærkes, at kategorien "Samhandel" udgør over 42 pct., men kategorien omfatter primært handel mellem private parter via fx dba.dk, Facebook og falske webshops, som sjældent har NemID autentifikation ved betaling, hvorfor svindel med NemID og NemKonto sjældent vil være relevant i denne sammenhæng.



Figur 4: Antal anmeldelser om it-relateret økonomisk kriminalitet i 2019 og 2020. Kilde: LCIK årsrapport 2020, s. 10

Anmeldelseskategorierne i figur 4 er vurderet for relevans i forhold til identitetstyveri af NemID i samarbejde med National enhed for Særlig Kriminalitet. De vurderer, at anmeldelseskategorierne "Kreditbedrageri" og "Misbrug af adgang til netbank m.m." er de mest relevante, da anmeldelserne i disse kategorier i høj grad

vurderes relateret til identitetstyveri af NemID. De to kategorier indeholder dog også anmeldelser, som ikke nødvendigvis relaterer hertil, samt anmeldelser om forsøg på identitetstyveri af NemID, men ikke reelt misbrug. Derudover vurderer politiet, at kategorien "Kontaktbedrageri mod private" ikke er relevant for decideret identitetstyveri, men kan indebære, at en borger kontaktes og forsøges narret, eller bliver narret, til selv at gennemføre en svigagtig overførsel. Selvom dette ikke omhandler decideret identitetstyveri af NemID, vurderes kategorien relevant at belyse, da borgere narres til benytte sine NemID oplysninger til svindlerens fordel. Der kan også være tilfælde heri, hvor borgeren er blevet lokket til at udlevere sine oplysninger og udsat for decideret identitetstyveri. Politiet vurderer dog, at dette udgør et fåtal.

Disse tre kategorier udgør i 2020 tilsammen knap 8.000 anmeldelser[2]. Endeligt er kategorien "Misbrug af kortoplysninger", med knap 4.000 anmeldelser[3], ifølge National enhed for Særlig Kriminalitet i mindre grad relevant for omfanget af identitetstyveri af NemID. Der kan dog være anmeldelser heri, hvor et NemID har været misbrugt til at omgå to-faktor autentifikationen ved betaling med misbrugte kortoplysninger.

Det bemærkes desuden til figur 4, at "Misbrug af adgang til netbank mm." stiger mest og markant fra 2019 til 2020. Det sker samtidigt med det største og markante fald i "Misbrug af kortoplysninger". Jf. afsnit 2.2. kan dette muligvis skyldes den begyndende implementering af kravet om to-faktor autentifikation i 2019, som har gjort det sværere at misbruge kortoplysninger uden at anskaffe sig adgang til borgeres NemID og NemID login-oplysninger. Hvis de kriminelle i den forbindelse får uberettiget adgang til en borgers NemID, er det alt andet lige mere fordelagtigt for dem at svindle sig til et stort pengebeløb ved netbankssvindel end ved at handle varer på nettet med andres betalingskortoplysninger.

Ovenstående gennemgang indikerer, at op mod 8.000 - 12.000 anmeldelser i 2020 i et vist omfang kan være relateret til identitetstyveri af NemID eller forsøg herpå. Tallene omfatter dog også anmeldelser, som ikke er NemID-relaterede. Derudover bør det bemærkes, at ovenstående tal belyser antal anmeldelser og ikke antal borgere, da den samme borger kan optræde blandt flere af anmeldelserne og på tværs af kategorierne.

Specifik viden om NemID fra Rigspolitiet
Nationalt Efterforskningscenter har i 2021 udgivet en temarapport med titlen "Uretmæssig adgang til NemID". Den havde til hensigt specifikt at kortlægge omfanget af politianmeldelser i perioden 2017-2020, hvor gerningspersonen har forsøgt at få uretmæssig adgang til og/eller har misbrugt andre personers NemID.

---

[2] Total antal anmeldelser i 2020 for "kreditbedrageri", "misbrug af adgang til netbank m.m." og "kontaktbedrageri mod private": 3.736 + 3.076 + 1.142 = 7.954 anmeldelser
[3] I 2020 var der 3.957 anmeldelser om misbrug af kontaktoplysninger.

Rigspolitiet har bekræftet, at der er mange metodiske forbehold knyttet til temaundersøgelsen. Eksempelvis er alle anmeldelser inkluderet, som er fremkommet efter en "NemID-autokategorisering", trods at flere ved manuel gennemgang ikke vedrørte misbrug af NemID, men blot indeholdte ordet "NemID" (NEC 2021, s. 3-4). Til gengæld belyser undersøgelsen identitetstyveri af NemID mere specifikt end NCIKs samlede anmeldelser for it-relateret økonomisk kriminalitet, hvorfor undersøgelsen her udfoldes trods de metodiske forbehold.

Temaundersøgelsen beskriver følgende fordeling af politianmeldelser om forsøg på uberettiget tilegnelse eller identitetstyveri af NemID:

- 2017: 3012 politianmeldelser
- 2018: 2795 politianmeldelser
- 2019: 3645 politianmeldelser
- 2020: 9172 politianmeldelser

Rapporten fremhæver, at stigningen i anmeldelsestallet kan skyldes flere faktorer. Dels formodes implementeringen af tidligere omtalte krav til to-faktor autentifikation ved alle elektroniske betalinger, at have påvirket stigningen fra 2019 til 2020 (ibid. s. 5-6). Hertil bør det dog bemærkes, at Finanstilsynet primært finder denne effekt fra 2021 jf. afsnit 2.2. Dels formodes Covid-19 at have bidraget til en stigning, da befolkningens øgede tilstedeværelse i hjemmet har bidraget til at forskubbe fysisk berigelseskriminalitet til kriminalitet på internettet (ibid.). Desuden oprettede politiet ved udgangen af 2018 enheden Landsdækkende Center for It-relateret økonomisk Kriminalitet (som i dag hedder Nationalt Center for It-relateret Kriminalitet/NCIK). Dette medførte en ændret og mere detaljeret registreringspraksis, hvorfor stigningen i data også kan skyldes dette (NEC 2021, s. 7).

Rigspolitiet har desuden oplyst, at de fremlagte data er dynamiske, hvorfor anmeldelsestallene løbende kan stige bagudrettet. Det forekommer eksempelvis, hvis en efterforskning af en anmeldelse senere fører til kendskab til yderligere forurettede, som derfor efterregistreres. Derudover er antal anmeldelser ikke ensbetydende med antal forurettede eller efterforskninger. Én person kan optræde som forurettet flere gange, og én efterforskning kan indeholde anmeldelser fra flere ofre. Eksempelvis var 2800 af anmeldelserne i 2020 knyttet til to konkrete efterforskninger. Det bør også understreges, at anmeldelserne både repræsenterer identitetstyveri af NemID, men også forsøg herpå som kan være mislykket – hvorfor der i disse tilfælde ikke vil være tale om decideret identitetstyveri af NemID.

Endeligt konkluderer rapporten, at uretmæssig tilegnelse af NemID ikke skyldes tekniske mangler ved NemID-systemet, men snarere ofres uopmærksomhed og manglende viden (ibid. s. 11). Dette uddybes nærmere i kapitel 3.

Rigspolitiets viden om svindel med NemKonto
Rigspolitiet har ikke mulighed for præcist at kortlægge hvor mange ofre for identitetstyveri af NemID, der også udsættes for svindel med NemKonto. I et

svar til Retsudvalget i juni 2021 fra finansministeren fremgår det dog, at Rigspolitiet på baggrund af en søgning i politiets sagsbehandlersystem estimerer, at de i 2019 og 2020 modtog ca. 200 anmeldelser årligt i relation til svindel med NemKonto (Finansministeriet 2021). Antallet er fremkommet ved søgning på forskellige variationer af ordet NemKonto på tværs af sagers resumé, og kan derfor være behæftet med en vis usikkerhed om, hvorvidt der reelt er tale om svindel med NemKonto, eller blot forsøg herpå eller andre årsager til at NemKonto fremgår af en sags resumé. Det er desuden vigtigt at pointere, at de 200 anmeldelser ikke repræsenterer 200 unikke borgere, da én borger, som har oplevet svindel med NemKonto, sagtens kan have anmeldt flere forhold. Uagtet dette er antallet væsentligt mindre end antallet af politianmeldelser, som kan være knyttet til identitetstyveri af NemID.

Viden fra Justitsministeriets offerundersøgelse
Justitsministeriets offerundersøgelse er et relevant supplement til opgørelserne af politianmeldelser, da man her på befolkningsniveau afdækker oplevelsen af at være udsat for kriminalitet begået på internettet. Dette kan bidrage til et bredere perspektiv, end vi kan få fra politianmeldelserne, da der kan være it-relateret kriminalitet, som ikke anmeldes. Dette fremgår også at Justitsministeriets offerundersøgelse, som desuden forklarer, at det eksempelvis kan skyldes, at borgeren ikke anser hændelsen for at være kriminel eller alvorlig nok - eller hvis ofret selv helt eller delvist har dækket det økonomiske tab (Justitsministeriet (B) 2021, s. 133). I lyset af dette rationale kan man dog formode, at forhold der vedrører identitetstyveri af NemID eller svindel med NemKonto formentligt ofte anmeldes, da disse handlinger er meget alvorlige.

Data fra Justitsministeriets offerundersøgelse belyser således alene respondentens oplevelse, som ikke nødvendigvis er overensstemmende med de juridiske afgrænsninger for kriminalitet. Desuden anvender LCIKs årsopgørelse og Justitsministeriets offerundersøgelse ikke samme opgørelsesmetode og afgrænsning af kriminalitet begået på internettet, hvorfor de to kilder ikke er velegnede til direkte sammenligning.

Nedenstående tabel viser fordelingen af oplevelser af at have været udsat for kriminalitet begået på internettet inden for det seneste år. Respondenterne er adspurgt i løbet af 2020. Dataindsamlingen bag undersøgelsen er gennemført som led i Danmarks Statistiks undersøgelser af flere emner - og beror på 13.255 respondenter ud af deres samlede stikprøve på 25.122 tilfældigt udvalgte i alderen 16-74 år (Justitsministeriet (B) 2021, s. 11-12). Tallene er ekslusiv forsøg på svindel. Endeligt kan en respondent i undersøgelsen have oplevet kriminalitet flere gange inden for det seneste år. Dog angiver 55 pct. kun af have oplevet kriminalitet én gang (ibid. s. 128). Det betyder dog, at ét offer kan optræde i flere af kategorierne. Estimaterne bør læses med disse forbehold:

Ofre for kriminalitet begået på internettet, eksklusiv forsøg, 2020, fordelt efter type af kriminalitet				
Type	**Andel**	**95 % sikkerhedsin-terval**	**Estimeret antal ofre**	**95 % sikkerhedsin-terval**
Misbrug af betalingskortoplysninger	2,3 %	(2,1 – 2,6 %)	100.200	(87.000 – 111.000)
Samhandel på internettet	1,4 %.	(1,2 – 1,6 %)	60.700	(52.000 69.000)
Kontaktbedrager (dvs. overført penge til en person, som viste sig at være en bedrager)	0,3 %	(0,2 – 0,4 %)	14.500	(10.000 – 18.000)
Misbrug af personoplysninger	0,4 %	(0,3 – 0,5 %)	17.200	(13.000 – 22.000)
Hadefulde ytringer	0,5 %	(0,4 – 0,6 %)	21.100	(16.000 – 26.000)

Tabel 1: Ofre for kriminalitet begået på internettet.. Kilde: Justitsministeriet (B), december 2021. s. 127.

Samhandel på internettet dækker i Justitsministeriets offerundersøgelse, at man ikke har modtaget en betalt vare eller har modtaget en kopivare - eksempelvis efter private handler på dba.dk og Facebook mv. eller efter køb på falske webshops (ibid. s. 134, 179). Politiet formoder som tidligere nævnt, at dette som udgangspunkt ikke er relevant for identitetstyveri af NemID. I følgende ses derfor bort fra disse samt hadefulde ytringer, der ligeledes ikke har relevans for identitetstyveri af NemID.

Misbrug af personoplysninger estimeres at omfatte 0,4 pct. af befolkningen eller ca. 17.200 borgere. Kategorien afdækker situationer, hvor en anden har anvendt offerets personoplysninger, fx navn, cpr-nummer, e-mail eller identitetsbeviser til eksempelvis at bestille en vare/ydelse eller oprette et abonnement i offerets navn (Justitsministeriet (B) 2021, s. 140, 178). Ofre for identitetstyveri af NemID bør derfor være repræsenteret i denne kategori. Der vil dog også være mange oplevelser, som formentligt er relateret til misbrug af andre personoplysninger såsom e-mail, navn, cpr mv. - som alt andet lige er lettere at misbruge.

Kontaktbedrageri estimeres til at omfatte 0,3 pct. af befolkningen eller ca. 14.500 borgere. Kategorien afdækker oplevelser af at være blevet narret til at gennemføre en transaktion til en svindler, som har kontaktet borgeren på internettet (ibid. s. 139, 178). Som tidligere nævnt er der i disse tilfælde sjældent tale om decideret identitetstyveri af NemID, men da borgeren narres til at gennemføre en transaktion, som i flere tilfælde godkendes med NemID, kan kategorien alligevel inddirekte være relevant for problematikken i et vist omfang.

Misbrug af betalingskortoplysninger estimeres til at omfatte 2,3 pct. af befolkningen eller ca. 100.200 borgere. Kategorien afdækker oplevelsen af, at offerets kortoplysninger er blevet misbrugt til at købe en vare eller ydelse på internettet (ibid. s. 129). Det kan principielt også være tilfælde, hvor børn eksempelvis har benyttet deres forældres betalingskort uden tilladelse. Kategorien dækker eksempelvis også situationer, hvor ofre er blevet narret til at opgive deres betalingskortoplysninger i en phishing e-mail eller pr. sms eller ledt ind til en falsk webshop, som sjældent anvender to-faktor autentifikation (ibid.). Som tidligere

nævnt formoder politiet, at misbrug af betalingskort kun i mindre grad kan være relevant for identitetstyveri af NemID. Derudover viser Finanstilsynets data i figur 3, afsnit 2.2, at misbrug af betalingskort i 2020 hovedsageligt fandt sted i situationer, hvor der ikke blev benyttet to-faktor autentifikation. Der er således god indikation for, at kategorien "Misbrug af betalingskortoplysninger" fra Justitsministeriets offerundersøgelse kun i begrænset omfang kan være relevant for identitetstyveri af NemID.

Endeligt bør det nævnes, at Justitsministeriet offerundersøgelse i deres kapitel 3 belyser fysisk tyveri. Der kan være tilfælde heriblandt, hvor både NemID nøglekort, personoplysninger og nedskrevne login-oplysninger et er blevet fysisk stjålet. Dette er dog ikke muligt at kvalificere nærmere ud fra Justitsministeriets offerundersøgelse. Nævnte tilfælde kan dog medføre identitetstyveri af NemID, som dog forhåbentligt bremses hurtigt med spærring af NemID'et, da det formentligt er hurtigere at opdage indbrud eller tasketyveri end digitalt tyveri.

Opsamling på tværs af Justitsministeriets offerundersøgelse og politianmeldelser
Gennemgangen af Justitsministeriets offerundersøgelse peger på, at kategorien "Misbrug af personoplysninger", som estimeres at udgøre 0,4 pct. af befolkningen, er den kategori i offerundersøgelsen, som med størst sandsynlighed afdækker ofre for identitetstyveri af NemID, om end kategorien også indeholder mange forhold, som ikke relaterer sig til identitetstyveri af NemID.

Kategorien "Kontaktbedrageri", som estimeres at udgøre 0,3 pct af befolkningen, kan derudover være relevant på mere inddikrete vis. Heri indgår formentligt ikke identitetstyveri af NemID, men svindelsituationer hvor en borger narres til at gennemføre en transaktion med sit NemID.

Der kan desuden være tilfælde af identitetstyveri af NemID, som er relateret til misbrug af betalingskortoplysninger eller fysisk tyveri, men det er ikke muligt at beskrive relevante procentsatser herfor ud fra Justitsministeriets offerundersøgelse.

Endeligt kan et og samme offer overlappe og indgå i flere af kategorierne, hvorfor kategorierne ikke skal sammenlægges.

Den tidligere gennemgang af politianmeldelser viste, at der formentligt er op mod 8.000 - 12.000 anmeldelser i 2020, som i et vist omfang kan være relateret til identitetstyveri af NemID. Tallene omfatter dog også anmeldelser, som ikke er relateret til identitetstyveri af NemID, og kan dække over flere anmeldelser fra samme borger. Derudover afdækker politianmeldelser også anmeldte forsøg, som kan være mislykket. Disse forskellige forbehold betyder, at der er færre borgere bag anmeldelserne end antallet af potentielt relevante politianmeldelser.

Det er således ikke muligt at angive et sikkert estimat for, hvor mange der udsættes for identitetstyveri af NemID på baggrund af Justitsministeriets

offerundersølgelse og tilgængelige politianmeldelserne. Gennemgangen af de forskellige kilder peger dog på, at der er tale om en meget lille andel af befolkningen - og en endnu mindre andel som potentielt også udsættes for svindel med NemKonto. Alle tilfælde tages dog meget alvorligt, da det kan have store konsekvenser, for den der rammes. Tiltag, der kan minimere svindlen på området, og hjælpe de der rammes, udfoldes i kapitel 4.

2.4 Spærring af NemID og henvendelser til Digitaliseringsstyrelsen

Det beskrives i dette afsnit, hvilket kendskab Digitaliseringsstyrelsen har til antal spærringer af NemID fra Nets samt henvendelser til styrelsens Hotline ved identitetstyveri. Tal herfra skal ikke læses som tilfælde, der ikke allerede kan være inkluderet i ovenstående afsnit om it-relateret kriminalitet, men som supplerende uddybende kilder.

Spærringer fra Nets

Nets indrapporterer svindelrelaterede spærringer til Digitaliseringsstyrelsen i relation til to kilder: Første kilde er to CERT-enheder (Computer emergency response team), der i forbindelse med håndtering af phishing-hjemmesider, har detekteret, at borgere har udleveret NemID-oplysninger, hvorfor borgernes NemID bør spærres. Anden kilde, som generelt står for en mindre andel end CERT-enhederne, er Politiet. Indrapporteringer herfra beror på aktuelle efterforskninger eller spørgsmål om NemID-transaktioner med henblik på spærring.

Disse rapporteringer viser, at Nets har registreret 10.318 spærringer af NemID i 2020. Tilsvarende rapporteringer viser, at Nets har registreret 2.105 spærringer i 2021. Det højere antal spærringer i 2020 vurderes at skyldes, at en større efterforskning af keyloggere på landets biblioteker i sommeren 2020 førte til spærringer af NemID. Over 6.000 af spærringerne i 2020 blev registreret i juli og august 2020.

Det kan ikke udelukkes, at én identitet er præsenteret flere gange i tallene. Indrapporteringerne fra Nets skelner desuden ikke mellem, om der har fundet misbrug sted, eller der blot er tale om en potentiel mulighed for/mistanke om misbrug i registeringen i NemID. En del af registreringerne vil derfor ikke omhandle reel misbrug af NemID. Eksempelvis vil mange af NemID spærringerne være relateret til situationer, hvor en svindler kan være kommet i besiddelse af en borgers CPR-nummer, hvilket har medført en spærring for en sikkerheds skyld. Samtidigt er det væsentligt at bemærke, at der i tillæg til Nets svindelrelaterede registreringer også forekommer svindelrelaterede spærringer på borgernes anmodning. Dette sker, hvis borgeren selv kontakter NemID privat-supporten, eller selv foretager spærringen i NemID-selvbetjeningen. Eksempelvis fordi borgeren er blevet manipuleret til at udlevere sine NemID-oplysninger. Borgerne kan også selv foretage spærringer uden angivelse af grund i NemID-selvbetjeningen og –supporten. Disse spærringer vil ikke nødvendigvis indgå i ovenstående tal. Endeligt finder et stort antal spærringer sted, fordi borgere har indtastet deres adgangskode forkert, eller

indrapporterer, at de har tabt deres NemID nøglekort i forbindelse med tab af pung eller mobiltelefon. Disse spærringer indgår ligeledes ikke i ovenstående tal.

Ovenstående rapporteringer fra Nets er således behæftet med en række metodiske usikkerheder. Tallene er derfor ikke en god indikator for, hvor mange NemID der spærres som følge af, at der er foregået reel svindel eller svindelforsøg.

Hotline ved identitetstyveri
Digitaliseringsstyrelsen åbnede i juni 2021 en hotline ved identitetstyveri. Fra lanceringen til 2. januar 2022 har hotlinen modtaget ca. 3.500 opkald. Henvendelser til hotlinen er steget løbende siden åbningen. I størstedelen af disse opkald har borgeren ikke oplevet et reelt misbrug, men søger vejledning for at forhindre, at det sker. Borgerne angiver, at phishing, smishing og vishing var de primære kilder til forsøgene på svindel (Digitaliseringsstyrelsen 2021).

Henvendelserne til hotlinen fordeler sig på disse kategorier:

- Misbrug af personlige oplysninger (fx NemID og CPR-nummer) Udgør ca. 14 pct.
- Risiko for misbrug af personlige oplysninger (fx NemID og CPR-nummer) - hvor borgerens personlige oplysninger er blevet tilgængelige for kriminelle, der har til hensigt at svindle borgeren. Udgør ca. 36 pct.
- Mislykkedes forsøg på identitetstyveri gennem fx phishing, hvor borgeren ikke har udleveret sine oplysninger. Udgør ca. 8 pct.
- Forebyggende vejledning, hvor der ikke har været en hensigt om svindel rettet mod borgeren. Udgør ca. 23 pct.
- Opkald om emner uden for hotlinens vejledningsområde. Udgør ca. 19 pct.

I perioden har ca. 300 af opkaldene specifikt omhandlet misbrug af NemID. I ca. 20 af disse opkald blev der også berettet om ændring af NemKonto. Det understreges, at flere af opkaldene omhandler én og samme sag, hvorfor antallet alene er et udtryk for antal opkald.

Ovenstående skal desuden læses med forbehold for, at formålet med hotlinen er at hjælpe borgerne, hvorfor journalisering ikke foretages med henblik på specifikt at kortlægge omfang, men for kvalitativt at kunne orientere sig i tidligere samtaler ved genkald. Hotlinen har således registreret antal opkald, og ikke antal sager eller individer, og beskriver alene borgerens oplevelse.

Konkrete svindelformer og tendenser

3. Konkrete svindelformer og tendenser

Dette kapitel beskriver konkrete former for svindel, som borgere kan opleve efter identitetstyveri med NemID. Hvor muligt angives kendt omfang. Derudover beskrives observerede ændringer i måden, der svindles på.

Hvis man udsættes for identitetstyveri af NemID, kan man opleve svindel af forskellig karakter. Samarbejdet med Finans Danmark, Finans & Leasing og Rigspolitiet har ført til viden om de primært observerede former for svindel. Disse beskrives enkeltvis nedenfor.

Metoderne bag svindel på området har ud over malware og fysisk tyveri udviklet sig til i høj grad at omfatte social engineering. Finans Danmark vurderer, at social engineering udgør størstedelen af NemID-svindel i dag. Svindel med malware beror på, at ondsindet soft- eller hardware installeres, eller på anden vis placeres på computere og andre enheder. Svindlere kan benytte dette som led i teknisk at bryde ind i diverse systemer, og gøre skade på disse eller hente data derfra. Ved social engineering udnytter svindlere derimod, at mennesker kan manipuleres. De kriminelle kontakter her deres ofre via e-mail (phishing), sms (smishing) eller telefonopkald (vishing) og overbeviser dem om, at de skal udlevere personlige oplysninger eller selv gennemføre svigagtige transaktioner mv. Svindlere udnytter især, at de kan manipulere deres offer til selv at gennemføre svigagtige transaktioner, da de i dette tilfælde ikke har udfordringen med at anskaffe både NemID, brugernavn og password. I stedet gennemfører borgeren i god tro selv alle trin i transaktionsprocessen. Denne tendens og bevægelse udfoldes i sidste afsnit af dette kapitel.

3.1 Indbrud i Netbank

Kriminelle kan misbruge en borgers NemID og personlige login oplysninger til at bryde ind i offerets netbank og herefter foretage svigagtige transaktioner til trods for to-faktor autentifikation. Enten ved at stjæle borgerens NemID og login-oplysninger, fysisk eller digitalt, eller gennem social engineering hvor offeret er blevet narret til at udlevere sine oplysninger - eller til selv at gennemføre en svigagtig transaktion. Loginløsninger til netbanker sker i dag med NemID, eller fra oktober 2021 med MitID, hvorfor data om netbankssvindel er en relevant indikator for identitetstyveri af NemID. Det bemærkes dog, at der ikke nødvendigvis foretages et decideret identitetstyveri af NemID, hvis kunden manipuleres til selv at gennemføre en svigagtig transaktion. Kunden vil dog stadig opleve at blive svindlet.

Tal fra Finans Danmarks hjemmeside viser, at der på tværs af banksektoren er registreret følgende:

Netbankssvindel			
Type	**2019**	**2020**	1. **Halvdel af 2021**
Svindel med fysiske stjålne identiteter og anden malware	516 forsøg, heraf 370 med tab (72 %)	485 forsøg, heraf 303 med tab (62 %)	(203 forsøg, heraf 121 med tab) (59,6 %)
Svindel med social engineering	936 forsøg, heraf 543 med tab (58 %)	1.485 forsøg, heraf 763 med tab (51 %)	(881 forsøg, heraf 347 med tab) (39 %)
Total	1.452 forsøg, heraf 913 med tab (63 %)	1.970 forsøg, heraf 1.066 med tab (54 %)	(1.084 forsøg, heraf 468 med tab) (45 %)

Tabel 2: Netbankssvindel. Kilde: Finans Danmark (A), 2022..

Der ses heraf en nedgang i antal forsøg på svindel med fysisk stjålne identiteter og andet malware. Samtidigt ses en stigning i antal forsøg med social engineering, som både dækker situationer, hvor svindleren har franarret offeret sine NemID login-oplysninger, eller narret offeret til selv at gennemføre en svigagtig transaktion. Ca. 75 pct. af alle forsøg på netbankssvindel i 2020 kom fra social engineering, hvilket er en stigning på over 10 procentpoint fra 2019. Finans Danmark har desuden vurderet, at i ca. 80 pct. af disse tilfælde er det kunden, som narres til selv at gennemføre en svigagtig transaktion.

Derudover ses en positiv udvikling i andelen af forsøg, som resulterer i tab. Det peger på, at flere forsøg på svindel mislykkes. Endeligt er det væsentligt at pointere, at der årligt gennemføres flere hundrede millioner NemID-transaktioner i netbank-regi, hvorfor tallene i relation til dette udgør en meget lille andel.

Finans Danmark er blevet spurgt specifikt til omfanget af identitetstyveri af NemID og svindel med NemKonto. Dette er forsøgt imødekommet, men da det af flere årsager er vanskeligt at udarbejde et præcist sektorestimat, og da svindel med NemID i finanssektoren primært er knyttet til netbankssvindel, vurderer Finans Danmark, at ovenstående er det bedst dækkende sektorestimat.

Derudover er der generelt usikkerheder forbundet med forskellige registreringsmetoder, og risiko for at ét identitetstyveri er blevet brugt til svindel mellem flere forskellige banker. Oplysningerne i tabel 1, skal læses med forbehold for eventuelle forskelle i registreringspraksis. Finans Danmark vurderer dog, at overblikket i tabel 1 er et fornuftigt sektorestimat for netbankssvindel, som primært er knyttet til login med NemID.

LCIK modtog 3076 politianmeldelser om "misbrug af adgang til netbank m.m." i 2020 og 1699 politianmeldelser herom i 2019 – jf. figur 1 i afsnit 2.3. Disse tal er således højere end det rapporterede antal fra Finans Danmark vedrørende netbankssvindel. Det kan blandt andet skyldes, at politianmeldelseskategorien "misbrug af adgang til netbank m.m." også indeholder anmeldelser vedrørende indbrud i andre systemer end bankernes. Eksempelvis kompromitterede logins til bonusordninger for flyrejsende, spilplatforme, streamingtjenester og lignende (LCIK

2021, s. 37). I disse tilfælde er login med NemID formentligt i mindre grad adgangsgivende, hvorfor det ikke nødvendigvis er identitetstyveri af NemID, som er metoden til denne svindel. Der kan også være flere politianmeldelser på en sag fra samme individ. Derudover kan der være konkrete tilfælde af svindelforsøg, som ikke er registreret af bankerne, eksempelvis tilfælde som er blevet opdaget og forhindret tidligt i processen. I så fald vil disse ikke indgå i ovenstående tabel fra Finans Danmark i alle tilfælde, men kan indgå i politiets data, hvis der er indgivet en politianmeldelse.

3.2 Optagelse af blankolån

Kriminelle kan også udnytte identitetstyveri af NemID til at optage et eller flere lån i offerets identitet. I nogle tilfælde skjules svindlen yderligere for offeret, hvis svindleren også ændrer offerets NemKonto til sin egen eller en tredjemands, hvorved offeret har svært ved at opdage, at der udbetales et lån. Det er primært forbrugslånsvirksomheder/banker specialiseret i forbrugslån, der tilbyder blankolån, som er et lån tildelt uden et formål om at finansiere en bestemt genstand såsom en computer eller cykel, der rammes af svindlen. Ifølge Finans & Leasing skyldes det formentligt, at kriminelle ved, at de ikke kan ansøge om enkeltstående kontantlån hos "fullservicebanker" uden at indgå et helkundeforhold med oprettelse af lønkonto mv.

Finans & Leasing oplyser, at 10 ud af deres 12 forbrugslånsselskaber, samt tre ud af deres 45 billåns- og leasingselskaber, tilsammen har registreret 850 sager om identitetstyveri af NemID i 2020 og tilsvarende 430 sager i de første tre kvartaler af 2021. Finans & Leasings medlemmer forsøger løbende at hindre svindel med forskellige tiltag. Eksempelvis indførte et medlem i december 2020 en alarmeringspraksis, hvorefter de har haft færre svindelsager. Alarmeringen udløses eksempelvis, hvis der ansøges om lån fra udlandet eller ved gentagende låneanmodninger fra samme kontonummer.

Det er primært forbrugslånsbanker, der rammes af svindel som følge af identitetstyveri med NemID, og Finans & Leasing vurderer, at ovenstående tal er et realistisk bud på et sektorestimat. Sagerne er dog ikke krydsregistreret på individniveau, hvorfor de 850 sager kan være et udtryk for færre identitetstyverier med NemID, da kriminelle kan optage flere lån på tværs af låneselskaberne med ét og samme identitetstyveri. Derudover er registreringen foretaget manuelt.

I et svar til Finanstilsynet i januar 2020 angiver Finans & Leasing desuden et forsigtigt omfangsestimat på ca. 630 sager i 2019 vedrørende svindel foranlediget af identitetstyveri af NemID. De 630 sager er dog indrapporteret fra otte medlemmer, hvorimod de 850 sager fra 2020 er rapporteret fra ti medlemmer. Ovenstående metodiske forbehold og usikkerheder gør sig fortsat gældende.

3.3 Svindel med NemKonto

I NemKonto løsningen er det muligt at anvise sin NemKonto til en bankkonto, som ikke er ejet af en selv, hvilket kaldes en tredjemandskonto. Dette muliggør, at

flere personer kan anvende samme NemKonto. Muligheden imødekommer eksempelvis ægtefællers ønske om en fælles NemKonto. Det er muligt at ændre sin NemKonto, hvis NemKonto-ejeren enten kontakter sit pengeinstitut, eller benytter selvbetjeningsløsningen på www.nemkonto.dk med sit NemID.

Der er set konkrete tilfælde, hvor der i forbindelse med identitetstyveri af NemID er blevet svindlet med NemKonto. De kriminelle har i disse tilfælde anvendt offerets NemID-oplysninger på selvbetjeningsløsningen, til at omdirigere borgerens NemKonto til egen bankkonto - eller til en stråmandskonto hos en tredje part.

Finans Danmark oplyser, at en større nordisk bankkæde i 2020 registrerede 34 sager om svindel med NemKonto som følge af identitetstyveri. De vurderer, at denne bankkæde repræsenterer langt størstedelen af svindlen på deres område. Tilsvarende registrerede bankkæden i løbet af de første tre kvartaler af 2021 ti sager. Registreringerne af svindel med NemKonto er dog foretaget manuelt og skønnes af Finans Danmark måske at kunne være op til dobbelt så stort. Finans Danmark vurderer dog, at faldet fra 2020 til 2021 er reelt, og de oplever i 2021 mindre svindel med NemKonto, som følge af identitetstyveri med NemID, på tværs af alle deres medlemmer. Timingen korrelerer med, at Digitaliseringsstyrelsen den 19. april 2021 implementerede et fysisk aktiveringsbrev som et ekstra godkendelsestrin ved anvisning af en NemKonto via selvbetjeningsløsningen (NemKonto 2021).

Finans & Leasing oplyser, at de fleste af deres medlemmer ikke opgør antallet af sager vedrørende svindel med NemKonto. Et af deres medlemmer har dog i 2020 registreret 145 politianmeldelser relateret til identitetstyveri af NemID, hvoraf de anslår, at 60-70 tillige har været udsat for svindel med NemKonto. Dette kan pege på, at der i lånesektoren er medlemmer, som oplever, at svindel med NemKonto kan forekomme i op mod næsten halvdelen af deres sager om identitetstyveri af NemID. Dette kan i så fald tyde på, at der kan være en hyppigere forekomst af svindel med NemKonto i forbrugslånssektoren end i finanssektoren generelt – om end tallene bør læses med tidligere nævnte metodiske forbehold.

Endeligt fremgår det af afsnit 2.3, at Rigspolitiet har lavet et estimat på ca. 200 årlige anmeldelser i relation til svindel med NemKonto. Tallet er dog behæftet med flere metodiske usikkerheder og repræsenterer alene antal anmeldelser, hvoraf flere kan komme fra den samme borger.

Svindel med NemKonto på tværs af aktører
På baggrund af oplysningerne fra bank- låne- og politisektoren er det således ikke muligt at lave et sikkert estimat for omfanget af svindel med NemKonto. Der vil være overlap mellem tal fra især politianmeldelserne og tallene fra Finans Danmark og Finans & Leasing, og som tidligere beskrevet er der yderligere metodiske usikkerheder forbundet med estimaterne. Det tyder dog på, at svindel med NemKonto udgør en væsentligt mindre andel end det totale omfang af identitetstyveri af NemID.

Til trods for at NemID og NemKonto med flere millioner af brugere generelt er meget sikre at anvende, kan det have store konsekvenser for de, der rammes. Alle borgere skal kunne have fuld tillid til brugen af Danmarks digitale infrastrukturer, hvorfor alle tilfælde af svindel med løsningerne tages alvorligt. Det uddybes i kapitel 4, hvilke tiltag der kan bidrage til at minimere svindel på området - og hjælpe de der rammes.

3.4 Indkøb på internettet

Såfremt den kriminelle både har stjålet eller franarret offerets NemID oplysninger og betalingskortoplysninger, er det ligeledes muligt at misbruge disse til internethandel trods to-faktor autentifikation ved betaling. Som nævnt i afsnit 2.3 viser tal fra Finanstilsynet dog, at svindel med danske korttransaktioner, der benytter to-faktor autentifikation, udgør mindre end en promille af alle korttransaktioner.

3.5 Login til personfølsomme oplysninger

Ofre for identitetstyveri af NemID kan desuden opleve, at det bliver misbrugt til at logge ind på diverse selvbetjeningsløsninger hos fx Skat.dk, Sundhed.dk og andre portaler med adgang til personfølsomme data. Der vil sjældent være tale om økonomisk kriminalitet i dette scenarie, men konsekvenserne for offeret kan alligevel være store og ubehagelige.

Skattestyrelsen oplyser, at de har set konkrete tilfælde med skattesvindel, men at svindelscenariet har været forbundet med ændring af NemKonto, som den kriminelle har udnyttet til at omdirigere eksempelvis restskat til egen konto.

3.6 Ændring i svindelmetoder

Der er gennem flere år set en generel bevægelse i svindelmetoder relateret til svindel med NemID. Der forekommer fortsat svindel med malware og fysisk tyveri, men der observeres en udvikling inden for social engineering, som flere centrale aktører i dag oplever som den mest udbredte metode til svindel med NemID. Det formodes især at skyldes, at sikkerhedsforbedringer har gjort det sværere at svindle med ondsindet soft- og hardware - og fordi det er blevet sværere at svindle med et betalingskort alene, som der er redegjort for i afsnit 2.2. Der har således været incitament blandt kriminelle til at finde nye svindelmetoder. Denne formodning bakkes op af både bank- og lånesektoren, og er ligeledes en af hovedpointerne fra Rigspolitiets temaundersøgelse (NEC 2021, s. 5-6). De konkluderer desuden:

> *"… gerningspersonerne anvender primært metoder som phishing-mails og fupopkald til at franarre NemID-oplysninger. Ingen af disse svindelmetoder involverer tekniske mangler ved NemID-systemet, men udnytter i stedet ofres uopmærksomhed og manglende viden.*" (NEC 2021, s. 11).

Finans Danmark og Finans & Leasing har ligeledes observeret denne bevægelse. I højere grad end tidligere opleves social engineering desuden ikke blot ved

phishing-mails og -sms'er, men især også ved direkte kontakt. Typisk via telefonopkald hvor der opbygges tillid mellem offer og svindler, som efterfølgende misbruges.

Der skelnes mellem svindler-udført og kunde-udført social engineering:

- **Svindler-udført social engineering**
  Svindleren overtaler offeret til at udlevere personlige oplysninger, og franarrer muligvis vedkommendes NemID. Svindleren kan nu foretage svigagtige transaktioner, optage lån mv.
- **Kunde-udført social engineering**
  Svindleren overbeviser offeret om, at vedkommende eksempelvis skal gennemføre en transaktion eller godkende en anmodning i fx NemID Nøgleapp. I disse tilfælde sker der teknisk set ikke et indbrud i offerets netbank, fordi log-in og transaktion er foretaget af kunden selv. Denne form kan derfor også være sværere at registrere og bevise. Finans Danmark oplyser, at denne form for social engineering skønnes at udgøre op mod 80 pct. af al social engineering på området.

Det er dog vigtigt at bemærke, at udviklingen ikke gør sig gældende på tværs af alle former for svindel. Finanstilsynet oplyser, at social engineering ikke er den primære svindelmetode, når det kommer til misbrug af betalingskort med to-faktor autentifikation. Svindel med betalingskort sker derimod oftest på baggrund af stjålne kortdetaljer. Social engineering benyttes især ved kontooverførsler, hvor der eksempelvis overføres penge fra offerets konto til en svindlers eller en tredjemands konto. Muligvis fordi det er for svært at svindle på anden vis i disse tilfælde. Dette er i overensstemmelse med Finans Danmarks observationer af, at social engineering udgør størstedelen af svindel ved indbrud i netbank. Finanstilsynet påpeger, at det kan skyldes, at det er for svært at manipulere et offer til både at udlevere sine kortoplysninger og verificere en betaling med to-faktor autentifikation eller udlevere NemID oplysninger. Ved svindel med betalingskort skal svindleren derudover enten købe noget, eller stå i ledtog med en internetforretning, hvilket også kompliserer denne type svindel, hvorimod man i højere grad kan narre folk til at udføre en svigagtig kontooverførsel fra offerets netbank direkte til en konto, svindleren ejer eller har adgang til. Der er alt andet lige også større økonomisk vinding ved at svindle med overførsler af større beløb, eller store lån, end ved køb af diverse genstande og ydelser.

Den europæiske banktilsynsmyndighed, EBA, fremhæver ligeledes, at der i højere grad ses svindel trods to-faktor autentifikation, ved kontooverførsler frem for ved kortbetaling med to-faktor autentifikation (EBA 2022, s. 24-25). Her påpeges ligeledes, at det kan skyldes, at kundeudført social engineering i højere grad er muligt ved kontooverførsler (ibid.). To-faktor autentifikation vil ikke have sin tilsigtede effekt, hvis et offer gennemfører en overførsel, fordi vedkommende er manipuleret til at tro, det er nødvendigt/korrekt.

Professionelle svindlere efterligner myndigheder og virksomheder
Kriminelle på området er blevet dygtige til at efterligne myndigheder og udnytter herved borgernes tillid til disse. På baggrund af oplysninger fra Finans Danmark, Finans & Leasing samt Rigspolitiet ved vi, at svindlere eksempelvis henvender sig til deres ofre og udgiver sig for at være fra politiet. Der informeres om, at politiet har opdaget svindel med borgerens NemID, hvorfor de skal have borgerens NemID oplysninger verificeret. Der ses ligeledes eksempler på, at kriminelle udgiver sig for at være fra banker, it-leverandører, styrelser eller andre myndigheder og institutioner. I nogle tilfælde bedes borgeren om at ringe tilbage på et telefonnummer, hvor borgeren modtages af officielle menuer med ventetoner mv., hvilket styrker borgerens oplevelse af at være i kontakt med en reel myndighed. I mails kopierer svindlere myndigheder og virksomheders design, logoer og signaturer, hvilket ligeledes højner troværdigheden. Derudover udnyttes timingen i perioder, hvor myndigheder eksempelvis kontakter mange borgere om skift fra NemID til MitID, årsopgørelser og udbetalinger fra Skat m.m. Dette kan muligvis medføre øget svindel i netop disse perioder.

Ydermere ses social engineering også i form af kærlighedssvindel, hvor gerningspersonen får kontakt til sit offer via sociale medier eller datingsites og apps. Efter at have opbygget et tillidsbånd sendes svigagtige links, eller tillidsbåndet udnyttes til at overtale offeret til at overføre penge (Finans Danmark (B) 2022).

Der forekommer ligeledes social engineering i form af investeringssvindel, hvor den stigende tendens til at investere blandt den almene befolkning udnyttes. Ofre lokkes til at investere gennem falske firmaer og opdager det typisk først, når de på et tidspunkt ikke kan hæve deres gevinst (Finans Danmark (C) 2022).

Andre former for borgerrettede svindelmetoder
I visse tilfælde forekommer svindlen også fra nære relationer eller bekendte, som eksempelvis stjæler offerets betalingskort, personoplysninger og NemID (NEC 2021, s. 10). Det kan eksempelvis forekomme fra personale til udsatte borgere, eller i familier, kollektiver og lignende, hvor man omgås tæt.

Keylogging er en metode, hvor svindlere installerer software eller hardware, på fx offentlige computere, som kan lagre tastetryk foretaget på computeren og derved indsamle brugernes login-oplysninger mv. (ibid.). Hvis computeren har mange brugere, kan man fra en enkelt computer ramme mange. Ifølge Finans Danmark er der ikke observeret større sager af dette, siden man satte ind efter to større sager på flere af landets biblioteker i 2020. Eksempelvis er muligheden for at se antal resterende nøgler på NemID nøglekortet ved login blevet fjernet. Det skyldes, at man i keylogger-sager har set, at svindlere har misbrugt denne information til at planlægge indbrud i postkasser i forbindelse med fremsending af nye nøglekort.

Endeligt kan identitetstyveri med NemID misbruges til at oprette virksomheder og andre konstellationer, som eksempelvis kan udnyttes til skattesvig.

Ældre er særligt udsatte for misbrug af adgang til netbank
It-relateret økonomisk kriminalitet rammer alle aldersgrupper. Som helhed rammes de 20-49-årige mest - og allerflest politianmeldelser findes i aldersgruppen 20-29 årige (LCIK 2021). De yngre handler også mest online, om end der som tidligere nævnt er mest vækst i internet-handel blandt de ældre aldersgrupper (Danmarks Statistik (C) 2020).

Ældre aldersgrupper er dog mest udsatte, når det kommer til misbrug af adgang til netbank, som oftest vil involvere svindel med NemID. Antallet af politianmeldelser på området viser, at over halvdelen (56,2 pct.) af alle anmeldelser i 2020 om misbrug af adgang til netbank m.m. kom fra de 60+ årige (LCIK 2021, s. 69).

Det ses dog også at tilbøjeligheden til at foretage forebyggende handlinger, såsom at ændre kodeord som følge af phishing mails og smishing sms'er, er næsten dobbelt så stor blandt de 60+ årige som blandt de 18-29-årige (Digitaliseringsstyrelsen et al. 2020, s. 14). Tilslutningen til at benytte løsninger såsom passwordmanagers er dog lavere hos ældre (ibid. s. 22-23).

Finans Danmark har påpeget, at ældre muligvis også er mere udsatte for social engineering i form af især manipulerende telefonopkald (vishing), fordi de kan være mere tilbøjelige til at ønske teknisk hjælp fra en, som eksempelvis udgiver sig for at være sikkerhedsafdelingen i en bank, Nets eller en offentlig myndighed. Eller fordi de ikke forbinder telefonopkald med muligheden for svindel. Der er set sager i både Danmark og andre nordiske lande, hvor kriminelle eksempelvis har udnyttet telefonlister med navne, som i højere grad tilhører den ældre del af befolkningen, til udvælge ofre fra.

Muligheder for minimering af svindel med NemID og NemKonto

4. Muligheder for minimering af svindel med NemID og NemKonto

Dette kapitel beskriver igangsatte og mulige tiltag, som kan bidrage til at mindske identitetstyveri af NemID og svindel med NemKonto yderligere. Kapitlet indeholder de tiltag, der er igangsat eller planlagt til og med ultimo maj.

Sikkerheden i Digitaliseringsstyrelsens løsninger er kontinuerligt i fokus, hvorfor der løbende foretages justeringer i takt med at ny viden opstår. Nedenfor beskrives tiltag, som har til hensigt at bidrage til at minimere identitetstyveri af NemID og svindel med NemKonto.

Derudover henvises til Digitaliseringsstyrelsens halvårlige sikkerhedsrapport, som rapporterer om sikkerheden for henholdsvis NemKonto, NemID og MitID.

4.1 Sikkerhedstiltag i NemID

Sikkerheden er løbende blevet vurderet og forbedret i NemID, i takt med at ny viden om svindelmetoder er opstået. Listen nedenfor er derfor ikke udtømmende, men eksempler på relevante nyere sikkerhedstiltag:

1. Ændring på nemid.nu således, at et nyt nøglekort ikke automatisk fremsendes, når en borger spærrer sit nøglekort.
2. Ved login med NemID, vises ikke længere, hvor mange resterende nøgler der er på nøglekortet. Det minimerer risikoen for, at kriminelle kan aflure, hvornår et NemID fremsendes og planlægge indbrud i postkassen herefter.
3. Lanceringen af NemID nøgleapp har minimeret risikoen for stjålne NemID nøglekort. Det er sværere at misbruge nøgleappen, da det både kræver pinkode til telefonen og til appen. Appen havde i februar 2022 ca. 4,2 mio. unikke brugere.
4. Ændring i krav og processer har medført øget validering af identiteter inden udstedelse af NemID i Borgerservice.
5. Etablering af en hotline til hjælp ved identitetstyveri pr. 1. juni 2021

4.2 Sikkerhedstiltag i MitID

Når MitID afløser NemID, styrkes sikkerheden i løsningen yderligere på især tre områder, som beskyttet borgerne bedre mod identitetstyveri: I den tekniske løsning, i forhold til identifikationsmidlerne og i kravene til identitetssikring. Eksempelvis kan følgende nævnes:

1. Nøglekortet som bruges til NemID udfases, hvilket forhindrer, at nøglekort kan stjæles eller kopieres og anvendes uden yderligere pinkode, og forhindrer at alle nøgler er synlige på én gang.
2. Adgangskoden til MitID appen valideres centralt og er integreret i pinkoden til appen. Når denne centrale sikkerhedsvalidering integreres direkte i appen, minimeres risikoen for afluring af adgangskoder på svigagtige hjemmesider designet hertil - eller ved eksempelvis keylogging på offentlige pc'er.
3. MitID appen sender ikke push-notifikationer, som praksis ellers har været i NemID appen. Dette forhindrer, at ejeren uforvarende kommer til at godkende en anmodning, som vedkommende ikke selv har startet. Anmodningen i MitID appen forsvinder efter fem minutter, hvorfor det er svært at komme til at godkende en svigagtig anmodning eller transaktion, når man samtidigt ikke notificeres herom.
4. Brugere kan fremover se af en hjemmesides URL, at hjemmesiden er legitim til at benytte MitID-login, da mit.dk vil fremgå i hjemmesidens URL. Dette betyder, at man får bedre forudsætninger for at gennemskue falske hjemmesider.
5. Der er indført en karensperiode for ændring af sikkerhedsmæssigt kritiske indstillinger på MitID.dk. Eksempelvis ved ændring af bruger-ID, telefonnummer, e-mail, notifikationer, adgangskode samt tilføjelse af nye identifikationsmidler. Brugerne skal logge ind to gange med en times mellemrum for at foretage sådanne ændringer, hvilket gør det sværere for en svindler eksempelvis at overtale et offer i telefonen til at godkende en ændring.
6. Der sendes en notifikation til brugeren, hvis der anmodes om at foretage kritiske ændringer. Dette skal bidrage til at gøre brugeren opmærksom på hurtigt at spærre sit MitID, såfremt anmodningen ikke kommer fra vedkommende selv.
7. Forbedret risikodata i MitID gør det i højere grad muligt at lokalisere usædvanlig aktivitet og advare MitID-brokere herom. Eksempelvis advares ved geografisk usædvanlig aktivitet, ved brug på nye enheder eller ved brug på nye IP-adresser under autentifikation.
8. MitID's infrastruktur er mere modulær og fleksibelt opbygget, hvilket gør det hurtigere at reagere teknisk på skiftende internettrusler og løbende tilpasse løsningen derefter.

Som beskrevet i afsnit 3.6 udnytter svindlere typisk timingen i perioder, hvor myndigheder har hyppig kontakt med borgere. Eksempelvis ved at udgive sig for at være SKAT omkring årsopgørelsen eller Digitaliseringsstyrelsen omkring skiftet fra NemID til MitID. Derfor lanceres yderlige tekniske tiltag, der skal styrke sikkerhed ved overgangen fra NemID og MitID.

4.3 Fysiske aktiveringsbreve til NemKonto

Siden midt april 2021 har Digitaliseringsstyrelsen udsendt fysiske aktiveringsbreve ved anvisning af NemKonto via selvbetjeningsløsningen. Som tidligere nævnt observerer flere aktører, at dette ekstra godkendelsestrin har haft en positiv effekt og

bidraget til markant mindre svindel med NemKonto. Fysiske aktiveringsbreve, eller andre former for godkendelse i flere trin, bør derfor ligeledes overvejes fremadrettet, hvis der opleves svindel med omdirigering og svigagtige aktiveringer i andre sammenhænge.

4.4 Analyse af muligheder for begrænset anvisning af NemKonto

Digitaliseringsstyrelsen har i foråret 2022 undersøgt tekniske og juridiske muligheder for at begrænse muligheden for at kunne anvise NemKonto til en tredjemand via selvbetjening. De sidste afklaringer pågår fortsat. Det indledningsvise arbejde indikerer, at det er muligt at gennemføre.

4.5 Borgerrettede informationskampagner

Informationskampagner, som kan styrke borgeres kendskab til risikosituationer og især styrke deres evne til at ændre adfærd, er helt centralt for at minimere svindel på området yderligere. Det skyldes især, at det i tiltagende grad er social engineering, der ligger bag svindel med NemID. Da kriminelle udnytter, at mennesker kan manipuleres, er borgernes viden og adfærd afgørende for omfanget af denne type svindel.

Digitaliseringsstyrelsen arbejder løbende med at oplyse og kompetenceudvikle borgere og offentligt ansatte om cyber- og informationssikkerhed. Eksempelvis udvikler og driver Digitaliseringsstyrelsen www.sikkerdigital.dk sammen med Erhvervsstyrelsen. Derudover er politiet og en lang række private virksomheder og offentlige myndigheder, herunder Digitaliseringsstyrelsen, involveret i appen Mit Digitale Selvforsvar. Bidragsyderne oplyser og advarer brugerne om særlige tendenser, aktuelle falske mails og sms'er mv.

Der er dog fortsat behov for yderligere kampagner, som når endnu bredere ud i befolkningen og især til de potentielt mere udsatte grupper. Blandt andet fordi en megafonundersøgelse udført for Digitaliseringsstyrelsen finder, at desto mere man er opmærksom på truslen og risikobetonet adfærd, desto mere er man tilbøjelig til at efterleve anbefalingerne for sikker digital adfærd (Digitaliseringsstyrelsen et. al., 2020, s. 32). Det er desuden vigtigt, at borgerettede kampagner formidles på en meningsfuld måde, skaber en klar handlemulighed, kommer på rette tidspunkt og gentages flere gange for at højne sandsynligheden for adfærdsændring (ibid. s. 35). Digitaliseringsstyrelsen har flere kampagner planlagt i 2022 – herunder en direkte målrettet identitetstyveri. Fra maj løber desuden en kampagne for Hotline ved identitetstyveri på flere sociale medier for at gøre borgerne opmærksom på, hvor de kan få hjælp og vejledning herom.

4.6 Erfaringsudveksling og netværk

Viden om de kriminelles adfærd og nyeste trends er vigtig for at kunne tilpasse sikkerhedsindsatser derefter. Digitaliseringsstyrelsen følger nøje med i aktuelle svindeltendenser, og er derfor i løbende dialog med relevante parter på området. I forbindelse med det igangsatte arbejde om at skabe et bedre og bredere overblik over omfanget af svindel med NemID og NemKonto, er Digitaliseringsstyrelsen i

tæt dialog med Finans Danmark, Finans og Leasing og Rigspolitiet herom. Herudover er Digitaliseringsstyrelsen i løbende dialog med forskellige aktører på området, bl.a. Forbrugerrådet Tænk ift. sikkerdigital.dk og appen Mit digitale selvforsvar, og med Nationalt Center for IT-Kriminalitet ift. kampagner og analyser.

Som opfølgning på denne rapport er Rigspolitiet, Finans Danmark og Finans & Leasing inviteret til at deltage i en samarbejdsgruppe med Digitaliseringsstyrelsen. Formålet hermed er at følge udviklingen i omfanget af svindel på området og identificere mulige tiltag blandt parterne, som kan bidrage til at minimere svindel på området yderligere.

4.7 Hjælp til ofre for identitetstyveri af NemID og svindel med NemKonto

Til trods for at er en meget lille andel der udsættes for identitetstyveri af NemID og svindel med NemKonto, kan det have meget store konsekvenser for den enkelte, der rammes. Digitaliseringsstyrelsens hotline ved identitetstyveri er blandt andet oprettet for at yde døgnrådgivning og hjælp til disse borgere. Samt for at give forebyggende vejledning.

Derudover er der fremsat et lovforslag om en kompensationsordning i tilfælde af svindel med NemKonto (Høringsportalen 2022). Dette skal sikre retssikkerheden for ofre for svindel med NemKonto, hvor anden lovgivning ikke dækker, så man som borger ikke risikerer at hæfte økonomisk, såfremt man har handlet forsvarligt, men alligevel udsættes for svindel.

Endeligt har regeringen tilkendegivet, at man ønsker at nedsætte en tværministeriel arbejdsgruppe, som frem mod udgangen af efteråret 2022 skal afdække, hvad man yderligere kan gøre for at hjælpe borgere, der har været ude for, at deres digitale ID ved svindel er blevet brugt til at indgå aftale.

Konklusion

5. Konklusion

Afslutningsvist opsummeres rapportens hovedkonklusioner.

Rapporten belyser, at Danmark er frontløber inden for offentlig digitalisering og internethandel. NemID er et af de mange tiltag, som bidrager til, at denne digitalisering forløber med et meget højt sikkerhedsniveau. Digitaliseringen har især i løbet af seneste årti ændret adfærden i befolkningen, så langt flere i dag handler på internettet og benytter digitale løsninger i hverdagen. Udviklingen har store fordele, men medfører også, at flere er i risiko for at opleve it-relateret kriminalitet.

Det er ikke muligt at angive et nøjagtigt estimat for omfanget af identitetstyveri af NemID og svindel med NemKonto på grund af forskellige registreringspraksis og metodiske usikkerheder ved sammenligning af eksisterende data. Der er dog præsenteret en række kilder i rapporten, som på forskellig vis kan bidrage til at indkredse omfanget, såfremt de læses med deres metodiske forbehold.

Der ses en positiv udvikling inden for misbrug af danske betalingskort, som siden 2016 er reduceret med ca. 44 pct. Flere aktører peger på, at implementeringen af to-faktor autentifikation, som ofte udføres med NemID, har bidraget til den positive udvikling, men det har forventeligt også øget efterspørgslen på NemID-oplysninger hos de kriminelle – især efter fuld implementering af kravet i januar 2021.

Gennemgangen af Justitsministeriets offerundersøgelse peger på, at kategorien "Misbrug af personoplysninger", som estimeres at udgøre 0,4 pct. af befolkningen, er den kategori i offerundersøgelsen, som med størst sandsynlighed afdækker ofre for identitetstyveri af NemID, om end kategorien også indeholder mange forhold, som ikke relaterer sig til identitetstyveri af NemID.
Derudover kan kategorien "Kontaktbedrageri", som estimeres at udgøre 0,3 pct af befolkningen, være relevant på mere inddikrete vis. Heri indgår formentligt ikke identitetstyveri af NemID, men svindelsituationer hvor en borger narres til at gennemføre en transaktion med sit NemID.
Desuden kan der være tilfælde af identitetstyveri af NemID, som er relateret til misbrug af betalingskortoplysninger eller fysisk tyveri, men det er ikke muligt at beskrive relevante procentsatser herfor ud fra Justitsministeriets offerundersøgelse.
Endeligt kan et og samme offer overlappe og indgå i flere af kategorierne, hvorfor kategorierne ikke skal sammenlægges.

Politianmeldelser er muligvis en mere relevant indikator for omfanget af identitetstyveri af NemID, såfremt det antages at ofre herfor anmelder det til politiet. Rapportens gennemgang af politianmeldelser fra NCIK indikerer, at op mod 8.000-12.000 politianmeldelser fra 2020, i et vist omfang kan være relateret til

identitetstyveri af NemID. Tallene omfatter dog også anmeldelser, som ikke er relateret til identitetstyveri af NemID, og kan dække over flere anmeldelser fra samme borger. Derudover afdækker politianmeldelser også anmeldte forsøg, som kan være mislykket. Disse forskellige forbehold betyder, at det reelle antal ofre for identitetstyveri af NemID formodes at være væsentligt færre end antallet af potentielt relevante politianmeldelser.
Rigspolitiets vurderinger af politianmeldelser for it-relateret økonomisk kriminalitet peger på, at misbrug af adgang til netbank og kreditbedrageri formentligt er de mest relevante kategorier for potentielt identitetstyveri af NemID, og at kategorien "Kontaktbedrageri mod private" på mere indirekte vis kan være relateret til problematikken. Misbrug af betalingskortoplysninger vurderes i mindre grad forbundet med identitetstyveri af NemID.
Endeligt peger tilgængelige tal på, at en mindre andel af ofre for identitetstyveri af NemID også udsættes for svindel med NemKonto. Flere aktører oplever desuden færre tilfælde af svindel med NemKonto efter implementeringen af et yderligere aktiveringsbrev i april 2021.

Selv om det samlet set er en lille andel, der oplever identitetstyveri af NemID, og endnu færre der også oplever svindel med NemKonto, kan det have store konsekvenser for de, der rammes. Digitaliseringsstyrelsens Hotline ved identitetstyveri og lovforslaget om en kompensationsordning ved svindel med NemKonto skal derfor hjælpe de, som rammes og er i en alvorlig situation. Derudover pågår der pt. analyse af effekter og muligheder for at begrænse muligheden for at anvise en NemKonto til en tredjemands bankkonto.

Siden NemID blev lanceret i 2010, har der været kontinuerlig udvikling af sikkerheden i løsningen. Når MitID afløser NemID, styrkes sikkerheden i løsningen yderligere på især tre områder, som beskyttet borgerne bedre mod identitetstyveri: I den tekniske løsning, i forhold til identifikationsmidlerne og i kravene til identitetssikring.

Der kan forekomme forskellige svindelmetoder, men der ses en generel udvikling inden for især social engineering. Her franarres ofre oplysninger eller manipuleres til at gennemføre svigagtige transaktioner via e-mail (phishing), sms (smishing) eller telefonopkald (vishing). Finans Danmark vurderer, at social engineering er hovedårsagen til svindel med NemID, med en særlig fremgang af metoden vishing, hvor ofre gennem samtale narres til selv at gennemføre en transaktion - uden egentligt at blive udsat for identitetstyveri af NemID.

Langt størstedelen af alle forsøg på social engineering mislykkes, men nogle vil blive ramt. Social engineering udnytter ofres uopmærksomhed, manglende viden og tillid til myndigheder og autoriteter. Rigspolitiet påpeger, at svindelmetoderne i tilfælde af identitetstyveri af NemID primært udnytter dette, og at det derfor ikke skyldes tekniske mangler ved NemID systemet.

Manipulation af mennesker kan ikke elimineres fuldstændigt – hverken i den fysiske eller digitale verden. Oplysnings- og konkret handlingsanvisende kampagner vil være nødvendige for at hjælpe og guide borgere til sikker digital adfærd og opmærksomhed over for, at noget er galt, hvis de får henvendelser fra ukendte personer om deres NemID – eller bedes godkende en transaktion i NemID appen. Endeligt kan udbredelsen af password-managers, samt øget samarbejde og vidensdeling, muligvis bidrage til at minimere svindel på området yderligere. Derudover skal Digitaliseringsstyrelsens hotline ved identitetstyveri og lovforslaget om kompensationsordning ved svindel med NemKonto hjælpe de, som rammes og står i en alvorlig situation.

6. Referenceliste

Oversigt over anvendte referencer fremgår alfabetisk nedenfor.

Danmarks Nationalbank, 2020. Danskerne betaler fortrinsvist elektronisk. Rapport. Tilgængelig i januar 2022 fra: https://www.nationalbanken.dk/da/publikationer/Documents/2020/09/ANALYSE_Nr.%2015_Danskerne%20betaler%20fortrinsvist%20elektronisk.pdf

Danmarks Statistik (A), 2019: "*Rekordmange danskere handler på nettet, men flere oplever problemer, svindel og bedrag*". (Artikel). Tilgængelig i december 2021 fra: https://www.dst.dk/da/Statistik/nyheder-analyser-publ/bagtal/2019/2019-11-08-Rekordmange-handler-paa-nettet

Danmarks Statistik (B), 2019. "*Danske ældre er de mest digitale i EU*". Artikel. Online. Tilgængelig i december 2021 fra: https://www.dst.dk/da/Statistik/nyheder-analyser-publ/bagtal/2019/2019-04-23-danske-aeldre-er-de-mest-digitale-i-eu

Danmarks Statistik (C), 2020. *IT-anvendelse i befolkningen*. (Rapport) Tilgængelig i december 2021 fra: https://www.dst.dk/Site/Dst/Udgivelser/GetPubFile.aspx?id=29450&sid=itbef2020

Danmarks Statistik (D), 2020. *Stigning i anmeldt bedrageri*. Online artikel. Tilgængelig i december 2021 fra: https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=30212

Danmarks Statistik (E), 2022. *Fald i anmeldte bedragerier*. Online artikel. Tilgængelig i december 2021 fra: https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=38285

Dansk Erhverv, Theil H., 2020. *Nets: Misbrug på dankort halveret*. Online artikel. Digital Handel. Tilgængelig i januar 2022 fra: https://www.fdih.dk/nyheder/2020/august/nets-misbrug-pa-dankort-halveret

Digitaliseringsstyrelsen et. al., 2020. *Danskernes informationssikkerhed 2020*. (Rapport). Tilgængelig i december 2021 fra: https://digst.dk/media/23592/dankernes-informationssikkerhed-2020.pdf

Digitaliseringsstyrelsen, 2021. *Hotline medvirker til at forebygge identitetstyveri: antallet af opkald er tredoblet på tre måneder*. Online artikel. Tilgængelig i januar 2022 fra: https://digst.dk/nyheder/nyhedsarkiv/2021/december/hotline-medvirker-til-at-forebygge-identitetstyveri-antallet-af-opkald-er-tredoblet-paa-tre-maaneder/

Digitaliseringsstyrelsen, 2022. *Tal og Statistik*. Online Tilgængelig i januar 2022 fra: Tal og statistik (digst.dk)

Engmann T., 2019. Danmarks Statistik: "*Danske ældre er de mest digitale i EU*". Artikel). Tilgængelig i december 2021 fra: https://www.dst.dk/da/Statistik/nyheder-analyser-publ/bagtal/2019/2019-04-23-danske-aeldre-er-de-mest-digitale-i-eu

Eurostat, 2021. *E-commerce statistics*. Artikel. Online. Tilgængelig i januar 2022 fra: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=E-commerce_statistics

Finans Danmark (A), 2022. *Netbanksvindel*. Online. Tilgængelig i januar 2022 fra: https://finansdanmark.dk/tal-og-data/institutter-filialer-ansatte/kriminalitet/svindel-med-netbank-og-betalinger/netbanksvindel/

Finans Danmark (B), 2022. *Kærlighedssvindel*. Online. Tilgængelig i januar 2022 fra: https://finansdanmark.dk/tal-og-data/institutter-filialer-ansatte/kriminalitet/svindel-med-netbank-og-betalinger/kaerlighedssvindel/

Finans Danmark (C), 2022. *Investeringsssvindel*. Online. Tilgængelig i januar 2022 fra: https://finansdanmark.dk/tal-og-data/institutter-filialer-ansatte/kriminalitet/svindel-med-netbank-og-betalinger/investeringssvindel/

Finans Danmark (D), 2022. *Betalingskortmisbrug*. Online. Tilgængelig i januar 2022 fra: https://finansdanmark.dk/tal-og-data/institutter-filialer-ansatte/kriminalitet/svindel-med-netbank-og-betalinger/betalingskortmisbrug/

Finansministeriet, 2021. *Svar på Retsudvalgets spørgsmål nr. 718 (Alm. del) af 26. februar 2021 stillet efter ønske fra Peter Skaarup (DF)*. Online. Tilgængelig i januar 2022 fra: https://www.ft.dk/samling/20201/almdel/reu/spm/718/svar/1792209/2412422.pdf

Finanstilsynet, 2021. *Temaundersøgelse om brugen af stærk kundeautentifikation i e-handlen. (Rapport)*. Tilgængelig i december 2021 fra: https://www.finanstilsynet.dk/Nyheder-og-Presse/Pressemeddelelser/2021/temaundersogelsetofaktor.

Folketinget, 2021-22. *Lovforslag nr. L103: Forslag til Lov om ændring af straffeloven (Kriminalisering af identitetsmisbrug)*. Online. Tilgængelig i marts 2022 fra: https://www.ft.dk/samling/20211/lovforslag/L103/tidsplan.htm

Høringsportalen, 2022. *Udkast til Forslag til Lov om ændring af lov om offentlige betalinger m.v. (Mulighed for økonomisk kompensation ved svindel med Nemkonto)*. Tilgængelig i januar 2022 fra: https://hoeringsportalen.dk/Hearing/Details/66031

Justitsministeriet (A), 2021. *Regeringen og støttepartier enige om at kriminalisere identitetstyveri på nettet.* Artikel. Online. Tilgængelig i januar 2022 fra: https://www.justitsministeriet.dk/pressemeddelelse/regeringen-og-stoettepartier-enige-om-at-kriminalisere-identitetstyveri-paa-nettet/

Justitsministeriet (B), 2021. *Udsathed for vold og andre former for kriminalitet. Offerundersøgelserne 2005-2020.* Justitsministeriets forskningskontor. København K. Tilgængelig i januar 2022 fra: https://www.justitsministeriet.dk/wp-content/uploads/2021/12/Udsathed-for-vold-og-andre-former-for-kriminalitet.-Offerundersoegelserne-2005-2020-WT.pdf

Konkurrence- og forbrugerstyrelsen, 2020. *Betalingsrapport 2020*. Rapport. Online. Valby. Tilgængelig i januar 2022 fra: https://www.kfst.dk/media/xafnckqk/betalingsrapport-2020.pdf

LCIK (Landsdækkende Center for It-relateret økonomisk Kriminalitet), 2021. *Årsrapport 2020 – En rapport om it-relateret økonomisk kriminalitet anmeldt i 2020*. Rigspolitiet. Tilgængelig i januar 2022 fra: https://politi.dk/-/media/mediefiler/landsdaekkende-dokumenter/statistikker/oevrige-udgivelser/aarsrapport-om-it-relateret-oekonomisk-kriminalitet-anmeldt-i-2020.pdf?la=da&hash=6CEA8F49E0D116D3A5C120B988CC00BBA4873D64

NEC (Nationalt Efterforskningscenter), 2021. *Uretmæssig adgang til NemID – kortlægning af politianmeldte forsøg på tilegnelse af og uretmæssig anvendelse af andre personers NemID i perioden 2017-2020.* (Rapport). Retsudvalget 2020-2021.

Nets, 2019. *Svindel med dankort i frit fald.* (Pressemeddelelse). Tilgængelig d. 21. December 2021 fra: https://www.nets.eu/dk-da/nyheder/Pages/Svindel-med-Dankort-i-frit-fald.aspx

NemKonto, 2021. *Ændret proces for selvbetjening.* Online. Tilgængelig fra: https://www.nemkonto.dk/da/Borger/AEndret-proces-for-selvbetjening

Rigspolitiet, 2021. *Markant stigning i anmeldelser om svindel med NemID.* Online. Tilgængelig fra: https://politi.dk/rigspolitiet/nyhedsliste/markant-stigning-i-anmeldelser-om-svindel-med-nemid/2021/09/28

Bilag 1: Uddybning af metode

Som nævnt i afsnit 1.2 findes der i dag ikke fyldestgørende opgørelser og information, som er velegnet til at beskrive et præcist omfang af identitetstyveri med NemID og svindel med NemKonto.

Det varierer, om eksisterende opgørelser og information inkluderer forsøg på svindel, eller kun omhandler svindel, der er resulteret i et egentligt økonomisk tab - eller andre former for beviseligt misbrug. Flere kilder skelner ydermere ikke svindel med NemID og NemKonto fra andre former for it-relateret økonomisk svindel. Det varierer også, om eksisterende registreringspraksisser opgør i eksempelvis antal ofre, politianmeldelser, sager eller økonomisk tab. Derudover kan der være tilfælde, som ikke er anmeldt eller registreret.
Disse faktorer betyder, at det ikke er muligt at give et konkret estimat på omfanget af svindel med NemID og NemKonto ud fra nuværende registreringspraksis på tværs af aktører - og gør mange af kilderne uegnede til direkte sammenligning.

Den bedst tilgængelige viden om området må derfor blandt andet findes på tværs af undersøgelser og rapporter fra relevante kilder. Hertil benyttes især opgørelser af politianmeldelser fra Nationalt Center for It-Kriminalitet og seneste offerundersøgelse fra Justitsministeriet. Da disse kilder bidrager med henholdsvis politianmeldelser på området samt befolkningens oplevelse af at være udsat for kriminalitet på internettet, er de særligt relevante i tilstræbelsen på at få et mere kvalificeret helhedsbillede af kilder, der potentielt kan indeholde data med relevans for identitetstyveri af NemID og svindel med NemKonto. Inkluderet indhold er desuden drøftet og vurderet i samarbejde med rapporternes afsendere i forhold til relevans og forbehold. Dette beskrives løbende i rapporten.

I bestræbelsen på også at indsamle mere specifik viden om identitetstyveri med NemID og svindel med NemKonto er Finans Danmark og Finans & Leasing blevet spurgt specifikt hertil. Finans Danmark og Finans & Leasing har i den forbindelse bidraget med konkret information på baggrund af eksisterende registreringspraksis fra deres medlemmer.
Hertil har Finans Danmark oplyst, at der er forskellig registreringspraksis på tværs af banksektoren, hvorfor det ikke er muligt at give et samlet estimat for hele sektoren. De har dog et sektorestimat for netbankssvindel, som de vurderer er det mest sigende for identitetstyveri i deres branche – og har derudover indhentet data fra en større nordisk bankkæde, som har bidraget med registreringer af svindel med NemKonto. Finans Danmark vurderer, at denne bankkæde afdækker størstedelen af svindlen i deres sektor.
Finans & Leasing oplyser ligeledes, at branchen har forskellige registreringspraksis. Antal sager er derudover ikke nødvendigvis retvisende for antallet af identi-

tetstyveri af NemID, blandt andet fordi ét identitetstyveri kan misbruges til at optage flere forskellige lån. Finans & Leasing vurderer dog, at de indrapporterede antal sager udgør et realistisk bud på et sektorestimat.
Endeligt er Dansk Kreditråd kontaktet med henblik på at vurdere, om de ligeledes har medlemmer, som er i besiddelse af relevante sager vedrørende identitetstyveri af NemID. De oplyser dog, at deres medlemskreds er anderledes, hvorfor de primært oplever identitetstyveri af NemID indirekte blandt de af deres medlemmer, som har inkassofunktion. Dansk Kreditråd vurderes derfor ikke relevant, at inddrage yderligere.

I tillæg til samarbejdet med Finans Danmark, Finans & Leasing og Rigspolitiet har vi gennemgået en række undersøgelser og rapporter på området, hvorfra følgende kilder har bidraget med viden fra kvantitative og kvalitative undersøgelser:

- *LCIK Årsrapport 2020* fra Politiets Landsdækkende Center for It-relateret Økonomisk Kriminalitet (Nationalt Center for it-relateret økonomisk kriminalitet fra 2022).
- *Udsathed for vold og andre former for kriminalitet - Offerundersøgelserne 2005-2020* fra Justitsministeriets Forskningskontor, december 2021.
- *Uretmæssig adgang til NemID 2020-2021* fra Politiets Nationale Efterforskningscenter
- *Danskernes informationssikkerhed 2020* fra Digitaliseringsstyrelsen, Kommunernes Landsforening, Danske Regioner, DKCERT og DeiC med afsæt i en undersøgelse udført af Megafon A/S.
- *Betalingsrapport 2020 – regler og udvikling på betalingsmarkedet* fra Konkurrence og Forbrugerstyrelsen.
- *Temaundersøgelse om brugen af stærk kundeautentifikation i e-handlen 2021* fra Finanstilsynet.
- *Digital Risikoadfærd 2021* fra Det Kriminalpræventive Råd.
- Opgørelser og artikler fra blandt andet Danmarks Statistik, Danmarks Nationalbank, Dansk Erhverv, Eurostat, Nets, Finans Danmark, Finans & Leasing samt Digitaliseringsstyrelsen.

Rapportens metode hviler derfor på viden fra eksisterende undersøgelser og rapporter kombineret med kvalitativ og kvantitativ viden, af deskriptiv karakter, fra samarbejdet beskrevet ovenfor. Alle inddragede kilder er gennemgået og metodiske forbehold drøftet forud for inddragelse.

Udarbejdet af Digitaliseringsstyrelsen

digst.dk