4. juni 2024

Forebyggelse af vishing i Danmark

En analyse af det nuværende netværk og forebyggende tiltag

Kandidatspeciale i Kriminologi af
Andrea Østergaard Busk | 20195517
Tone Rosenberg Stauning | 20220481

Vejleder: Annick Prieur
Antal tegn: 191.924
Antal sider: 80

AALBORG UNIVERSITY

Abstract

This paper examines the current prevention network and measures against fraud, where vishing serves as the modus operandi in a Danish context and explores the opportunities to further strengthen these preventative measures. Using an abductive approach, the study investigates the prevention network through an interplay between theory and empirical findings. By applying Actor-Network Theory, the paper initially identifies actors within the Danish prevention network and their current implemented preventative measures. The empirical basis of the study consists of semi structured expert interviews with representatives from selected actors within the network and various supporting documents. The study has uncovered a complex and diverse network of actors that continually expands due to the nature of vishing as a social engineering strategy, often combined with other strategies such as smishing, phishing, spoofing, and persuasive narratives, rendering the crime perpetually adaptable.

The study identifies 22 preventative measures implemented by the selected actors before, during, and after vishing attacks are carried out. By utilizing Routine Activity Theory, the paper finds that the majority of the implemented measures aim to protect vulnerable targets through information dissemination or enhancing capable guardians' competences to thwart vishing attempts. Through Bjørgo's comprehensive prevention model, the analysis finds that the current preventative measures primarily activate mechanisms for 'Protecting vulnerable targets' and 'Disrupting criminal acts' which can 'Reduce harmful consequences', 'Incapacitate perpetrators', and 'Reduce the rewards from criminal acts'.

Finally, the paper explores how the current preventative mechanisms can be expanded and further strengthened through enhanced opportunities for data sharing, involvement of relevant stakeholders to impose shared responsibility for averting vishing attempts, and political prioritization of police investigative resources.

Forord

Vi vil gerne takke alle, der har bidraget til udviklingen af vores speciale.

Et dybfølt tak går til vores otte informanter, Jakob, Jens, Jesper, Lene, Niels, Pernille, Sofie og Torben. Uden jer ville vi ikke have været i stand til at gennemføre undersøgelsen. Vi er taknemmelige for jeres tid værdifulde indsigter. Tak til alle, der har hjulpet med at etablere kontakt til disse eksperter.

En særlig tak til vores vejleder, Annick Prieur, for at være en uvurderlig sparringspartner og for den konstruktive feedback, vi har modtaget undervejs.

Tak til stifteren af Center mod Økonomisk IT-Svindel, Sine Gregersen, for at præsentere os for tre spændende undersøgelsesforslag vedr. datingsvindel, der vakte vores interesse for digital svindel. Tak til vores underviser, Rasmus Munksgaard, for at rette vores opmærksomhed mod anmeldelses- og opklaringsniveauet af digital svindel, der sporede os ind på forebyggelsesproblematikken og førte til vores indledende undersøgelse af problemfeltet.

Aalborg, 2024,
Andrea og Tone

Indholdsfortegnelse

1. Problemfelt

Danmark er et af de mest digitaliserede lande i verden, hvilket betyder at danskerne i højere grad kommunikerer med hinanden og myndighederne elektronisk (Danmarks Statistik, n.d. *a*). Den kontaktløse kommunikationsform skaber lette og effektive løsninger i dagligdagen, som fordrer implementering af sikkerhedsforanstaltninger, der gør det sikkert for danskere f.eks. at foretage digitale overførsler og mindsker risikoen for at løsningerne udnyttes af kriminelle. På trods af implementerede sikkerhedsforanstaltninger, som f.eks. MitID, stiger anmeldelserne om it-relateret økonomisk kriminalitet (NCIK, 2024: 51). I 2023 modtog Politiets Nationale Center for IT-relateret økonomisk Kriminalitet (NCIK) 35.258 anmeldelser, hvilket er en stigning på 30 % fra 2022 (NCIK, 2024: 13). I Danmark blev der i 2023 svindlet for i alt 627 mio. kr., hvilket er en stigning på næsten 48 % fra 2022 (Finans Danmark, 2024 *b*; Finans Danmark, 2023: 4).

De kriminelle gør i høj grad brug af *social engineering*, som er metoder til at manipulere den forurettede til at omgå sikkerhedsforanstaltninger ved selv at autorisere overførsler til gerningspersonen eller udlevere personlige oplysninger, der misbruges eller kan gøre gerningspersonen i stand til at autorisere betalinger og overførsler i forurettedes navn (NCIK, 2024: 51). Social engineering er med til at komplicere kriminalitetsbilledet, da metoderne både omhandler teknisk manipulering af f.eks. opkalds-ID på telefonsamtaler og overtalelses-teknikker, som bruges til at franarre vedkommende penge eller personfølsomme oplysninger. Dette udmønter sig i det NCIK kalder 'Kontaktbedrageri mod private' (Ibid.: 31). Det kan være alt fra, at gerningspersonen udgiver sig for at være en bekendt i økonomisk nød, til at være en myndighedsperson, der advarer forurettede om at deres bankkonto er ved at blive tømt af kriminelle og dermed overtaler forurettede til at overføre penge til en "sikker konto" (Ibid.). Kontaktbedrageri er således en bred vifte af forskellige former for digital svindel. Kontakten kan oprettes gennem forskellige medier, såsom telefon, e-mail, SMS, sociale medier, chattjenester m.m. og svindelforsøg kan spredes til flere personer hurtigere, hvilket komplicerer kriminalitetsbilledet yderligere (Ibid.: 5).

På grund af det digitale element kan kriminaliteten foregå på tværs af landegrænser. Der er dog eksempler på sager om digital svindel, hvor *vishing* (svindel gennem telefonopkald) indgår som kontaktmodus (herefter betegnet 'modus'), hvor både gerningsperson og forurettede opholder sig inden for de danske grænser. Eksempelvis blev fire mænd den 15. december 2023, idømt i

alt 23 års fængsel for deres forsøg på at svindle 455 personer over halvandet år, hvoraf de lykkedes i 193 tilfælde, med et samlet udbytte på lidt over 15 mio. kr. (Østjyllands Politi, 2023). NCIKs årsrapport fra 2022, viser at anmeldelser om kontaktbedrageri, hvor vishing indgik som modus, udgjorde ca. 1/3 (750 ud af 2.328) af de samlede anmeldelser om kontaktbedrageri, hvilket var en markant stigning fra 2021, hvor vishing kun udgjorde ca. 9,4 % (200 ud af 2.127) af anmeldelserne (NCIK, 2023: 33+51). Til sammenligning faldt der kun domme i 5 ud af de 750 sager det år. I 2023 omhandlede størstedelen af 1.229 sager, kategoriseret som 'Andet' kontaktbedrageri, vishing (NCIK, 2024: 32). Ifølge politiforsker ved Syddansk Universitet, Adam Diderichsen, er en af årsagerne til at anmeldelsestallene er stødt stigende, at, *"Kriminalitet flytter gerne der hen, hvor der er størst udbytte og især mindst risiko for at blive opdaget og straffet"* (Kirkebæk-Johansen & Jorsal, 2023). Jesper Helbrandt, seniorrådgiver ved Institut for Cyber Risk, påpeger også, at politiet endnu ikke har stor nok kapacitet med de nødvendige kompetencer og ressourcer til at håndtere det stigende antal anmeldelser (Ibid.). Det antyder således, at selvom sager om digital svindel med vishing som modus, ikke nødvendigvis overskrider landegrænser, er efterforskningen, og dermed retsforfølgelsen, af disse sager alligevel udfordret. Vi finder det derfor relevant at undersøge følgende problemformulering:

Hvordan forebygges der aktuelt mod digital svindel, hvor vishing indgår som kontaktmodus, i en dansk kontekst? Og hvilke muligheder kan der være for at styrke forebyggelsen yderligere?

1.2 Afgrænsning

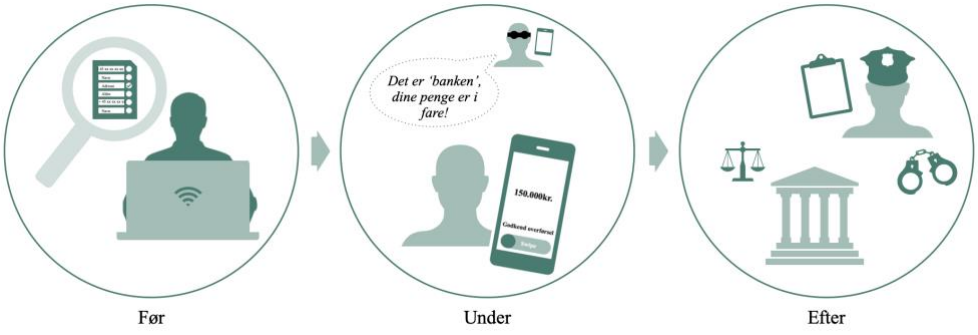
I denne undersøgelse afdækker vi, hvilken forebyggelse, der foretages af udvalgte aktører før, under og efter kriminaliteten udføres, men afgrænser os fra at inddrage hvidvask og brugen af muldyr i stadiet efter udførelsen af selve vishingangrebene.

Før den digitale svindel, hvor vishing anvendes som modus (herefter betegnet 'vishing'), udføres, anvender de kriminelle bl.a. computere og internettet til at finde kontaktinformation om potentielle ofre og planlægge hvordan kriminaliteten skal udføres. En del af planlægningen kan involvere smishing (SMS) og/eller phishing (E-mail), da der i nogle tilfælde sendes SMS'er eller E-mails ud med henblik på at få forurettede til at rette direkte henvendelse til gerningspersonerne. Dette under påskud af, at de kriminelle er den person/virksomhed/ myndighed, de udgiver sig for at være (Forbrugerrådet Tænk, 2023).

Under udførelsen af vishingforsøg forsøger de kriminelle, gennem telefonisk kontakt, at overbevise den forurettede om handlingens legitimitet vha. social engineering strategier. Vishing er i sig selv en form for social engineering, hvor gerningspersonerne eksempelvis kan *spoofe* opkalds-ID'et på opkaldet, så det ligner at det er den forurettedes bank, der ringer vedkommende op, og binde den forurettede en falsk fortælling på ærmet (NCIK, 2024: 29). Med afsæt i David S. Walls typologier om cybercrime, betegner vi vishing som computer-assisterede forbrydelser (Viano, 2016: 5), idet forbrydelsen udføres vha. computerteknologier.

Efter svindlen har fundet sted, kan der, som ved alle former for kriminalitet laves en politianmeldelse, som jf. retsplejeloven § 742, stk. 2 igangsætter en efterforskning, der kan lede til retsforfølgelse af de kriminelle.

Figur 1*: Før, under og efter vishing*



Note: Egen illustration

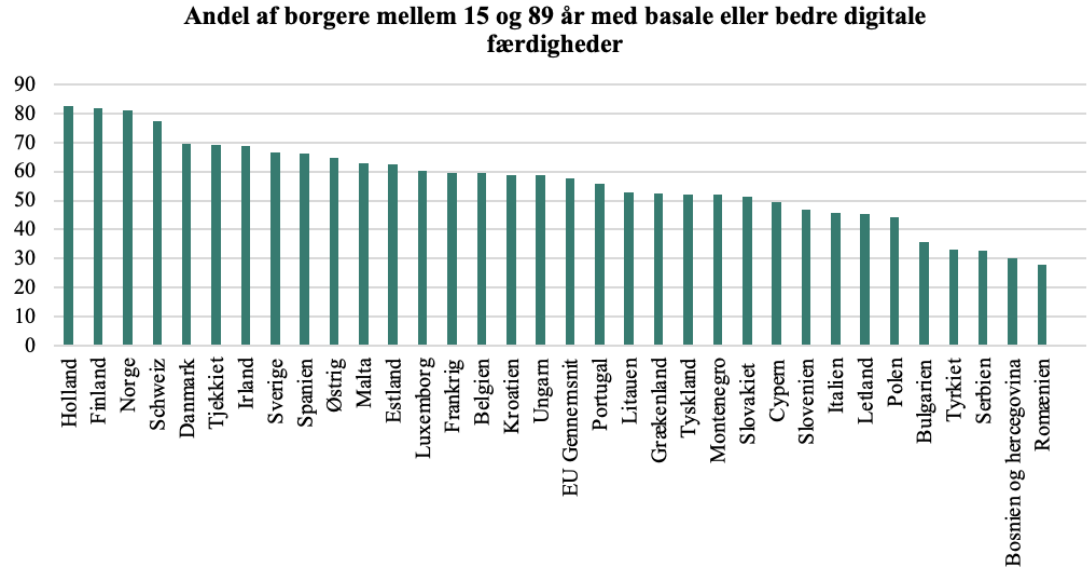
2. Baggrundsviden

Formålet med afsnittet er at give læseren en bedre baggrundsviden til undersøgelsens problemfelt. Først redegør vi for samfundets digitaliseringsniveau og dets indvirkning på det nuværende kriminalitetsbillede, samt hvordan kriminalitetsbilledet aktuelt ser ud. Derigennem redegør vi for, hvilke former for it-relateret økonomisk kriminalitet vishing indgår som modus i. Afsluttende beskriver vi, hvordan kriminaliteten udfordrer politiets efterforskning og hvad vores indledende undersøgelse af problemfeltet peger på, er forudsætningerne for den nuværende forebyggelse.

2.1 Digitalisering og kriminalitet

Danmark er et af de mest digitaliserede lande i Europa, hvor 92 % af befolkningen mellem 16 og 74 år har en smartphone (Jacobsen et al., 2023: 14) og omkring 78 % af befolkningen mellem 15 og 89 år anvender internettet dagligt (Ibid.: 7). I EU-kommissionens årlige undersøgelse af europæiske borgeres digitale færdigheder fra januar 2024, fremgår det, at 69 % af den danske befolkning mellem 15 og 89 år, mener at de har basale eller gode digitale færdigheder, hvilket placerer Danmark på en europæisk 5. plads, og over det europæiske gennemsnit (Eurostat, 2024).

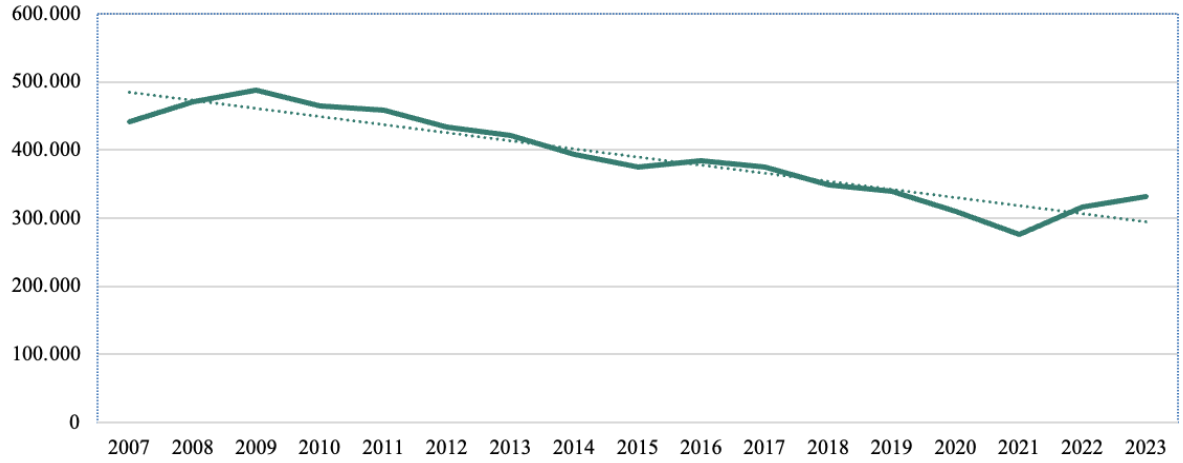
Figur 2*: Europæiske digitale færdigheder 2023*



Kilde: Eurostat, Databrowser: Individuals' level of digital skills Digital skills

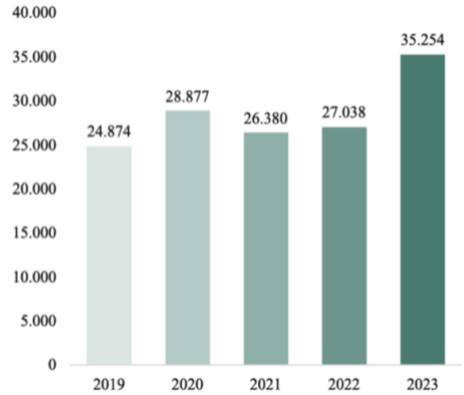
Digitaliseringen af dagligdagen kan dog blive udnyttet til at skabe nye kriminalitetsformer eller anvendt som et nyt redskab til at udføre eksisterende kriminalitetsformer. I 2023 blev der for andet år i træk ikke begået et eneste fysisk bankrøveri i Danmark (Finans Danmark, 2024 *a*). Til gengæld er forekomsten af it-kriminalitet steget. Hovedtallene for Justitsministeriets Offerundersøgelser fra 2005-2022, viser at 3,5 % af respondenterne i 2022 havde været udsat for digital svindel, hvilket svarer til omkring 169.000 personer i alderen 16-74 år (Pedersen et al., 2023: 25). På trods af at kriminalitetsniveauet i Danmark overordnet er faldende og langt de fleste (87 %) af danskerne mellem 15 og 89 år mener, at de har tilstrækkelig viden om it-sikkerhed (Jacobsen et al., 2023: 62), stiger antallet af anmeldelser om it-relateret økonomisk kriminalitet kontinuerligt:

Figur 3*: Dansk kriminalitetsudvikling 2007-2023*



Kilde: Danmarks Statistik (n.d. b), register: STRAF11 Anmeldte forbrydelser

Figur 4*: Anmeldelser om IT-relateret økonomisk kriminalitet 2019-2023*



Kilde: NCIK, 2024: 13[1]

[1]2020 var et særligt år med nedlukning af samfundet pga. Covid-19 epidemien.

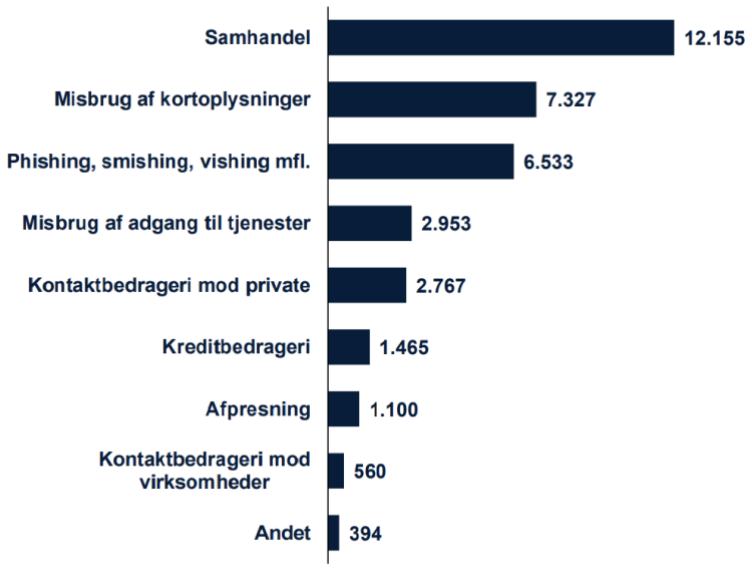
Stigningen i anmeldelser om it-relateret økonomisk kriminalitet begyndte allerede for et årti siden. Mellem 2014-2018 steg antallet af anmeldelser om it-relateret økonomisk kriminalitet med 188 % (Rigspoliti & Rigsadvokaten, 2020). Den eksponentielle stigning førte i december 2018 til oprettelsen af NCIK, dengang LCIK (Landsdækkende Center mod IT-relateret Kriminalitet) (Retsudvalget, 2022: 1).

2.2 NCIK

Formålet med at oprette NCIK var at styrke indsatsen mod it-relateret økonomisk kriminalitet og skabe et samlet overblik på landsplan. NCIK modtager alle landets anmeldelser om it-relateret økonomisk kriminalitet og står for den indledende efterforskning af en sag. Hvis sagen ikke henlægges, sendes den ud til den pågældende politikreds, der får til opgave at videreføre efterforskningen og eventuelt føre sagen til sigtelse (Ibid.: 1). NCIK er organiseret under den Nationale enhed for Særlig Kriminalitet (NSK). Den nationale samling af sager gør det muligt for NCIK at identificere mønstre på tværs af politikredse og sammenkæde sagerne (Rigspolitiet, 2019). Det skaber ligeledes overblik på fordelingen af, hvilke typer af it-relateret økonomisk kriminalitet, der anmeldes og hvilke dele af populationen, der primært rammes, hvilket styrker forebyggelsesarbejdet (Rigspolitiet, 2021). NCIKs forebyggelsesarbejde uddybes i afsnit 2.4 Forebyggelse.

NCIK inddeler anmeldelserne i ni søgenøgler: Afpresning, Kontaktbedrageri mod private, Kontaktbedrageri mod virksomheder, Kreditbedrageri, Misbrug af adgang til tjenester, Misbrug af kortoplysninger, Samhandel, Tværgående tema og Andet (NCIK, 2024: 14). 'Andet' dækker over sager, der falder uden for NCIKs søgenøgler eller endnu ikke er blevet tildelt en søgenøgle.

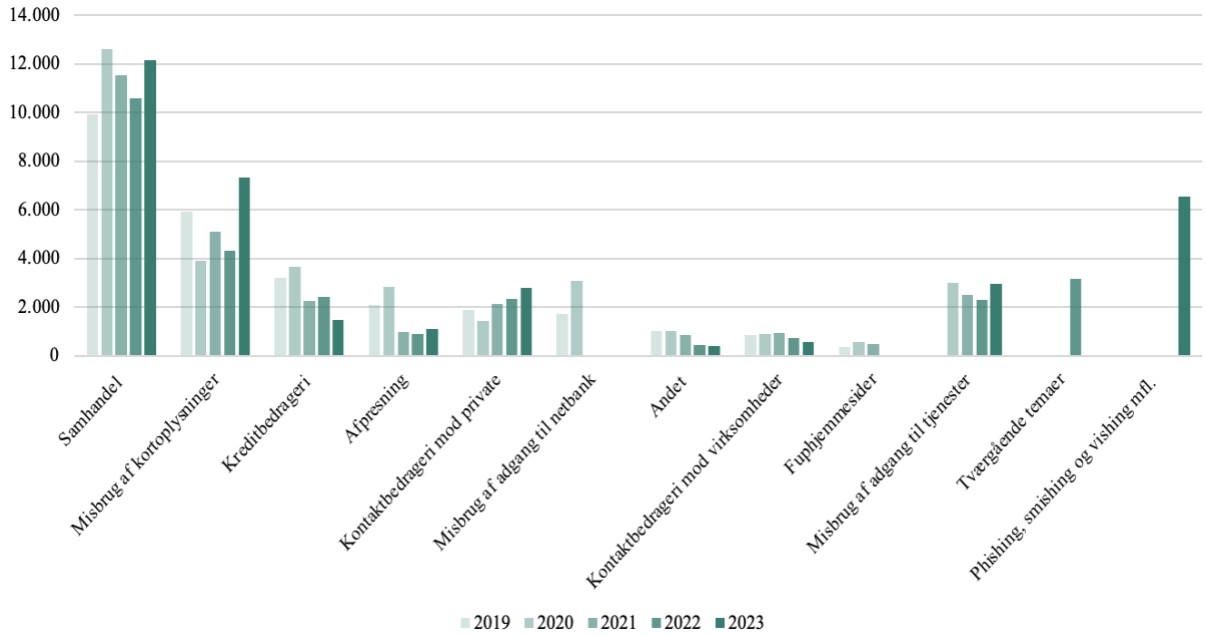
Figur 5: *Fordeling af anmeldelser om it-relateret økonomisk kriminalitet til NCIK 2023*



Kilde: NCIK, 2024: 14

Nogle anmeldelser indeholder flere kriminalitetsformer, hvortil NCIK anvender prioriteringsnøgler, der angiver hvilken søgenøgle anmeldelsen skal tælles med i (Ibid.: 10). Ved at dykke ned i NCIKs årsrapporter for 2019-2023, kan der ses nærmere på udviklingen af anmeldelser fordelt på søgenøgler:

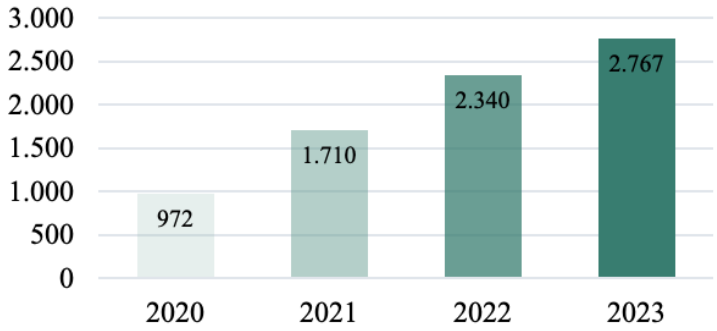
Figur 6: *Udvikling i anmeldelser fordelt på søgenøgler 2019-2023*



Note: Figuren er lavet på baggrund af LCIK og NCIKs årsrapporter. Kilde: LCIK: 2020, 2021 & NCIK: 2022, 2023, 2024

Figur 6 viser en interessant udvikling, der bl.a. afspejler at NCIK løbende opdaterer deres kategoriseringer, hvilket udfordrer sammenligningsgrundlaget fra år til år. Eksempelvis er der i årsrapporten for 2023 tilføjet en ny kategori, 'Phishing, smishing og vishing mfl.', som erstatter 'Tværgående temaer'. Den nye kategori dækker over sager, hvor anmeldelsen enten er mangelfuld eller det er svært at afgøre, hvad sagen handler om (NCIK, 2024: 14). I størstedelen af sagerne under denne søgenøgle er der heller ikke rapporteret et økonomisk tab. Phishing, smishing og vishing indgår også som modus i anmeldelser, der kategoriseres under andre søgenøgler. Figuren viser ligeledes, at antallet af anmeldelser vedrørende Kontaktbedrageri mod private (fremover omtalt som 'kontaktbedrageri') er den eneste søgenøgle, der kontinuerligt er steget i antal de sidste fire år, på nær 2020, som var et særligt år pga. covid-19 (NCIK, 2023: 13).

Figur 7: *Udvikling i antal af anmeldelser om Kontaktbedrageri mod private 2020-2023*



Kilde: NCIK, 2024: 32[2]

Den ledende politiinspektør for NSK, udtaler at en af årsagerne til den vedvarende stigning i anmeldelser om kontaktbedrageri, er at disse kriminalitetsformer fungerer som social engineering til at omgå digitale sikkerhedsforanstaltninger, der implementeres for at forhindre andre former for it-relateret økonomisk kriminalitet (NSK, 2022). Implementeringen af sikkerhedsforanstaltninger mod it-relateret økonomisk kriminalitet, er således med til at øge gerningspersoners brug af social engineering, hvilket øger forekomsten af kontaktbedrageri og måder hvorpå kontaktbedrageri kan foregå.

[2]Tallene i figur 6 afviger fra tallene i figur 5, fordi NCIKs årsrapporter kontinuerligt justeres efter sagsbehandling. Tallene i figur 5 er angivet efter hvert års årsrapport og tallene i figur 6 er angivet efter den de nyjusterede tal årsrapporten for 2023.

2.2.1 Kontaktbedrageri

Kontaktbedrageri anvendes som en fælles søgenøgle for svindeltyper, hvor gerningspersonen får kontakt til forurettede gennem digital henvendelse og får vedkommende til at overføre eller udlevere værdier og/eller personlige oplysninger under falske forudsætninger (NCIK, 2024: 31). Søgenøglen opdeles i seks svindeltyper, der betegner hvordan den forurettede er blevet bedraget: Bekendt i knibe, Datingsvindel, Falske konkurrencer, Falske låne/investerings-muligheder, Nigeriabreve og Andet (NCIK, 2023: 32-33). I hver af de seks svindeltyper kan gerningspersonen anvende forskellige midler til at kontakte og overbevise den forurettede. Følgende tabel 1 præsenterer en oversigt over de forskellige svindeltyper, hvad bedrageriet består af og hvilket middel der ofte anvendes til at oprette kontakt mellem gerningsperson og forurettede. Oversigtens beskrivelser er formuleret ud fra informationerne i årsrapporterne for 2022 og 2023:

Tabel 1: *Svindeltyper jf. NCIKs årsrapporter*

Type	**Bedrageriets indhold**	**Middel**
Bekendt i knibe	Gerningspersonen udgiver sig for at være en person forurettede kender, som har brug for akut økonomisk hjælp.	SMS, chattjenester, Facetime og e-mail
Datingsvindel	Gerningspersonen påtager sig en falsk identitet til, gennem længere tid, at opbygge en tæt, følelsesmæssig relation til forurettede med henblik på at opfinde en økonomisk nødsituation, som forurettede vil hjælpe til med, ved at overføre store pengebeløb.	Datingsider, chattjenester, telefon, e-mail.
Falske konkurrencer	Gerningspersonen opretter en falsk konkurrence, som forurettede skal betale for at deltage i.	Hjemmesider, e-mail og sociale medier.
Falske låne/investeringsmu ligheder	Gerningspersonen kontakter forurettede gennem falske annoncer eller direkte besked på sociale medier og overbeviser forurettede om at investere i en falsk investerings-/låneside.	Annoncer, sociale medier, chattjenester, telefon og e-mail
Nigeriabreve	Gerningspersonen udgiver sig for at være en person fra udlandet, fx en advokat, der vil informere forurettede om at de har en stor arv til gode, som forurettede kan indløse ved at betale arveafgift, hvorefter 'arven' aldrig udbetales.	E-mail
Andet	Dækker over forskellige former kontaktbedrageri, som ligger udenfor de andre svindeltyper. I 2022 omhandlede størstedelen af anmeldelserne i denne kategori vishing, hvor gerningspersonen får forurettede til at udlevere personlige informationer eller værdier ved fx at udgive sig for at være en myndighedsperson.	E-mail, telefonopkald, sms, chattjenester og sociale medier.

Kilde: NCIK, 2023: 32-33; NCIK, 2024: 31

Udover Kontaktbedrageri, er smishing, vishing og phishing identificeret i sager under søgenøglerne Misbrug af kortoplysninger, Misbrug af adgang til tjenester, Kreditbedrageri og Kontaktbedrageri mod virksomheder. Der er i alt 13.632 sager på tværs af søgenøgler i 2023, hvor smishing, vishing eller phishing er identificeret som modus (NCIK, 2024: 43). I 553 af disse sager, er to af disse modi blevet identificeret i samme sag (Ibid.).

2.3 Efterforskning

Digitalisering, spoofing (Teknisk sløring af afsender-ID) og social engineering gør det nemmere for gerningspersonerne at lave flere vellykkede svindelforsøg på kortere tid, hvilket medfører et fortsat stigende antal anmeldelser (NCIK, 2024: 29). Den stigende mængde sager udfordrer politiets behandlingstider, hvilket var en af årsagerne til at den daværende regering og seks af Folketingets partier i 2020 indgik en flerårsaftale for Politiet og Anklagemyndigheden, gældende for 2021-2023 (Justitsministeriet, 2020). Formålet med aftalen var at tildele ressourcer til at styrke politiets og anklagemyndighedens indsats "*...mod den alvorlige, økonomiske, organiserede og it-relaterede kriminalitet, som har en stadig voksende trussel mod samfundet"* (Ibid.: 1). Med aftalen ønskede aftaleparterne at opretholde borgernes tillid til retssamfundet og sikre retfærdighed for de forurettede. Tiltagene til at forbedre bekæmpelsen af it-relateret økonomisk kriminalitet omfatter bl.a. optimering af politiets og anklagemyndighedens arbejde og it-støtte, udvidelse af politiuddannelsens optag, nedbringelse af sagsbehandlingstider og værktøjer til prioritering af sager (Ibid.: 2). Prioriteringsværktøjerne handlede om at give politi og anklagemyndigheden mulighed for at inddrage yderligere 'relevante hensyn', når der tages stilling til, hvorvidt en sag skal efterforskes. Relevante hensyn er f.eks. hvorvidt anmelderen har lidt et tab og omfanget af det, samt prioritering efter typer af it-relateret økonomisk kriminalitet (Ibid.: 18).

Politiet og Anklagemyndigheden har, foruden disse tiltag, allerede brede muligheder for at prioritere i sager jf. retsplejelovens § 742, f.eks. ved at henlægge sager (Retsudvalget, 2022: 2-3). Henlæggelse er fortsat blevet anvendt i sager om kontaktbedrageri under aftalens forløb, på trods af at der generelt er større økonomiske tab for forurettede i disse sager (Ibid.: 2). I Rigsrevisionens beretning om Politiets efterforskning, af bl.a. it-relateret økonomisk kriminalitet fra 2019-2022, "*... er det årlige antal henlæggelser i NCIK steget med 500 %*" (Abildgaard et al., 2023: 19). I 2022 modtog NCIK 2.328 anmeldelser om kontaktbedrageri og

henlagde samme år 1.088 sager om kontaktbedrageri (Bilag 1). En af årsagerne til at sagerne henlægges er, at efterforskningen ofte kræver samarbejde med udenlandske myndigheder, fordi sagerne typisk er kendetegnet ved, at de digitale spor kan følges til udlandet (Retsudvalget, 2022: 2). Udenlandske myndigheder bliver dog kun inddraget i en efterforskning, hvis det danske politi har en rimelig formodning om at de udenlandske myndigheder kan yde assistance og det forventes at gerningspersonen kan udleveres (Ibid.: 3). Der vil ikke være en rimelig formodning om at kunne få udenlandsk assistance, hvis sagen handler om; et enkeltstående tilfælde af kriminalitet, efterforskningsmulighederne er begrænsede og ressourcekrævende ift. kriminalitetens art og alvorlighed, eller en domfældelse kun vil føre til en mindre straf (Ibid.: 4-5).

I Rigsrevisionens beretning om politiets efterforskning, har statsrevisorerne bemærket, at "*I de sager om økonomisk it-kriminalitet, som NCIK sendte til politikredsene i 2019, havde NCIK gennemført en indledende efterforskning i ca. ⅔ af sagerne. I 2022 gjaldt dette for mindre end halvdelen af sagerne, NCIK sendte videre til politikredsene"* (Abildgaard et al., 2023: 17). Det skyldes bl.a. at Rigspolitiet, i anden halvdel af 2022, besluttede at NCIK skulle iværksætte en oversendelsesproces pga. stor ophobning i NCIKs sagsbeholdning. Omkring 25.000 sager blev derfor sendt videre til politikredsene, uden en indledende efterforskning i NCIK (Ibid.: 20). Rigsrevisionen har dog fundet, *"... at der er en signifikant større sandsynlighed for, at politikredsene kan rejse sigtelse mod en formodet gerningsperson i de sager, hvor NCIK har gennemført en indledende efterforskning… "* (Ibid.: 25). Ifølge Rigspolitiet har NCIKs primære formål ændret sig, så NCIK ikke længere skal stå for den indledende efterforskning i en sag, men kan, "*... hvis de tidsmæssige og økonomiske rammer tillader det*" (Ibid.: 18). Ifølge Rigsrevisionen er det dog ikke et spørgsmål om ressourcer, da det står beskrevet i cirkulæret for NCIK og i Rigspolitiets beskrivelse af NCIK fra 2022, at NCIK skal gennemføre den indledende efterforskning, inden sagerne sendes ud til politikredsene (Ibid.: 18). Selvom de ca. 25.000 sager blev sendt videre fra NCIKs sagsbeholdning i 2022, var der stadig 25.181 sager ophobet i slutningen af 2022, som havde en gennemsnitsalder på 604,3 dage (Ibid.: 3+17). NCIKs gennemsnitlige sagsbehandlingstid (fra NCIK modtager en anmeldelse, til sagen sendes videre til en politikreds) er steget fra 77,1 dage i 2019 til 157,3 dage i 2022 (Ibid.: 23) Når den indledende sagsbehandling tager lang tid, er der risiko for at spor går tabt. Eksempelvis bliver oplysninger, der kan identificere ejeren af en anvendt IP-adresse i en sag, slettet efter et år (Ibid.: 19+25). Derudover kan sagerne blive forældet, hvorefter der ikke kan retsforfølges. Det stigende antal anmeldelser gør det således svært for NCIK at følge med efterforsknings-

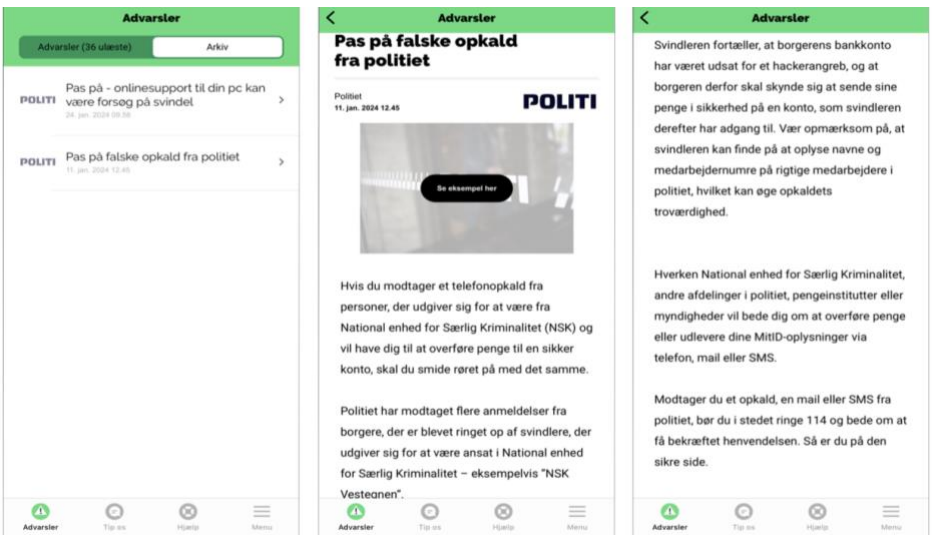
mæssigt, hvilket i sidste ende kan lede til at flere gerningspersoner går fri og de forurettedes retsfølelse bliver krænket.

2.4 Forebyggelse

NCIK har oprettet forebyggelsessamarbejdet, Forum mod IT-relateret økonomisk kriminalitet (FIT), som blev etableret i 2015 på baggrund af politiets *co-creation metode* (Rigspolitiet, 2021: 30). Siden 2014 har politiet anvendt co-creation metoden til at "... *etablere helhedsorienterede, tværsektorielle samarbejder med relevante myndigheder, private virksomheder, borgere m.fl.* [for at] *skabe værdifulde løsninger på udfordringerne på tværs af aktører*" (Ibid.: 5). Politiet anvender co-creation metoden, når den pågældende kriminalitetsform er så kompleks, at der ikke findes effektive løsningsmuligheder internt i politiet (Ibid.). I FIT samarbejder NCIK med private og offentlige organisationer om at forebygge og mindske forekomsten af it-relateret økonomisk kriminalitet (Politi, n.d. *a*). FIT-samarbejdet giver aktørerne mulighed for at dele viden med hinanden og samarbejde om konkrete problemstillinger (Bilag 2).

I 2017 førte FIT-samarbejdet til udviklingen af app'en "Mit digitale selvforsvar", udviklet af Forbrugerrådet Tænk, i samarbejde med Det Kriminalpræventive Råd (DKR) og Trygfonden (Forbrugerrådet Tænk, n.d.). Gennem app'en kan diverse aktører, inklusive politiet selv, udsende advarsler til borgerne om digitale trusler.

Billede 1: *Eksempel på vishing-advarsel på Mit digitale selvforsvar-appen, Forbrugerrådet Tænk (2017).*



FITs arbejde med it-relateret økonomisk kriminalitet adskiller sig fra politiets andre co-creation initiativer, fordi kriminalitetsformen er grænseløs. De andre co-creation initiativer er lokalt forankrede om f.eks. narkotika i Næstved og indbrud i Hjørring (Rigspolitiet, 2021: 7). Uanset geografisk afgrænsning af den pågældende problematik, deles erfaringerne fra co-creation samarbejderne både nationalt og internationalt.

Selvom FIT skaber muligheder for at de involverede aktører kan dele viden med hinanden, er der, i modsætning til det operative forebyggelsessamarbejde vedr. hvidvask- og terrorfinansiering, ODIN-netværket (Justitsministeriet, 2021), endnu ikke udarbejdet et lovforslag eller lignende, der kan gøre det muligt for FITs aktører at dele fortrolige informationer med hinanden. Udover at der ikke er juridisk grundlag for at samarbejdspartnerne i FIT kan dele fortrolige informationer med hinanden, er der yderligere udfordringer med at dele informationer blandt samarbejdspartnere, der arbejder i samme branche og dermed også samarbejder om forebyggelse af it-relateret økonomisk kriminalitet udenfor FIT. Det gælder især finanssektoren.

2.4.1 Forebyggelse i Finanssektoren

Tal fra Finans Danmark viser, at der alene i 2022 blev svindlet for 425 mio. kr. i Danmark, hvilket er en stigning på 27 % ift. 2021 (Finans Danmark, 2023: 4). I 2023 steg tallet til 627 mio. kr. (Finans Danmark, 2024 *b*). Stigningen i digital svindel har medført en intensivering af finanssektorens forebyggelsesinitiativer og bekæmpelse af heraf. Bankerne bruger årligt omkring 750 mio. kr. på at forebygge og bekæmpe digital svindel og formår at stoppe omkring 60 % af svindelforsøgene (Finans Danmark, 2023: 4). Svindelforsøg bliver standset ved at bankerne monitorerer kundernes transaktionsmønstre og stopper overførsler, der virker mistænkelige. Det kan f.eks. være, hvis der foretages flere overførsler på store beløb inden for kort tid eller der overføres til udlandet (Ibid.: 10-11). I bekæmpelsen af digital svindel arbejder bankerne således tæt sammen med deres kunder. Indsatsen mod digital svindel har derfor medført en stigning i oplysningskampagner, som sendes direkte ud til kunderne gennem netbank, bankernes hjemmesider, Mit Digitale Selvforsvar-app'en, sociale medier og lign. (Ibid.: 14). Da svindelforsøg spredes gennem forskellige medier, samarbejder bankerne ligeledes med andre sektorer såsom Teleindustrien og e-mail domæner for at sikre beskyttelse af privatpersoners konti og informationer. Eksempelvis har alle danske banker implementeret

DMARC, som er en godkendelsesprotokol til e-mail, der reducerer risikoen for at kunderne modtager spoofede e-mails (Ibid.: 16). Derudover er banksikkerhedssamarbejdet, FinansCERT, etableret for at bankerne kan dele viden med hinanden om, hvordan og på hvilke platforme de kriminelle udfører deres handlinger. Ved at dele viden med hinanden kan bankerne bl.a. hurtigere lukke falske investeringshjemmesider (Ibid.). Finans Danmark har etableret en Svindel Task Force, der i slutningen af 2024 vil komme med anbefalinger til tiltag for at bekæmpe digital svindel (Ibid.: 19). Som led i udarbejdelsen af anbefalingerne, skal Svindel Task Forcen pege på, hvilke lovgivningsmæssige udfordringer, der står i vejen for at bankerne kan implementere effektive forebyggelsestiltag (Ibid.).

I modsætning til hvidvask- og terrorfinansieringsområdet, er der endnu ikke udarbejdet deciderede lovforslag, der kan styrke grundlaget for vidensdelingen i samarbejder om bekæmpelse og forebyggelse af digital svindel mellem bankerne og andre aktører. Der findes, som tidligere beskrevet, allerede tværsektorielle samarbejder mellem banker, politi og andre, som f.eks. det i FIT. Svindel Task Forcen er også et samarbejde mellem den nuværende regering, Finans Danmark, Forbrugerrådet Tænk, Teleindustrien og Ældre Sagen om at implementere en række initiativer for at bekæmpe digital svindel (Ibid.: 20). Initiativerne implementeres i løbet af 2024 og omhandler følgende fire tiltag:

1. Bankerne sænker beløbsgrænsen for straksoverførsler pr. dag fra 500.000 kr. til 50.000 kr. Beløb derover vil kun blive godkendt ved at rette kontakt til sin bank.
2. Finans Danmark opfordrer deres medlemmer til at implementere kriminalpræventive tiltag over for kunder, der er særligt udsatte for svindel, som f.eks. fuldmagter til pårørende, der kan sænke deres næres beløbsgrænse for straksoverførsler yderligere end de 50.000 kr. (Erhvervsministeriet, 2023).
3. Teleindustrien vil sammen med teleselskaberne gøre det muligt at beskytte legitime afsendernavne på SMS'er, således at de ikke kan spoofes af andre.
4. Finans Danmark, Forbrugerrådet Tænk, Teleindustrien og Ældre Sagen vil sammen fortsætte med at styrke oplysningsindsatsen, rettet mod borgerne.

(Finans Danmark, 2023: 20)

De fire initiativer i Svindel Task Forcen, samt udviklingen af Mit Digitale Selvforsvar-app'en gennem FIT-samarbejdet, søger alle at styrke borgerens modstandsdygtighed. Et lignende

fokus ses i anbefalingerne fra NCIKs årsrapport fra 2022, hvor det påpeges, at forebyggelsen af it-relateret økonomisk kriminalitet kræver oplysning og adfærdsændring hos befolkningen:

> "*Det handler også om at klæde særligt udsatte dele af befolkningen bedre på til at beskytte sig selv digitalt. Det gælder om at ruste dem til at søge og forstå viden om de tekniske foranstaltninger, man kan implementere for at forebygge, at gerningspersoner kan opnå kontakt og få held med at manipulere forurettede"* (NCIK, 2023, 51).

Det tyder således på, at de nuværende forebyggelsestiltag mod it-relateret økonomisk kriminalitet i Danmark, og dermed vishing, særligt består af oplysningskampagner til borgerne, og at beskyttelsen mod digital svindel således, i høj grad, hviler på borgernes egen viden og kompetencer, hvilket undersøges nærmere i analysen.

3. Begrebsafklaring

Tabel 2: *Begrebsafklaring*

Begreb	Definition
Vishing	Telefonsvindel, hvor forurettede narres til enten at udlevere personlige oplysninger eller penge, som de kriminelle kan udnytte, eller til selv at foretage en pengeoverførsel til de kriminelle (Finans Danmark, n.d. *a*). Vishing vil gennem specialet blive anvendt som betegnelse for svindel(forsøg), hvor telefoner er anvendt som kontaktmodus. Både alene eller i kombination med andre former for kontaktmodus som f.eks. smishing eller phishing.
Phishing	Phishing er en metode, hvor svindlere gennem e-mail forsøger at narre forurettede til at oplyse personlige oplysninger (kreditkort- eller netbankoplysninger). I mailen opfordres forurettede til at indsende oplysninger per e-mail eller indtaste dem via link til en falsk internetside (Det Kriminalpræventive Råd, n.d.).
Smishing	Smishing er en metode hvor svindlere gennem SMS forsøger at narre forurettede til at oplyse personlige oplysninger (kreditkort- eller netbankoplysninger). I SMS opfordres forurettede til at trykke på et link til en falsk hjemmeside og indtaste personlige oplysninger, eller til at ringe til et telefonnummer angivet i SMS'en (Det Kriminalpræventive Råd, n.d.).
Modus	Kontaktmodus beskriver gerningspersoners måde at kontakte forurettede på, med henblik på at udsætte dem for digital svindel, som f.eks. vishing, der dækker over telefonisk kontakt (NCIK, 2024: 43). Gennem specialet omtales kontaktmodus som 'modus'.
Kontaktbedrageri	Betegner en forskellige former for digital svindel, hvor svindlere/bedrager/gerningsperson tager personlig kontakt til forurettede og, i nogle tilfælde, bruger tid på at opbygge en relation, hvorved svindlerne kan få forurettede til enten at overføre penge eller udlevere personlige oplysninger (NCIK, 2024: 31-32).
Spoofing	Spoofing er en teknisk måde at ændre visningen af et telefonnummer på modtagerens telefon. Ved at spoofe et telefonnummer kan personer således ringe og udgive sig for en anden end de i virkeligheden er (NCIK, 2024: 29).
Social engineering	Metoder til at manipulere forurettede til at omgå sikkerhedsforanstaltninger ved selv at autorisere overførsler til gerningspersonen eller udlevere personlige oplysninger, der misbruges af gerningspersonen (NCIK, 2024: 25). Metoderne dækker både over Spoofing, vishing, smishing, phishing og diverse overtalelsesteknikker.
Techgiganter	Internationale IT-virksomheder som Google, META (bl.a. Facebook og Instagram) og Apple (Den Danske Ordbog, n.d.)

4. Litteraturreview

I dette afsnit præsenteres noget af den eksisterende relevante forskningslitteratur om vishing for at give læseren indblik i det forskningsfelt, vi skriver specialet ind i. Vishing udføres, som tidligere beskrevet, ofte i kombination med phishing og/eller smishing. Dette afspejles i forskningslitteraturen, hvor der kun findes et begrænset antal forskningsartikler om vishing som isoleret fænomen. Vi har anvendt databaserne Google Scholar og Primo til at søge efter eksisterende forskning med følgende søgeord; "*vishing", "voice phishing", "prevention of online fraud", "prevention of voice phishing", "online fraud", "preventing online fraud" og "phone scams".*

4.1 Crime scripts analyser af vishing

Store dele af forskningslitteraturen, der handler om vishing som isoleret fænomen, er foretaget som crime scripts analyser og sigter mod at forklare gerningspersonernes fremgangsmåde. De fleste studier er foretaget i Asien, hvor kriminalitetsformen blev rapporteret for første gang i Taiwan i 2002 og senere i Sydkorea i 2006 (Choi et al., 2016: 456). I Sydkorea er der senere foretaget to undersøgelser af, hvordan vishing er organiseret som en transnational kriminel handling (Choi et al., 2016: 460; Lee, 2020: 212). Studiernes resultater er ikke direkte overførbare til en dansk kontekst, men inddrages i dette litteraturreview, idet Sydkorea, ligesom Danmark, er blandt de mest offentligt digitaliserede lande i verden (United Nations, 2022: 8). Studierne giver ligeledes indblik i gerningspersonernes modus. Derudover finder studierne, at vishing i Sydkorea udføres af kriminelle organisationer, hvor forskellige grupper har ansvar for specifikke opgaver (Choi et al., 2016: 459-460; Lee, 2020: 212).

Choi et al. (2016) studiet finder, at der indgår tre stadier i et crime script for vishing: (1) Pre-crime, (2) Criminal event og (3) Post-offense. Pre-crime stadiet består af tre hovedaktiviteter: *Forberedelse*, herunder anskaffelse af telefoner og bankkonti, og forberedelse af tekniske løsninger. *Rekruttering* af telefonsælgere og *udarbejdelse af manuskripter*, som sælgerne skal følge. Criminal event stadiet består af to hovedaktiviteter: *telefonopkald*, der typisk er automatisk genererede opkald og sender forurettede videre til en rigtig person, hvis forurettede besvarer opkaldet. Herefter begynder den anden hovedaktivitet *samtalen*, hvor "sælgeren" udgiver sig for at være fra en myndighed eller familie og venner, og følger de udarbejdede manuskripter fra forrige stadie. For at kriminaliteten kan udføres, anvendes spoofing af telefonnumre, så det ligner at de reelt ringer fra myndigheder eller familie og venner. Post-

offense stadiet består ligeledes af to hovedaktiviteter: *Ind- og udbetaling,* hvor forurettede overfører penge til en konto som gerningspersonerne råder over. Pengene bliver efterfølgende hævet, hvilket fører til den anden hovedaktivitet, *pengeoverførsler*. Under denne aktivitet flyttes de hævede penge til bagmændene, der opholder sig i Kina (Ibid.: 459-464). I et studie fra 2020 undersøger Lee ligeledes vishing som en transnational kriminel handling gennem crime script analyse og finder, i overensstemmelse med Choi et al., (2016), at angrebene foretages i de tre førnævnte stadier. Studiet adskiller sig dog ved, at Lee (2020) undersøger teknologiens rolle i vishing og finder at teknologi har en bærende rolle i udførelsen. Gerningspersoner trænes i teknologier og teknikker, der er nødvendige for at udføre kriminaliteten, idet alle faser af et vishingforsøg indebærer unikke processer med teknologiske aspekter (Ibid.: 212-214).

4.2 Social engineerings indvirkning på vishing

Vishing er, som tidligere beskrevet i afsnit 1.2, en social engineering strategi, hvor gerningspersonen overbeviser den forurettede om at afsløre personlige oplysninger eller foretage sikkerheds kompromitterende handlinger, såsom at udlevere kodeord og brugernavn eller autorisere en bankoverførsel (Jones et al., 2020: 314; Ashfaq et al., 2024: 412; Armstrong et al., 2023: 275). Et studie af Jones et al. (2020), undersøger og identificerer, hvordan gerningspersoner implementerer overbevisningsprincipper i deres strategi for at få følsomme oplysninger ud af de forurettede. Studiet identificerer forskellige kombinationer af overbevisningsprincipper, samt hvordan de anvendes af gerningspersonerne. Overbevisnings-principperne der undersøges er: (*A) Authority*, at mennesker er tilbøjelige til at stole på autoriteter og betragte dem som eksperter; (C) *Commitment, reciprocation, and consistency*, at mennesker føler sig sikre i deres beslutninger, når de har sagt dem højt eller offentligt har forpligtet sig til en handling. Derudover har mennesker tendens til at tro på at andre taler sandt, når de fortæller, de vil hjælpe, hvilket skaber en følelse af forpligtelse til at gengælde handlinger; (D) *Distraction,* at mennesker fokuserer på deres egne behov, tidspres samt potentielle gevinster og tab, som distraherer dem fra, hvad der ellers foregår i situationen; (L) *Liking, similarity and deception,* at mennesker har tiltro til personer de er bekendte med, kender godt, kan lide og/eller er tiltrukket af; og (S) *Social proof,* at mennesker har tendens til at følge med strømmen, fordi de ønsker at være en del af gruppen og derved føler mindre ansvar for deres handlinger, når andre deltager i de samme adfærdsmønstre og risici (Ibid.: 317).

Resultaterne af undersøgelsen viser, at (A) Authority anvendes i langt størstedelen af de 86 undersøgte vishingforsøg, efterfulgt af (S) Social proof, (D) Distraction og (L) Liking, similarity and deception (Ibid.: 319). (C) Commitment, reciprocation, and consistency er således det overbevisningsprincip, der anvendes mindst i vishingforsøg (Ibid.: 319). De fem overbevisningsprincipper anvendes i forskellige kombinationer med hinanden i vishingforsøg, og den mest anvendte er en kombination af de fire mest anvendte principper ASDL. Her udgiver gerningspersonen sig for at være fra kendte institutioner og forsøger herved at overbevise forurettede om, at der er personlige fordele ved at efterkomme 'institutionens' (gerningspersonens) anmodning om eksempelvis at udlevere fortrolige oplysninger (Ibid.: 325).

I et andet studie foretaget af Armstrong et al. (2023) undersøges, opfattelsen af ærlighed i vishingopkald før, under og efter at gerningspersonerne forsøger at få forurettede til at udlevere oplysninger. Det undersøges yderligere om opfattelsen af ærlighed varierer afhængigt af, hvor følsomme oplysninger gerningspersonen forsøger at lokke ud af den forurettede. Der opstilles hertil scenarier, som er baseret på rigtige hændelser med vishing (Armstrong et al.: 278-279). Resultaterne viser, at opfattelsen af ærlighed varierer efter modus. Ved de scenarier, hvor gerningspersonerne forsøger at få følsomme oplysninger ud af den forurettede, falder tilliden i løbet af opkaldet og ærligheden af opkaldet vurderes derfor at være lav (Ibid.: 280-281). Forfatterne peger på, at gerningspersonerne udnytter det de beskriver som 'truth-default state' hos den forurettede, hvilket dækker over at individer som udgangspunkt antager at andre er ærlige, og derfor kun antager at andre lyver, hvis der er nogle tydelige tegn på det (Ibid.: 276). Gennem social engineering er det muligt at fastholde den forurettede i denne 'truth-default state', hvilket kan være en forklarende faktor for, hvorfor de efterlever gerningspersonernes anvisninger (Ibid.: 283).

4.3 Forebyggelse af online svindel

I forskningslitteraturen fremgår det, at vishing er blevet en mere almindelig kriminalitetsform i de senere år, som kan have alvorlige konsekvenser (Ashfaq et al., 2024: 413; Choi et al., 2016: 454). Der kan gennem forskningslitteraturen identificeres forskellige forebyggelsesstrategier, der kan opdeles i tre komponenter: *forebyggende teknikker (prevention techniques)*, *afbødningsteknikker (mitigation techniques)* samt *uddannelse af brugerne (brugeruddannelse) og oplysningskampagner* (Ashfaq et al., 2024: 415). Forebyggelsesstrategierne er således både funderet i tekniske løsninger og kampagner målrettede borgerne. I et litteraturstudie undersøger

Ashfaq et al. (2024: 411-412) forskellige forebyggelses- og begrænsningsteknikker. Gennem undersøgelsen evaluerer forfatterne ligeledes på effektiviteten af de forskellige teknikker og fremhæver styrker og svagheder ved disse. Studiet identificerer tre teknikker ved hver af de tre komponenter, der har til formål enten at stoppe et vishingforsøg inden det udføres, minimere skaderne af et angreb, eller uddanne og advare borgerne om vishing, så de kan identificere kriminaliteten og ved hvordan de skal reagere, hvis de udsættes for det. Forfatterne fremhæver i forlængelse heraf, at teknikkerne ikke kan stå alene og at en effektiv forebyggelsesstrategi bør indeholde teknikker fra alle tre lag (Ibid.: 417-418). Studiet fremhæver opkalds-ID autentifikation som en effektiv teknisk løsning i en forebyggelsesstrategi (Ibid.: 419). Det er dog fortsat muligt for gerningspersonerne, at omgå disse blokeringsteknologier ved at spoofe opkalds-ID, hvorved gerningspersonen kan få det til at se ud som om opkaldet er fra en troværdig afsender (Armstrong et al.: 2023: 275).

Som en af de mest effektive teknikker i en forebyggelsesstrategi fremhæver Ashfaq et al. (2024: 419) uddannelse af borgerne og oplysningskampagner. Gennem uddannelse og kampagner er det muligt at træne borgerne i at identificere mistænkelige telefonopkald og undgå at give følsomme oplysninger ud, samt oplyse om farerne ved vishingangreb. Det er dog ikke alle dele af forskningslitteraturen, der er kommet frem til samme konklusion, særligt når det handler om kampagner. Det fremhæves i et studie af Jensen et al. (2024: 1-2), at der ikke er meget empirisk evidens for at oplysningskampagner virker efter hensigten, og at effekten af kampagnerne er aftagende. Dette fremgår ligeledes af Cross & Kelly (2016: 816), hvis studie finder, at budskaberne i kampagner er kendetegnet ved en stor detaljegrad om, hvordan online svindel kan begås. Det indikerer, at detaljegraden kan have kontraproduktive effekter, idet informanterne i undersøgelsen ikke var i stand til at anvende denne viden om svindel, da de blev vist eksempler på phishing. Ifølge Cross & Kelly (2016: 810-811) kan dette skyldes, at potentielt forurettede leder efter de konkrete karakteristika eller ”plots” som beskrives i kampagnerne, men disse anvendes ikke nødvendigvis i den svindel, de udsættes for. På den baggrund argumenterer forfatterne for, at kampagnerne er præget af ”hvid støj” og anbefaler derfor, at der i arbejdet med oplysningskampagner fremadrettet fokuseres på enkelte og korte budskaber (Ibid.: 816).

Inspireret af Cross og Kellys (2016) fund, formulerede Jensen et al. (2024), i samarbejde med Spar Nord, en kort og generel advarselsbesked, de sendte ud til bankens kunder gennem netbank for at undersøge, hvorvidt sådan en advarselsbesked har en forebyggende effekt.

Jensen et al.s undersøgelse indeholder to forskellige statistiske designs, der begge opererer med en kontrolgruppe af kunder, som banken identificerede ikke har været udsat for svindel, og en gruppe af kunder, som banken ved har været udsat for svindel tidligere (Ibid.: 4). Det første er et difference-in-difference design, der sammenligner gruppernes transaktionsadfærd tre måneder før og efter beskeden blev sendt. Der tilføjes gradvist kontrolvariable som alder, uddannelsesniveau, køn og civilstatus for at tage højde for andre faktorers påvirkning af resultatet (Ibid.: 11). Det andet design er et regressions-diskontinuitetsdesign, der sammenligner transaktionsadfærd blandt kunder, der er omkring 40 år gamle, efter beskeden blev sendt (Ibid.: 12-13). Her anvendes ligeledes kontrolvariable til at determinere, hvem beskeden har størst effekt på i gruppen. Designet er afgrænset til de 40-årige, da beskeden var formuleret specifikt til denne målgruppe. Resultaterne af undersøgelsen viser, at alder generelt øger sårbarheden for at blive udsat for svindel, mens det at have en partner mindsker sårbarheden. Derudover fandt de at advarselsbeskeden havde en lille, ikke signifikant, effekt uanset svindeltype og kombination af variable. (Ibid.: 13+17).

I tråd med Jensen et al. (2024) fremhæver Brewer et al. (2019: 126), at der inden for forebyggelse af cyberkriminalitet mangler forskning af effekterne. Forfatterne fremhæver, at implementering af fremtidige cyberkriminalitetsinterventioner bør ske med evaluering for øje, og at der i udførelsen af disse bør fokuseres på undersøgelsesdesignet. Det skyldes, at forfatterne finder at randomiserede, kontrollerede forsøg, er de mest værdifulde studier, til at evaluere effekter (Brewer et al., 2019, 130+141). De anbefaler således, at forebyggelsesinterventioner mod cyberkriminalitet indtænkes både før, under og efter, ligesom fundene i Ashfaq et al.s (2024) litteraturstudie.

De australske myndigheder, i form af politi, handelsministerium og myndighed for konkurrence, forbrugeranliggender, handel og produkt-sikkerhed, har forsøgt sig med en offerorienteret tilgang til bekæmpelsen af online svindel (Cross, 2016: 130-132). Ved hjælp af denne tilgang forsøger myndighederne at identificere personer de mistænker er blevet udsat for svindel og retter herefter henvendelse til borgeren via brev, i et forsøg på at forebygge reviktimisering (Ibid.: 133). Cross (2016) undersøger i dette studie tre cases, som viser, at der var færre personer, der foretog nye oversøiske transaktioner, efter de havde modtaget et brev fra myndighederne. I nogle tilfælde har myndighederne sendt mere end et brev til personer, de mistænker for at være udsat for online svindel, og samarbejdet med banker om at blokere transaktioner (Ibid.: 131+134). Resultaterne af studiet tyder på, at det kan reducere risikoen for

at blive udsat for online svindel, hvis myndighederne intervenerer direkte til den forurettede. Studiet undersøger dog ikke, om der har været andre udslagsgivende faktorer, end brevene, der har fået de forurettede til at stoppe med at lave oversøiske transaktioner (Ibid.: 134).

I forskningslitteraturen afdækkes således en række forskellige forebyggelsesstrategier og tilgange. Der er dog ikke noget forskning der entydigt peger på, hvilke strategier eller tilgange der har den største effekt, og forskningslitteraturen er ligeledes uenig om effekten af nuværende forebyggelsestiltag.

4.4 De forurettede

Der er i forskningslitteraturen foretaget flere studier om konsekvenserne for individer, der har været udsat for online svindel. En ting der går igen i studierne er, at individer der udsættes for online svindel i mange tilfælde oplever at blive udsat for victim blaming (Cross, 2015). Cross (2015: 189) undersøger diskursen om at blive udsat for online svindel gennem interviews med 85 ældre personer, som har modtaget en svigagtig e-mail. Studiet undersøger ligeledes, hvorfor nogle ældre er mere tilbøjelige til at efterkomme anmodninger i svigagtige e-mails. Gennem interviewene afdækker Cross en stærk og gennemgående victim blaming af de forurettede. Victim blamingen baserer sig på antagelser om at de forurettede er grådige og godtroende, og mange personer tilskriver ligeledes de forurettede skyld og ansvar for deres handlinger (Ibid.: 193). Denne diskurs findes særligt blandt de informanter, der ikke efterkom anmodningen i e-mailen, men ligeledes blandt de forurettede selv (Ibid.: 201). Resultaterne af undersøgelsen viser endvidere, at victim blaming udgør en væsentlig barriere i samtaler om online svindel (Ibid.). De ældre anvender ofte humor som et middel til at distancere sig fra at anerkende deres egen sårbarhed. Humor bliver desuden en måde for de ældre at differentiere sig fra dem, der bliver udsat for svindel, og fungerer som en kollektiv måde at forstærke den negative diskurs om de forurettede (Ibid.). Ifølge Cross kan det få en række konsekvenser for de forurettedes velbefindende, idet victim blaming kan medføre, at de forurettede isolerer sig fra deres netværk og dermed ikke taler med familie og venner om det, de er blevet udsat for (Ibid.).

De forurettede for online svindel er ikke kun påvirket af victim blaming. Mange rammes ligeledes af barrierer, når de forsøger at anmelde, at de har været udsat for online svindel (Cross, 2020). I Australien, har politiets arbejde traditionelt set været territorialt afgrænset, men i takt med at kriminalitet har vundet indpas i den digitale verden, har det ændret sig og medført udfordringer ift. jurisdiktion (Ibid.: 362). Cross (2020: 358) undersøger, hvordan misforståelser

vedrørende jurisdiktion skaber forvirring omkring hvilke(n) politienhed(er) der kan efterforske online svindel i Australien. Studiet peger på, at udfordringerne med jurisdiktion kan give de forurettede en negativ oplevelse, når de anmelder sager om online svindel (Ibid.: 361). Gennem de forurettedes fortællinger afdækker Cross, hvordan der bl.a. er opstået en myte om, at det er det føderale politis ansvar at håndtere internationale lovovertrædelser. Denne antagelse er både afdækket hos de forurettede og hos lokale politikredse (Ibid.: 367-368). Flere af de forurettede har oplevet at blive sendt rundt til forskellige jurisdiktioner, ofte baseret på antagelser om, hvor pengene eller gerningspersonerne havde ophold (Ibid.: 371). Resultaterne af undersøgelsen peger først og fremmest på et øjeblikkeligt behov for forandring af politiets håndtering af sager om online svindel. Samtidig fremhæves det, at det har haft en positiv effekt at oprette en myndighed til at strømline anmeldelser om online svindel. Cross fremhæver dog, at der er plads til forbedringer og at der er et klart behov for at oplyse borgerne og skabe større gennemsigtighed for dem (Ibid.: 373).

4.5 Opsummering

I den eksisterende forskning om vishing, er det primært studier om kriminalitetstypens udførelse, såsom crime scripts, og undersøgelser af det manipulative aspekt, der undersøger vishing som et isoleret fænomen. Blandt disse studier fremhæves det at udførelsen af vishing kan opdeles i tre stadier; før, under og efter udførelsen, som kræver et omfattende planlægningsarbejde, teknisk viden og kendskab til overbevisningsteknikker for at være succesfulde. På forebyggelsesområdet fokuserer forskningen primært på tiltag, der kan afværge svindelforsøg eller oplyse borgere om potentielle risici. Forskningen mangler entydige svar på, hvilke tiltag, eller kombinationer af tiltag, der er mest effektive. Effekten af eksisterende forebyggelsestiltag er således heller ikke klart fastlagt. Studierne vedrørende viktimiseringens påvirkning på den enkelte har et bredt fokus på svindeltyper. Studierne peger primært på, at de forurettede oplever victim blaming og forvirring over anmeldelsesprocessen pga. at det digitale element udvisker politidistrikters geografiske afgrænsninger, hvilket skaber behov for nationalt at strømline anmeldelserne. Samlet set illustrerer litteraturen, at der mangler yderligere forskning af vishing, hvad end det gælder vishing som kriminalitetsform, forebyggelse af vishing, effekterne af bestemte forebyggelsestiltag eller de forurettedes oplevelser at blive udsat for online svindel. Generelt er der begrænset viden om vishing i dansk kontekst, særligt ift. forebyggelse. Med dette speciale søger vi således at bidrage med ny viden til feltet gennem detaljerede beskrivelser og gennemgange af, hvilke forebyggelsestiltag udvalgte aktører implementerer i en dansk kontekst før, under og efter vishing udføres, og med hvilket formål.

5. Teori

I afsnittet præsenterer vi de teorier, der danner grundlag for empiriindsamlingen og de efterfølgende analysedele. Først præsenteres aktør-netværk-teori, som vi anvender til at undersøge, hvilke aktører, der aktuelt tager del i forebyggelsen af vishing i Danmark og hvilke forebyggelsestiltag aktørerne implementerer. Dernæst præsenteres rutineaktivitetsteori, som vi vil anvende til at visualisere, hvordan de identificerede tiltag er tiltænkt at forhindre forekomsten af vishing. Til slut præsenteres en helhedsorienteret forebyggelsesmodel, som vi anvender til at undersøge, hvorvidt og hvorledes den nuværende forebyggelse mod vishing kan forbedres.

5.1 Aktør-netværk-teori

Den franske sociolog, filosof og antropolog, Bruno Latour, udviklede aktør-netværk-teori (ANT) som en alternativ samfundsteori, baseret på den franske sociolog, Gabriel Tardes, forståelse af videnskab og det 'sociale' (Latour, 2008: 25-27). Latour købte ind på Tardes argument om, at samfundet i sig selv ikke er en årsagsforklaring for sociale fænomener, som f.eks. kriminalitet og kriminalitetsforebyggelse (Ibid.). Det er i stedet nødvendigt at undersøge, hvordan de sociale fænomener skabes gennem aktuelle forbindelser mellem *aktører* og deres handlinger (Ibid.: 25-27+35+132). I ANT anses både mennesker, institutioner og objekter som aktører, hvilket betyder at menneskelige og ikke-menneskelige aktører er på lige fod, da begge kan influere, opmuntre, tillade og muliggøre handlinger for andre aktører (Ibid.: 95). Eksempelvis gør telefonen det muligt at modtage henvendelser fra enhver, kommunikere over store afstande, tilslutte sig internettet, udføre bankoverførsler osv. På den måde indgår telefonen som aktør i et *netværk* med andre aktører i form af internet, sociale medier, arbejdspladser, underholdning, mennesker m.fl. og influerer den måde vi som mennesker agerer på (Ibid.: 96). Nye aktører kan tilføjes og gamle kan fjernes, og dermed er netværk dynamiske og foranderlige, og skal forstås som et udtryk for aktørernes bevægelser og indvirkning på hinandens gøren.

Telefonen udgør i sig selv også et netværk, idet den er blevet skabt på baggrund af tidligere interaktioner mellem aktører, såsom opfinderen bag telefonen, materialerne den er lavet af og telemasterne, der muliggør dens kommunikation med andre telefoner (Ibid.: 98). På den måde er telefonen en *mediator*, der *translaterer* et tidligere netværk, hvilket betyder at telefonen taler

på vegne af det tidligere netværk, der har ført til dens opfindelse, og får brugere af telefonen til at interagere med andre aktører (Ibid.: 64) Således påvirker telefonen andre aktørers handlinger. Hvis noget (handlinger, objekter osv.) virker stabilt og forudsigeligt, og blot *formidler* en simpel årsagsforklaring på, hvorfor noget sker, uden at påvirke andre aktørers handlinger, bliver det betragtet som en *black box* (Ibid.: 62+236). En black box er således et netværk, hvis indre funktioner og interaktioner kun er kendte af aktørerne i netværket (Ibid.: 255-259). Dermed virker det, udefra, som en stabil enhed, hvis mekanismer er skjulte.

Ved hjælp af ANT vil vi undersøge, hvilke aktører, der aktuelt tager del i den danske forebyggelse af kriminalitet, hvor vishing indgår som modus og hvilke konkrete forebyggelses-tiltag, de iværksætter. Derigennem identificerer vi også, hvad der ligger til grund for aktørernes nuværende tiltag og hvilke udfordringer, de oplever i deres virke.

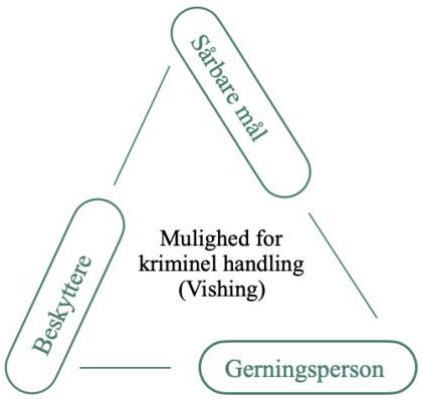
5.2 Rutineaktivitetsteori

De amerikanske kriminologer, Lawrence E. Cohen og Marcus Felsons udviklede rutineaktivitetsteorien i slutningen af 1970'erne. Teorien var et opgør med tidligere kriminologiske teoriers fokus på gerningspersonens motiv eller dårlige strukturelle forhold såsom arbejdsløshed, uddannelsesniveau eller generel velstand, som årsagsforklaringer bag kriminalitet (Cullen et al., 2022: 15). Ifølge Cohen og Felson er motivationen bag en kriminel handling et faktuelt grundlag for at kriminaliteten forekommer, og det interessante at undersøge er således, hvordan den rumlige og tidsmæssige organisering af *rutineaktiviteter*, skaber muligheder for at omsætte motivationen til kriminel handling (Cohen & Felson, 1979: 589). Rutineaktiviteter er gentagne, almindelige aktiviteter, der betragtes som grundlæggende i borgernes daglige liv eller arbejde, som brugen af smartphones eksempelvis er det i dag.

I udviklingen af teorien fokuserede Cohen og Felson (1979: 589) primært på *direct predatory violations*, hvor gerningspersoner direkte tager noget der tilhører andre eller fysisk skader dem. Dertil beskrev de, at de *egnede/sårbare mål* (personer eller objekter), der er særligt egnede at udsætte for kriminaliteten, udgøres af en kombination af målets værdi, synlighed, tilgængelighed og modstandsdygtighed, som gør målet dyre- og flytbart (Ibid.: 595). Det er især personer, der bor alene, som er i størst risiko for at blive viktimiserede, fordi de indgår i færre familierelaterede rutineaktiviteter end andre, hvilket mindsker deres chancer for at have

kompetente beskyttere omkring sig i dagligdagen, der kan hjælpe med at forebygge hændelsen (Ibid.: 590+596). Ifølge Cohen og Felson kan kriminalitetsraten stige, hvis rutineaktiviteterne tillader sammenfald af; en motiveret gerningsperson, sårbare mål (potentielle ofre) og mangel på kompetente beskyttere på samme tid og sted, da det er det, der skaber mulighed for at omsætte motivation til handling (Ibid.: 589). Således kan forbrydelsen forhindres, hvis blot ét af de tre elementer elimineres (Ibid.: 590+604).

Figur 8: *Rutineaktivitetsteori*



Note: Egen illustration

Rutineaktivitetsteorien kan anvendes til at beskrive, hvad der muliggør udførelsen af vishing, da det kan betragtes som en direct predatory violation, hvor gerningspersonerne tilegner sig de forurettedes penge eller oplysninger gennem direkte telefonisk kontakt. Selvom Cohen og Felson udviklede teorien før opfindelsen af mobiltelefonen, internettet og mobilbank, forbliver Rutineaktivitetsteorien således relevant inden for det digitale område. De personer, der oftest bliver udsat for vishing og derfor udgør sårbare mål, er ifølge NCIK:

> "*... 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…*" (NCIK, 2024: 51).

Som beskrevet i afsnit 2, ser vi at anmeldelsestallene for vishing stiger i takt med at danskernes hverdag er blevet stærkt digitalt præget. Der er således ikke længere tale om en teoretisk risiko

for, at lovlig teknologisk udvikling og deraf ændrede rutineaktiviteter, kan skabe nye kriminelle muligheder og risiko for viktimisering. Det er blevet en realitet.

I analysen vil vi anvende Rutineaktivitetsteori til at identificere og visualisere, hvilke af de mulighedsskabende elementer for vishing, de nuværende forebyggelsestiltag, identificeret gennem ANT-analysen, sigter mod at eliminere.

5.3 Helhedsorienteret forebyggelsesmodel

I forlængelse af ovenstående anvender vi Bjørgo's helhedsorienterede forebyggelsesmodel til at undersøge, om den nuværende forebyggelse af vishing i Danmark kan styrkes og hvordan. Modellen er en kombinationen af kerneelementerne fra fire forskellige, overlappende og til tider modsatrettede forebyggelsesmodeller: Retsforfølgelses-, Den sociale-, Den situationelle- og Risk management modellen (Bjørgo, 2016: 9+1). Tilsammen supplerer og forstærker kerneelementerne fra disse modeller hinanden i en helhedsorienteret tilgang til kriminalitetsforebyggelse, der både adresserer ny og gentagen kriminalitet, samt reducerer skadevirkningerne (Ibid.: 14).

Bjørgo's model består af *ni forebyggelsesmekanismer*, som aktiveres gennem forskellige aktørers *forebyggelsestiltag* (Ibid.: 3). Forebyggelsestiltag refererer til de handlinger, som aktører udfører for at starte en proces (forebyggelsesmekanisme), hvor disse handlinger påvirker faktorer, der resulterer i en reduktion af kriminalitet. De ni mekanismer omfatter:

1. Opbygning af **moralske barrierer** mod at begå kriminelle handlinger. Gennem forældre, skole, positive rollemodeller, lovgivere, medierne og autoriteter, kan individets moralske barrierer mod at begå kriminalitet opbygges, internaliseres og vedligeholdes (Ibid.: 16-18).
2. **Reducere rekruttering** til kriminelle sociale miljøer og aktiviteter. Ved at ændre negative sociale forhold, eksempelvis gennem meningsfulde aktiviteter i nærmiljøet, kan marginalisering mindskes og de mekanismer, der leder til at kriminalitet modarbejdes (Ibid.: 18-20).
3. **Generel- og individualpræventiv afskrækkelse** gennem trussel om straf (Ibid.: 21-22). Straf og sanktioner kan få mennesker til at fortage rationelle afvejninger af fordele

og ulemper ved kriminelle handlinger. Hvis ulemperne (hårdhed af straf, høj opdagelsesrisiko og hurtig gennemførelse af straffen) vejer tungest, kan det få dem til at afholde sig fra at begå kriminelle handlinger.

4. **Afværgelse** af kriminalitet (Ibid.: 23-24). Kriminaliteten kan enten opdages tidligt og føre til en advarsel for den mistænkte eller blive opdaget kort inden handlingen udføres, hvor der er bevisførelse nok til retsforfølgelse.
5. **Beskytte sårbare mål** (Ibid.: 26-27). Ved at foretage ændringer ved de situationelle omgivelser, øges risikoen for at blive opdaget og det kræver mere at udføre de kriminelle handlinger, hvilket kan påvirke gerningspersonens rationelle beslutning om at udføre de kriminelle handlinger.
6. **Reducere skadevirkninger** af de kriminelle handlinger, såsom dødsfald, og forurettedes svie og smerte, hvilket kan gøre det nemmere for forurettede at komme hurtigere videre efterfølgende (Ibid.: 28).
7. **Reducere gevinster** ved kriminelle handlinger ved at underminere værdien af gevinsten eller beslaglægge/destruere den (Ibid.: 29-30).
8. **Uskadeliggørelse** ved at fratage gerningspersoner evnen til at begå lovbrud (Ibid.: 25). Individet kan miste adgang til at kunne begå specifikke kriminelle handlinger gennem proaktiv uskadeliggørelse som f.eks. tilhold, forbud, eller gennem reaktiv uskadeliggørelse som f.eks. afsoning.
9. **Afholdenhed og rehabilitering** (Ibid.: 30-31). Når den kriminelle karriere lakker mod enden, er det vigtigt at støtte individet i at etablere et kriminalitetsfrit liv.

Et forebyggelsestiltag kan aktivere forskellige mekanismer på samme tid, men have forskellige funktioner i hver mekanisme (Ibid.: 5). Samtidig kan flere forskellige forebyggelsestiltag ligeledes igangsætte den samme mekanisme. Eksempelvis kan bankernes monitorering af transaktioner lede til afværgelse, reducere skadevirkninger og beskytte sårbare mål, og både monitorering af bankkonti og oplysningskampagner kan beskytte sårbare mål.

Forebyggelsesmekanismerne er generisk formulerede og kan anvendes på alle kriminalitetsformer, hvilket gør det vigtigt at formulere dem ud fra den specifikke kriminalitetsform, der ønskes forebygget eller skadesreduceret (Ibid.: 3+32). Som en del af analysen specificerer vi derfor mekanismerne for de forebyggelsestiltag, vi identificerer der aktuelt iværksættes for at forebygge vishing i Danmark. Som afslutning på analysen

visualiserer vi, hvilke mekanismer den nuværende forebyggelse mod vishing aktiverer. Dette gøres ud fra Bjørgo's (2016: 15) tre kronologiske grupperinger af 1) Mekanismer der søger at forebygge at kriminelle handlinger sker, 2) Mekanismer ved kriminelle handlinger, der allerede er sket og 3) Mekanismer, der søger at forebygge at kriminelle handlinger gentages. I forlængelse heraf undersøger vi, hvordan forebyggelsen potentielt kan styrkes ved at aktivere de mekanismer, vi identificerer at den nuværende forebyggelse endnu ikke aktiverer.

6. Metode

I dette afsnit præsenteres vores metodologiske tilgang til undersøgelsen og de metodiske rammer for empiriindsamlingen. Herunder præsenteres de dokumenter, vi indledende har anvendt til at orientere os i forebyggelsesnetværket og vores primære empiri; semistrukturerede ekspertinterviews. Derudover beskriver vi hvilke overvejelser vi har gjort os i forbindelse med rekruttering af informanter, udarbejdelse af interviewguider, afholdelse af interviews og den efterfølgende databehandling. Afslutningsvis beskrives vores etiske overvejelser og kvalitetssikring.

6.1 Metodisk tilgang

Vi har valgt at anvende en *abduktiv* tilgang, som kombineres med ANT til at undersøge forebyggelsen af vishing i Danmark (Kvale & Brinkmann, 2015: 259-260). I undersøgelsen skaber vi viden om det aktuelle forebyggelsesnetværk gennem en vekselvirkning mellem empiriske fund og teoretiske forståelser af forebyggelsesinitiativer. Ved at anvende ANT, har vi foretaget en empiridrevet undersøgelse, hvor vi gennem vores indledende undersøgelse, der har udmøntet sig i afsnit 2, identificerede de første aktører i forebyggelsesnetværket. Disse aktører inkluderer virksomheder, myndigheder, organisationer som f.eks. politi og banker, og forskellige dokumenter, som vi undersøger nærmere. Det har ført til identifikation af nye aktører, hvilket udvider netværket og danner grundlag for udvælgelsen af en afgrænset gruppe af aktører, der er centrale for analysen. Ved hjælp af ekspertinterviews giver repræsentanter fra de forskellige aktører indblik i, hvordan hver af de udvalgte aktører forebygger vishing, og hvordan tidligere udviklinger i deres respektive netværk skaber særlige forudsætninger for deres forebyggende arbejde. Herefter anvender vi teori til at analysere, hvilke forebyggelsesmekanismer det afgrænsede netværk igangsætter, og hvilke muligheder der kan være for at styrke dette yderligere.

6.2 Dokumenter som en del af netværk

Som beskrevet i det ovenstående afsnit, har vi først anvendt relevante dokumenter til at identificere aktører, der tager del i det eksisterende forebyggelsesnetværk af vishing. Hertil har vi anvendt sekundære dokumenter som f.eks. lovgivning og lovforslag, og tertiære dokumenter som rapporter og forskningslitteratur (Lynggaard, 2020: 187-188). Herefter har vi anlagt en

mere deskriptiv tilgang til de anvendte dokumenter, hvilket bl.a. ses i litteraturreviewet og analysen. Her har vi primært anvendt tertiære dokumenter i form af forskningslitteratur (Ibid.: 188). Med afsæt i ANT kan dokumenter anskues som aktører, der indgår i forebyggelsesnetværket, hvis de får andre aktører til at handle (Latour, 2008: 273) Nogle af de anvendte dokumenter, som eksempelvis lovparagraffer, fungerer således som mediatorer, da de påvirker handlinger i samfundet og andre aktører. Andre dokumenter, som eksempelvis Justitsministeriets Offerundersøgelse (Pedersen et al., 2023), har en mere formidlende rolle, da de primært informerer om f.eks. antallet af forurettede for digital svindel i 2022. Selvom dokumenterne ikke udgør den primære empiri i specialet, indgår de alligevel som en del af det netværk specialet udgør.

6.3 Semistruktureret ekspertinterviews

Den primære empiri består af ekspertinterviews med otte informanter, der er eksperter på forskellige fagområder, hvilket uddybes i afsnit 6.3.2. Interviewene blev primært gennemført som individuelle, semistrukturerede interviews (Harrits et al., 2020: 185). Der var ved gennemførelsen af et enkelt interview to informanter til stede. Interviewene har hjulpet os med at opnå konkret viden om forebyggelsesarbejdet af vishing indenfor, og på tværs af, aktører fra finanssektoren, cybersikkerhed, teleindustrien, politiet og det juridiske felt. I tråd med vores eksplorative tilgang, har vi anvendt den semistrukturerede interviewform for at kunne forberede spørgsmål forud for interviewet og samtidig skabe mulighed for at vores informanter kunne bringe ny, relevant viden i spil i interviewet og på den måde lade dem udbrede netværket for os (Harrits et al., 2020: 186-187; Tanggaard & Brinkmann, 2020: 43-44). Vores interviewguider er udarbejdet på baggrund af den indledende undersøgelse, hvilket uddybes i afsnit 6.3.3.

6.3.1 Introduktion af informanter

For at skabe overblik over vores otte informanter, præsenteres de i følgende tabel, hvor de fremstår ved navn, arbejdssted, stilling og bilagsnummeret for de transskriberede interviews.

Tabel 3: *Informanter*

Navn	Arbejdssted og stilling
Jens – Bilag 3	Professor i cybersikkerhed ved Aalborg Universitet
Jakob – Bilag 4	Direktør for Brancheforeningen, Teleindustrien
Torben – Bilag 5	Kontorchef for Digitalisering og cybersikkerhed i Finans Danmark
Jesper - Bilag 6	Fraud specialist ved Spar Nord - interviewet sammen med kollega Pernille.
Pernille – Bilag 6	Fraud specialist ved Spar Nord - interviewet sammen med kollega Jesper.
Niels - Bilag 7	Fraud specialist ved Danske Bank
Sofie - Bilag 8	Medarbejder hos NCIK, som er ansvarlig for FIT
Lene - Bilag 9	Professor i jura ved Aalborg Universitet

Alle informanterne er udvalgt på baggrund af vores indledende undersøgelse og den indsigt, vi har opnået i forebyggelsesnetværket i forbindelse med udarbejdelsen af problemfelt, baggrundsviden og litteraturreview. Det blev hurtigt tydeligt for os, at NCIK og derigennem FIT, bankerne og Finans Danmark er aktive aktører i forebyggelsen af vishing. Under vores research om forebyggelsesarbejdet stødte vi på Finans Danmarks Svindel Task Force, hvor informanterne Jakob, Jens og Torben er involverede. Deres involvering gjorde os opmærksomme på nye sektorer og brancher, som har været relevante for os at forstå, hvorfor vi har inkluderet dem i vores undersøgelse. De juridiske dokumenter pegede os i retning af det politiske område og vi forsøgte derfor at få sat et interview i stand med en politiker, der sidder i retsudvalget. Dette blev dog aflyst i sidste øjeblik. Det har ikke været muligt at sætte et nyt interview i stand, og vi har i stedet valgt at inddrage det politiske område gennem referater og andre dokumenter. I analysen inddrages flere forskellige aktører, som ikke har menneskelige talspersoner, gennem dokumenter (Olesen & Kroustrup, 2007: 77). Det er aktører som Forbrugerrådet Tænk, European Banking Federation, Mit Digitale Selvforsvar app'en og Folketinget.

6.3.2 Rekruttering af informanter

Vores informanter er udvalgt på baggrund af deres ekspertise og erfaringen inden for forebyggelse af digital svindel og dermed af vishing. Rekrutteringen af informanterne er forløbet på forskellige måder, som beskrives i det følgende.

I kontakten til fraud specialisterne fra bankerne har vi gjort brug af gatekeepers, som vi sendte en kort beskrivelse af vores undersøgelse og en forespørgsel om hjælp til at blive sat i kontakt med relevante personer med henblik på interviews (Harrits et al., 2020: 206). Gatekeeperne er personer, vi selv har fundet gennem et alumnenetværk for kriminologer på LinkedIn. Vi sendte forespørgsler ud til medarbejdere fra 11 forskellige banker, hvoraf Spar Nord og Danske Bank meldte positivt tilbage. Herigennem fik vi viden om, hvordan bankerne arbejder med forskellige svindeltyper. Efter en nærmere præcision af specialets problemformulering, kontaktede vi igen Spar Nord og Danske Bank med henblik på at sætte interviews op, hvilket begge banker indvilligede i.

I rekrutteringen af informanten fra NCIK har vi ligeledes anvendt en gatekeeper i form af lederen af NCIK, som vi kom i kontakt med til Midt- og Vestjyllands forebyggelseskonference d. 8. februar 2024. Herefter satte han os i forbindelse med NCIK-medarbejderen, Sofie, som er ansvarlig for FIT-samarbejdet. Tre af vores informanter, Jakob, Jens og Lene, har vi rettet direkte henvendelse til gennem e-mail, fordi vi havde fået specifik interesse for dem, gennem den indledende undersøgelse til specialet. Lene kendte vi fra en forelæsning på Kriminologiuddannelsen. Informanten Torben har vi fået kontakt til ved at skrive en e-mail til Finans Danmarks analysechef, som videresendte vores forespørgsel til to kollegaer, hvoraf Torben meldte positivt tilbage.

6.3.3 Interviewguider

Vi har udarbejdet syv interviewguider, ét til hver repræsenteret aktør, hvorfor forsknings-spørgsmålene i interviewguidene fremstår forskellige (se bilag 10-16) (Kvale & Brinkmann, 2015: 188-189). Den overordnede struktur er ens i seks af interviewguiderne, bestående af en briefing om vores undersøgelsesfokus efterfulgt af spørgsmål vedr. fagområdets rolle i forebyggelsen af vishing, konkrete forebyggelsesinitiativer fagområdet udfører, udfordringer og fremtidspotentialer for fagområdets forebyggelse, samarbejder med andre fagområder/ aktører og en debriefing. For at kunne stille relevante, velinformerede og undrende spørgsmål, har vi gennem udarbejdelsen af problemfeltet og litteraturreviewet undersøgt, hvilke forebyggelsesinitiativer der umiddelbart indgår i hver af eksperternes fagområder. Interviewguiden til Lene adskiller sig, da dette interview ikke fokuserede på de forebyggende aspekter af hendes arbejde. Interviewet har derimod haft til formål at hjælpe os med at forstå

de juridiske rammer som forebyggelsen af digital svindel skal tilpasses, såvel som de strafferetlige aspekter af kriminaliteten.

Derudover har vi gjort os bekendt med diverse fagsprog forinden afholdelse af interviewene, for at kunne anvende de korrekte terminologier. Det omfattende forarbejde til udarbejdelsen af interviewguiderne er udført for at kunne opnå en vis grad af symmetri i interviewrelationen, idet eksperter ofte er vant til at blive udspurgt om deres meninger og tanker inden for deres område (Ibid.: 201). Den grundige udarbejdelse af interviewguidene har samtidig gjort os i stand til, at forholde os kritisk til informanternes udtalelser og dermed udfordre nogle af disse, hvilket har ført til nye indsigter (Ibid.: 202).

Vi har i udformningen af interviewguiderne reflekteret over, hvilke spørgsmålstyper vi har anvendt. Vi har anvendt *åbne, direkte, informationssøgende, uddybende, strukturerende og fortolkende spørgsmål* (Harrits et al., 2020: 193-194). Interviewene startede, som tidligere beskrevet, ud med at vi introducerede os selv og specialets genstandsfelt. Herefter indledtes interviewet ved at spørge ind til den pågældende eksperts arbejde og stillingsbetegnelse. Den åbne start på interviewet, gav os nogle omfattende svar, som både gav os indsigt i aspekter af eksperternes arbejde, vi ikke på forhånd kendte til (Ibid.: 193), og gav informanterne mulighed for at tale sig varme om et faktabaseret emne. Herefter stillede vi informationssøgende spørgsmål for at få eksperterne til at fortælle om, hvordan der arbejdes med forebyggelse af vishing inden for deres fagområde. Disse spørgsmål blev fulgt op med uddybende spørgsmål, hvorved eksperterne blev opfordret til at tale mere om relevante emner eller nuancere et svar (Ibid.).

Tilgangen til interviewene er, som beskrevet, semistruktureret, hvorfor interviewguiden ikke er blevet fulgt slavisk i interviewsituationerne. Derimod har vi fulgt flowet i samtalen og i nogle tilfælde ladet eksperten være den styrende for interviewets kronologi. Vi har dog anvendt strukturerende spørgsmål, når interviewet har bevæget sig pludseligt fra én tematik til en anden for at sikre os, at vi gennemgik hvert tema på en udtømmende måde, inden vi skiftede emne (Ibid.: 194).

Flere af informanterne ønskede at få tilsendt interviewguiden inden afholdelsen af interviewet. Dette ønske har vi ikke valgt at efterkomme, for at opfylde kriterierne for det semistrukturerede interview om, at give informanterne mulighed for at påpege nye perspektiver og bringe ny

viden i spil (Ibid.: 186). Vi sendte dem i stedet de overordnede temaer og emner, som interviewet ville berøre, for at påvirke informanternes fokus for interviewet mindst muligt, samtidig med at lade dem forberede sig en smule på samtalens overordnede emner.

6.3.4 Afholdelse af interviews

Ved afholdelse af interviewene har vi bestræbt os på at afholde flest mulige fysisk. I to tilfælde har dette ikke været muligt, grundet geografisk placering af informanterne. Vi har i disse tilfælde afholdt interviewene over Microsoft Teams, hvilket gjorde det muligt at bibeholde noget af den nonverbale kommunikation (Kvale & Brinkmann, 2015: 141-142). Begge gruppemedlemmer har været til stede ved afholdelsen af alle interviewene, hvor den ene interviewede og den anden agerede suppleant. Hvem der påtog sig hvilken rolle blev tydeliggjort overfor informanterne under briefingen (Harrits et al., 2020: 207).

Fraud specialisterne fra Spar Nord blev interviewet sammen. Det var aftalt på forhånd og vi var derfor opmærksomme på, at dette interview ville forløbe lidt anderledes. Det har blot betydet, at vi strukturerede nogle af spørgsmålene lidt anderledes, for at begge informanter fik mulighed for at svare. Det blev ikke noteret i interviewguiden, men blev blot inkorporeret som en naturlig del af interviewsituationen. Dynamikken mellem de to informanter fungerede godt og de supplerede hinanden, hvilket har betydet, at vi ved nogle spørgsmål har fået svar der skildrer forskellige opfattelser og tanker om de forebyggelsestiltag, der implementeres og arbejdes med i Spar Nord.

Til afholdelsen af interviewene med Teleindustriens Brancheforening og Finans Danmark, havde informanterne forberedt PowerPoint præsentationer. Vi har ikke bedt vores informanter om at have en præsentation af deres arbejde klar til afholdelsen af interviewet. Tværtimod har vi i mailkorrespondancerne beskrevet, at vi gerne ville holde interviewene som en åben, men struktureret samtale, inden for den ramme interviewguiden har tilladt. Vi anser PowerPoint præsentationerne som et udtryk for, at disse informanter muligvis har haft en agenda med at sige ja til at deltage og har ønsket at fremme denne gennem interviewsituationerne (Ingemann et al., 2018: 157). Under afholdelsen af interviewet med Teleindustriens Brancheforening, blev præsentationen primært anvendt til at forklare og illustrere forebyggelsestiltag, som Teleindustrien enten laver på nuværende tidspunkt eller ønsker at indføre. I denne interview-situation formåede vi at være den styrende part ift. interviewet og vores interviewguide var den

røde tråd gennem interviewet. Det forholdt sig modsat under afholdelsen af interviewet med Finans Danmark. Her gik informanten i gang med sin præsentation, inden vi havde gennemført briefingen og dermed sat rammerne for interviewet. Informanten fik således en styrende rolle i interviewet selvom vi forsøgte at overtage styringen ved at vende tilbage til interviewguiden. Det lykkedes at komme igennem alle spørgsmålene i interviewguiden, men interviewet blev ustruktureret fremfor semistruktureret.

6.4 Kodningsstrategi

Interviewene er efter afholdelsen blevet transskriberet, for at oversætte det talte sprog til det skrevne (Tanggaard & Brinkmann, 2020: 50). Vi har anvendt en simpel transskriptionsstrategi, hvor fokus har været at fastholde meningsindholdet i det sagte (Ibid.: 51). Vi har anvendt en induktiv strategi til kodningen af transskriptionerne, idet vi foretager en empiridrevet undersøgelse. Gennem åben kodning, har det været muligt for os at genere koderne ud fra de emner, som har præsenteret sig i datamaterialet (Bjørnholt & Jakobsen, 2020: 220). Kode nr. 8, jf. tabel 4, er som den eneste direkte udledt af teori og anvendes til delanalyse 2. Selvom kodningsprocessen overvejende har været åben, har den stadig været præget af forskningsspørgsmålene, idet de har formet interviewguidene, der ligeledes har præget interviewene. Vi har kodet efter 12 koder (Ibid.), for at overskueliggøre empirien.

Tabel 4: *Koder*

Kode nr.	Navn på kode
1	Beskyldning af andre
2	Forebyggelsestiltag aktøren selv foretager
3	Forebyggelsestiltag aktøren ønsker at implementere, men er udfordret af/forslag til nye løsninger
4	Begrænsninger for forebyggelse/samarbejder
5	Aktører der nævnes som nogen der burde gøre noget mere, men som ikke gør det/gør nok
6	Udvikling der går forud for, hvordan forebyggelse/systemer fungerer nu
7	Hvordan udnyttes aktørens tjeneste eller middel til svindel
8	Bjørgo - de ni mekanismer i forebyggelsesmodellen
9	Nuværende ting der har en kontraproduktiv effekt
10	Hvilken viden de nuværende tiltag bygger på
11	Gode pointer / argumenter
12	Andet

Kodningen er foretaget manuelt og hver kode har fået tildelt en farve, enten i skriftfarve eller som overstregning. Nogle tekststykker er kodet med mere end en kode, hvilket typisk gør sig gældende for åbne kodninger (Ibid.). Gennem kodningen har vi til hver transskription noteret vores overvejelser og refleksioner ift. koderne, samt hvordan koderne vil kunne anvendes i begge delanalyser (Ibid.).

6.5 Forskningsetiske overvejelser

Som studerende er vi underlagt GDPR-reglerne og vi har derfor sat os godt ind i disse regler for at kunne beskytte og behandle informanternes oplysninger korrekt. Vi har derfor indhentet både mundtligt og skriftligt samtykke fra vores informanter. Det skriftlige samtykke er indhentet gennem samtykkeerklæringer, der rummer informanternes godkendelse af, at vi må behandle deres oplysninger og at disse ikke vil være mulige at pseudonymisere eller anonymisere. Særligt pseudonymiseringen har været vigtig for os at understrege over for vores informanter. Det skyldes først og fremmest, at informanterne jf. afsnit 6.3.2, er udvalgt på baggrund af deres ekspertise. Vi har på baggrund heraf vurderet, at det ikke vil være muligt for os at tilbyde pseudonymisering og samtidig beskrive informanternes ekspertise, fordi de gennem deres stillinger og ansættelsessted vil være identificerbare for læseren (Bengtsson & Mølholt, 2020: 195). Informanterne har haft forskellige ønsker til, hvordan de ønsker at blive omtalt i specialet, hvilket vi naturligvis har imødekommet.

Foruden overvejelser om pseudonymisering og/eller anonymisering, har vi gjort os overvejelser om fortrolighed. Vi har stillet informanterne spørgsmål om, hvilken viden de baserer deres nuværende forebyggelsesinitiativer på og ved at besvare dette, ville det for nogle af vores informanter betyde, at de ville dele forretningskritisk information. Det har dog været muligt at tale rundt om det i overordnede vendinger. Der har således været information som informanterne ikke har kunnet dele med os. For at sikre, at vi ikke viderebringer fortrolige oplysninger har vi, inden afleveringen, sendt vores informanter de af deres citater vi anvender i analysen, samt den kontekst de anvendes i, så de har kunnet godkende dem, hvilket ligeledes fremgår af samtykkeerklæringerne.

Vi har desuden været opmærksomme på, at nogle informanter har haft et image at beskytte. Der kan af den grund have været strategiske grunde for at informanterne har valgt at stille op

til interview og der kan derfor have været mere på spil i interviewsituation end at informanterne blot har villet hjælpe os med at skabe empiri til vores undersøgelse (Ingemann et al., 2018: 192). Der er i øjeblikket en øget mediebevågenhed på digitale svindeltyper, men det er ikke muligt at sige om dette har haft indvirkning på, hvordan informanterne har besvaret vores spørgsmål, eller om der har været information som de har valgt at tilbageholde, for at fremstå på en bestemt måde. I enkelte tilfælde gjorde informanterne opmærksomme på, at deres svar til et spørgsmål var uden for citat, men at de gerne ville dele informationen med os som baggrundsviden. Vi har i disse tilfælde forholdt os kritisk hertil og forsøgt at finde andre kilder til samme information (Ibid.). Derudover er disse citater blevet slettet fra transskriptionerne.

6.6 Kvalitetssikring

Vores undersøgelse er afgrænset til udvalgte forebyggelsesaktører, som vi har opnået viden om, gennem offentligt tilgængelige dokumenter, og ekspertinterviews. Interviewene har kun givet os indsigt i information, som informanterne vurderer må offentliggøres og, hvad de vælger at indvillige os i. Det har betydning for den viden undersøgelsen baseres på. For at sikre *pålideligheden* af undersøgelsen har vi bestræbt os på at være grundige og systematiske i vores gennemgang af teori og metodiske tilgang, samt skabe gennemsigtighed omkring vores valg, overvejelser, så undersøgelsestilgangen kan gentages i fremtiden (Riis, 2018: 352-353). Derudover har vi udvalgt centrale aktører i forebyggelsen ved at identificere, hvilke aktørers domæner og/eller systemer, der udnyttes til at udføre vishing. Formålet med udvælgelsen er, at mindske risikoen for at de inddragede aktører vil være irrelevante i en fremtidig undersøgelse, da netværk, jf. Latour (2008), er dynamiske, hvilket ligeledes styrker *overførbarheden* (Riis, 2018: 355). Udvælgelsen af aktørerne styrker desuden undersøgelsens *gyldighed*, da informanterne, som eksperter på området, kan uddybe det centrale netværks nuværende forebyggelse (Riis, 2018: 357). Derudover har vi understøttet fundene fra interviewene med information fra andre kilder og anvendt vores abduktive tilgang til at skabe en vekselvirkning mellem empiri og teori, som styrker gyldigheden yderligere.

8. Analyse

I dette afsnit behandler vi problemformuleringen gennem to kronologiske analyser. I den første delanalyse undersøger vi, hvordan der forebygges mod vishing i Danmark ved at beskrive de udvalgte aktørers forebyggelsesarbejde og derigennem identificere, hvilke konkrete forebyggelsestiltag de implementerer. Vi uddyber ligeledes, hvordan aktørernes forebyggelses-tiltag overlapper, og hvordan aktørerne samarbejder på tværs. I forlængelse heraf, identificerer vi udfordringer for forebyggelsesarbejdet, både internt, og i samarbejder. I den anden delanalyse anvender vi de identificerede forebyggelsestiltag til at undersøge, hvilke af Bjørgo's forebyggelsesmekanismer, tiltagende aktiverer. I forlængelse heraf, identificerer vi udfordringer og muligheder for at styrke forebyggelsen yderligere.

8.1 Delanalyse 1 - Forebyggelse af vishing

Afsnittet er opbygget kronologisk efter stadierne før, under og efter vishing, som er beskrevet og illustreret i afsnit 1.2. Dette gøres for at forklare, hvordan vi har udvalgt forebyggelsesaktørerne, beskrive deres arbejde med forebyggelse og identificere deres konkrete tiltag for at forebygge vishing.

8.1.1 Før Vishing

Inden vishing udføres, anvender gerningspersonerne apparater og teknologier til at lære, hvordan de kan omgå sikkerhedsforanstaltninger og finde kontaktoplysninger på personer, de anser som ønskede mål for deres kriminelle handlinger. De sender evt. smishing- eller phishingbeskeder til forurettede, der skal lede vedkommende til at tage kontakt til gerningspersonen, og planlægger, hvordan bedrageriet skal foregå. Planlægningen kan inkludere at finde inspiration i crime scripts, sløring af IP-adresser, spoofing af telefonnumre og betalingssider, samt udvælgelse af den strategi, der skal anvendes for at udføre angrebet.

Vi har identificeret, at de aktører, der muliggør planlægningen, er gerningspersoner, computere og internettet. Da denne fase primært kræver teknologisk viden og ekspertise, har vi valgt at inddrage professor i cybersikkerhed, Jens, som informant til at forstå, hvordan der (kan) forebygges på planlægningsfasen.

Cybersikkerhed

Ifølge Jens er det forholdsvist nyt, at personer med hacker- og cybersikkerhedsviden, som ham selv, inddrages i forebyggelsen af digital svindel. Kombineret med, at han sidder med i Finans Danmarks Svindel Task Force (Finans Danmark, n.d. *d*), som endnu ikke har præsenteret nogle resultater, er han således udfordret på at konkretisere, hvad han bidrager med på nuværende tidspunkt. Han beskriver derfor kun overordnet, at han aktuelt er med til at se på, *"Hvad er det for nogle områder, der skal prioriteres og hvad man kan gøre ved de områder. Det er jo meget sådan tilgangen til det"* (Bilag 3: 11). Udover at han kun overordnet kan beskrive arbejdet i Svindel Task Forcen, fortæller han, at han bidrager med viden om de tekniske mekanismer, men prøver stadig at finde ud af, "*... hvad jeg kan i det der, fordi hvor er det cyberkomponenterne kommer ind i det her?*" (Bilag 3: 11). Han beskriver, i tråd med Walls typologier, jf. afsnit 1.2, at der er forskel på, hvor store cyberkomponenter, der er inde over sager med vishing, alt efter hvordan den kriminelle handling er bygget op og udføres. Der er, i Jens' optik, heller ikke altid tale om teknologiske svagheder, der skal styrkes, men også menneskelige svagheder:

> *"Som jeg forstår det, er det jo meget mere nogle psykologiske mekanismer, man bruger, hvor man bilder folk nogle gode historier på ærmet. Når man får dem til at hæve deres penge og give dem til nogle kriminelle,* [...] *er der måske ikke så meget it-svaghed i det"* (Bilag 3: 8).

For at mindske de menneskelige svagheder, foreslår Jens, at danskernes generelle it-kompetencer kan styrkes gennem (efter)uddannelse, så de bedre kan begå sig i en hverdag, "*...hvor mere og mere kriminalitet bliver digital…*" (Bilag 3: 31). Udover at styrke borgernes digitale færdigheder, påpeger han, at der ligeledes er nogle strukturelle elementer, der kan skrues på, for at forbedre forebyggelsen. Han anfægter især, hvordan der politisk prioriteres med politiets ressourcer, hvor der er "*...paskontrol i toget [...], fordi det har vi ressourcer til, [...] det er altså det vi bruger vores politiressourcer på. Og ikke på den digitale kriminalitet*" (Bilag 3: 26). Ifølge Jens leder den nuværende prioritering af politiets ressourcer til, at befolkningen vænnes til at digital svindel er noget, der ikke kan gøres noget ved, fordi det er en mindre procentdel af anmeldelserne, der fører til domfældelse (Bilag 3: 27). I forlængelse heraf fremhæver Jens: "*Vi er nødt til at kunne få retsforfulgt nogle af dem, hvis vi gerne vil opretholde den retsorden, som vi kender*" (Bilag 3: 31). Han mener således det er nødvendigt

at der investeres og prioriteres anderledes for politiet, så der er mulighed for at ansætte flere personer med cyberrelevante kompetencer til at efterforske sager om digital svindel, så der er *"...en eller anden grad af retsfølelse, der bliver opretholdt"* (Bilag 3: 24). Derudover mener han, at den civile cybersikkerhed bør prioriteres og styrkes yderligere ved f.eks. at placere en del af cybersikkerheden hos Justitsministeriet eller Erhvervsministeriet (Bilag 3: 28). Center for Cybersikkerhed er i dag placeret under Forsvarets Efterretningstjeneste og har til opgave at hjælpe myndigheder og virksomheder med at ruste sig mod de trusler, der følger med digitaliseringen (Center for Cybersikkerhed, n.d.).

Udover styrkelse af borgernes it-kompetencer og forslag til strukturelle forandringer, nævner Jens, at der kan implementeres nogle tekniske løsninger, som enten begrænser forekomsten af svindel eller konsekvenserne af det. Det handler konkret om at forbedre identificeringen af indkomne opkald og modtageren ved anvendelse af MitID (Bilag 3: 8+22). På den måde mener Jens at det kan blive nemmere for forbrugeren at skelne mellem 'sikre' og 'farlige' opkald/overførsler. Derudover foreslår han at der implementeres individuelle beløbsgrænser på banktransaktioner frem for standardiserede, offentligt synlige grænser, *"Fordi [...], så er det alt andet lige sværere for svindlerne at gennemskue, hvad de kan slippe afsted med"* (Bilag 3: 6). I forlængelse heraf foreslår han at monitoreringen af banktransaktioner foretages mere kritisk, selvom det vil være begrænsende for de bankkunder, der har legitime årsager til at foretage større overførsler (Bilag 3: 22).

Ud fra Jens' udtalelser, virker det til at være nyt at cybersikkerhedseksperter inddrages i forebyggelsen af vishing i Danmark. Hvormed de endnu ikke har etableret sig som mediator i forebyggelsesnetværket. Det er således ikke muligt at sige noget om, hvilken indvirkning de aktuelt har på andre forebyggelsesaktører (Latour, 2008: 64+95). Jens anser sin egen og andre cybersikkerhedseksperters rolle for at være 'vidensleverandører' (Bilag 3: 19), og anfægter at deres ekspertviden ikke er blevet inddraget i forebyggelsen førhen:

> *"Det der hacker-mindset tror jeg man kan bruge til meget. Også ift., hvordan man forebygger. [...] F.eks. sådan noget som MitID, hvis man inden man havde lanceret det, havde smidt det ud til nogle af vores studerende og sagt, "*Hey, prøv lige at se, hvad I ville gøre med det her?"*, så tror jeg man kunne undgået nogle af de scams, man mødte i begyndelsen"* (Bilag 3: 15).

Jens giver herved eksempler på, hvordan cybersikkerhedseksperter kan anvendes mere aktivt i forebyggelsen og kommer med forslag til, hvordan mekanismerne bag diverse teknologier, som endnu ikke er implementeret i forebyggelsen, kan styrkes. Det giver os indtryk af, at det resterende netværk endnu ikke er bevidste om disse eksperters fulde potentiale, og at cybersikkerhed derfor kan fremstå som en black box for de andre aktører (Latour, 2008: 255-259). Alternativt kan det tyde på, at cybersikkerhedseksperter endnu ikke har formået at etablere sig som aktører i forebyggelsesnetværket, da det på nuværende tidspunkt ikke er muligt at identificere, hvordan deres handlinger i netværket bidrager til forebyggelsen (Latour, 2008: 16).

Opsummering

Ifølge Jens bidrager cybersikkerhedseksperters viden aktuelt til at identificere mulige tekniske indsatsområder, som kan styrke forskellige aktørers forebyggelsesinitiativer. De tekniske løsninger han peger på er identificering af indkommende svindelopkald og modtagere på overførsler. Således er Jens' udtalelser eksempler på, at cybersikkerhedseksperternes viden aktuelt kan hjælpe de kompetente beskyttere med at styrke deres forebyggelseskompetencer yderligere under udførelsen af kriminaliteten.

Figur 9: Opsummering – Cybersikkerhed

Note: Egen illustration

8.1.2 Under vishing

Som beskrevet i afsnit 1.2, er det i den telefoniske kontakt, at vishing udføres. Den forurettede er dog sjældent bevidst om, at de taler med en kriminel, idet vedkommende typisk udgiver sig for at repræsentere en myndighed, en virksomhed eller en af forurettedes bekendte. Som det tidligere er beskrevet, styrker gerningspersonerne deres troværdighed ved anvendelse af social engineering strategier, der kan kombineres med strategier, samt viden om, hvordan den pågældende myndighed/virksomhed, de udgiver sig for at repræsentere, håndterer kundekontakt.

I selve samtalen kan adskillige strategier anvendes til at overbevise forurettede om, at nogen i deres familie er i nød/fare, at deres informationer er blevet lækket, at deres bankkonti er ved at blive tømt osv. Som tidligere beskrevet, kan det føre til forskellige måder, hvorpå de kriminelle får udleveret forurettedes oplysninger eller penge. Det kan både ske ved aftale om fysisk møde for overlevering eller digitalt. Udleveringen af oplysninger, fører til, at gerningspersonen selv anvender oplysningerne til at foretage overførsler eller hæve penge på forurettedes kreditkort. Ved overdragelsen af penge til gerningspersonen, er det således forurettede, der selv laver en overførsel eller hæver kontanter til udleveringen.

Udførelsen af vishing involverer en del forudgående planlægning og tillært viden om sikkerhedsforanstaltninger, samt anvendelse af social engineering til succesfuldt at omgå sikkerhedsforanstaltningerne. For det andet anvendes den telefoniske kontakt til at understøtte troværdigheden og dermed opbygge tillid til gerningspersonen vha. kombinationen af spoofing og social engineering. I opkaldet er kun gerningspersonen og forurettede til stede og der er således et fravær af kompetente beskyttere (Cohen & Felson, 1979: 589). Da den forurettede ofte tror de er i kontakt med en virksomhed eller myndighed, som forsøger at hjælpe dem, kan der skabes en oplevelse for forurettede af, at der ér kompetente beskyttere til stede, som styrker troværdigheden af interaktionen. Social engineering er det centrale, gennemgående element i vishing, da det er gennem social engineering, der skabes bekymring/taknemlighed og incitament for handling hos den forurettede, som gør vedkommende til et sårbart mål (Ibid.).

Uanset, hvordan gerningspersonerne skaffer sig adgang til de forurettedes penge, er det i sidste ende de forurettedes bankkonti, der er målet for svindlen og den telefoniske kontakt, der anvendes som redskab til at nå dertil. Vi har derfor valgt at undersøge finanssektoren og Teleindustrien som de primære forebyggelsesaktører under udførelsen af kriminaliteten.

Teleindustrien

Vi har valgt at inddrage direktøren for Teleindustrien (TI), Jakob, som informant, da TI, som brancheforening, repræsenterer de danske teleselskaber og er ansvarlige for at skabe samarbejder mellem teleselskaber, myndigheder, medier og forbrugere (Teleindustrien, n.d.). En del af deres vision er at skabe sikre og trygge tjenester for forbrugerne. Det betyder at de arbejder for at forbedre beredskabet og cybersikkerheden ved at samarbejde både internt i virksomhederne og eksternt med myndighederne (Ibid.). Målet er at gøre danskerne trygge ved at benytte sig af teleselskabernes produkter og tjenester, fordi teleselskaberne aktivt beskytter deres kunder mod svindel og skadeligt indhold (Ibid.)

Jakob fortæller, at TI har implementeret tre forskellige tekniske løsninger, der beskytter privatpersoner, virksomheder og myndigheder mod at blive udnyttet til svindel. Disse vil blive præsenteret i det følgende.

Spoofingbeskyttelse - SMS'er

Den første teknologiske løsning er en brancheaftale om spoofingbeskyttelse af afsender-ID på SMS'er. Virksomheder og myndigheder kan lovligt spoofe deres egne masseudsendelser af SMS'er, så deres navn, f.eks. 'IKEA', fremgår som afsenderen i stedet for et telefonnummer. Det er kun muligt at spoofe gennem computere, der har adgang til Signalsystem 7 (Wright, n.d.), hvilket er det grundlæggende styresystem for telenettet (Bilag 4: 3). Systemet blev lavet, da der kun fandtes et enkelt teleselskab i hvert land, og det er fortsat Signalsystem 7, der anvendes til at foretage opkald og sende SMS'er i dag. I TIs spoofingbeskyttelse af afsender-ID er det muligt at tilkøbe beskyttelse af specifikke spoofingnavne. IKEA kan f.eks. betale for, at de er de eneste der må bruge 'IKEA' som afsender-ID på SMS'er. I den forbindelse skal selskabet gå til deres SMS-udbyder og definere, hvilke kilder deres SMS'er kommer fra. Det vil sige, *"... hvis SMS'er der har afsender-ID'et 'IKEA' kommer fra andre kilder end dem de [IKEA] har defineret, så sletter vi dem [...] Men hvis de [kriminelle] kaldte sig 'Selskabet*

IKEA', så bliver det ikke blokeret, bare fordi 'IKEA' indgår i navnet" (Bilag 4: 8). Det er, ifølge Jakob, ikke muligt at spoofe gennem sin egen telefon, men de kriminelle har mulighed for at spoofe, *"Hvis de bare kan finde ét teleselskab, som er villig til at lade dem lave deres svindel og manipulere afsender ID [...] både på sms'er og opkald og udgive sig for at være en anden. Og det er det vi slås med"* (Bilag 4: 4).

Selvom løsningen ikke kan blokere alle vishingforsøg, der anvender variationer på navnet af et selskab, vil den spoofede besked trods alt lægge sig i en anden tråd i modtagerens SMS-indbakke, end den legitime (Bilag 4: 8). Jakob ser de spoofede SMS'er som TIs største forebyggelsesmæssige udfordring. Udfordringen består i, at de spoofede SMS'er, der slipper gennem blokeringssystemet, i nogle tilfælde angiver et telefonnummer i beskeden, som forurettede kan ringe til i troen om, at det f.eks. er IKEA de ringer til, men i virkeligheden fører dem til gerningspersonen. Jakob understreger i den forbindelse, at;

> *"Grunden til at man kan det, er fordi du stadig kan få anonyme taletidskort. Og det bruger de kriminelle jo [...] Det vil sige, det der hedder, Lyca mobile og Lebara, har stadig anonyme taletidskort som du kan bruge, hvis du er kriminel, til at lave svindel på"* (Bilag 4: 9).

Den 3. marts 2022 stemte et flertal i Folketinget en lovændring vedr. ændringer i retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester igennem. Med lovændringen er det muligt at forbyde anonyme taletidskort, det er dog Justitsministeriet fastsætter tidspunktet for denne del af lovens ikrafttrædelse, hvorfor paragraffen omhandlende forbud mod køb af anonyme taletidskort endnu ikke er trådt i kraft (Folketinget, 2021-22: 4) .

Spoofingbeskyttelse - fastnettelefonnumre

Den anden løsning, TI har implementeret, er spoofingbeskyttelse af udvalgte fastnet-telefonnumre tilhørende banker, myndigheder og politi. Løsningen er baseret på antagelsen om, at spoofede opkald kommer fra udlandet (Bilag 4: 14). Løsningen blokerer således kun opkald fra udlandet, der udgiver sig for at være et af de udvalgte fastnetnumre, som har fået spoofingbeskyttelse. Jakob fortæller, at TI gerne vil kunne tilbyde løsningen på mobil-telefonnumre, men at de er udfordret af, at være underlagt e-privacy regler, som dækker over;

> *"Reglerne om persondatasikkerhed i den elektroniske kommunikationssektor har til formål at sikre privatlivets fred og beskytte abonnenter og brugeres personoplysninger. Elektroniske kommunikationstjenester dækker over traditionelle telefoni- og beskedtjenester som f.eks. SMS og taleopkald, såvel som tilsvarende online-tjenester f.eks. internetbaserede telefoni – og beskedtjenester samt webbaserede e-posttjenester*" (Digitaliseringsstyrelsen, n.d. *b*).

Det betyder, at selvom et dansk teleselskab registrerer, at der kommer et telefonopkald fra et mobilnummer ind over grænsen, og samtidig kan se at vedkommende, der angiveligt ringer, befinder sig inden for landets grænser, må teleselskabet ikke blokere det (Bilag 4: 19). Det vil være imod e-privacy reglerne, hvor der står, "*...at trafikdata må vi ikke bruge til andet formål end til at dirigere trafikken. Hvis vi brugte data om mig, om hvor jeg er henne, til at blokere et opkald, så ville det være et andet formål end det, vi har samlet data ind til"* (Bilag 4: 19). Sverige og Finland har allerede implementeret løsningen på mobiltelefonnumre, og TI har derfor i 2023 bedt erhvervsministeren om at undersøge, hvorvidt det er muligt at gøre i Danmark (Bilag 4: 19). Så vidt Jakob ved, er der nedsat en arbejdsgruppe mellem Justitsministeriet, Erhvervsministeriet, Klima- og Energiministeriet og Digitaliserings-ministeriet, der skal tage stilling til om TI må lave løsningen, men der er endnu ikke kommet en afklaring (Bilag 4: 20). TI har således et forebyggelsestiltag klar til implementering, som er udfordret af manglende afklaring fra politisk hold.

Farlige links

TIs tredje teknologiske løsninger beskyttelse mod 'farlige' links, som er implementeret hos Telenor og TDC Erhverv (Bilag 4: 12-13). Løsningen går ud på, at teleselskaberne selv kan få lov til at blokere links til hjemmesider, *"... hvor man kan blive snydt eller de lokker information ud af dig"* (Bilag 4: 12), uden først at få en dommerkendelse. Det kræver dog at teleselskaberne laver to tjenester: "*En hvor du får beskyttelsen, hvor vi blokerer, og en hvor du kan vælge at træde ud af beskyttelsen. Det er administrativt ret tungt at skulle håndtere to forskellige tekniske løsninger, hvis du har mange mio. kunder"* (Bilag 4: 13). Der er således kun to teleselskaber, der indtil videre har implementeret løsningen. Jakob fremhæver et ønske om at myndighederne giver TI mulighed til at lave en fælles løsning for teleselskaberne, i form af en database over farlige hjemmesider, der kontinuerligt opdateres og deles blandt alle

teleselskaberne, så hjemmesiderne blokeres for alle kunder, uden at kunderne først skal tilkendegive at de gerne vil tage imod tjenesten (Bilag 4: 13).

Udfordringer

Generelt giver Jakob udtryk for at forebyggelsesarbejdet i det danske telenet er udfordret af e-privacy reglerne og de grundlæggende rettigheder for privatlivets fred. TI ønsker bl.a. at kunne oprette SMS firewalls, hvor det, vha. kunstig intelligens, er muligt at analysere indholdet af masseudsendte SMS'er, for at detektere om der er tale om smishing: "*Vi har faktisk maskinerne stående. [...] Vi kunne tænde for det i morgen"* (Bilag 4: 22). Løsningen kan dog anskues som en krænkelse af privatlivets fred, da det vil bryde brevhemmeligheden, jf. straffeloven § 263. TI mener således der er tale om et politisk dilemma om, hvorvidt *"...det er tilstrækkeligt vigtigt at beskytte folk mod digital svindel, at vi vil tilsidesætte grundlæggende rettigheder som retten til privat kommunikation"* (Bilag 4: 23). Desuden pointerer Jakob, at en implementering af SMS firewalls kun kan beskytte masseudsendelser af SMS'er på telenettet, hvilket kan forskyde problemet til krypterede beskeder (Bilag 4: 31). Krypterede beskeder anvender *RCS* (Rich Communications Service), som foregår over internetforbindelse og kun kan ses af afsender og modtager (Google, n.d.). Dette fremhæver Jakob ligeledes: "*Det flytter over på de platforme, som vi ikke har magten over. Så der er nogle nye aktører, som skal inviteres med, eller der skal laves regulering, som kan hjælpe med til at lave bedre beskyttelse*" (Bilag 4: 31).

Hvis TI kunne implementere SMS firewalls og få godkendelse af myndighederne til at blokere farlige links på tværs af alle teleselskaberne, kan der dog ikke beskyttes mod al svindel, der foregår over telenettet (Bilag 4: 18). Jakob appellerer til, at der skal flere aktører med i forebyggelsen for at skabe bedre beskyttelse: *"Sociale medier, techgiganterne; Apple, Google, ift. telefonerne og det der kører som krypterede beskeder*" (Bilag 4: 19).

Udover tekniske løsninger, har TI anbefalet Ældresagen at fortælle deres medlemmer, at de kan beskytte sig selv ved at fjerne deres numre i de offentligt tilgængelige databaser, så de ikke er lige så lette for de kriminelle at finde (Bilag 4: 8). TI har også været med til at udgive en særudgave Anders And bladet til skoler, der handler om digital sikkerhed (Kejlberg, 2022). Derudover er de i dialog med Forbrugerrådet Tænk om, at udvide app'en, Mit Digitale Selvforsvar, med henblik på at lave en feature, der kan advare brugeren, når et indkommende opkald identificeres som vishingforsøg (Bilag 4: 35).

Opsummering

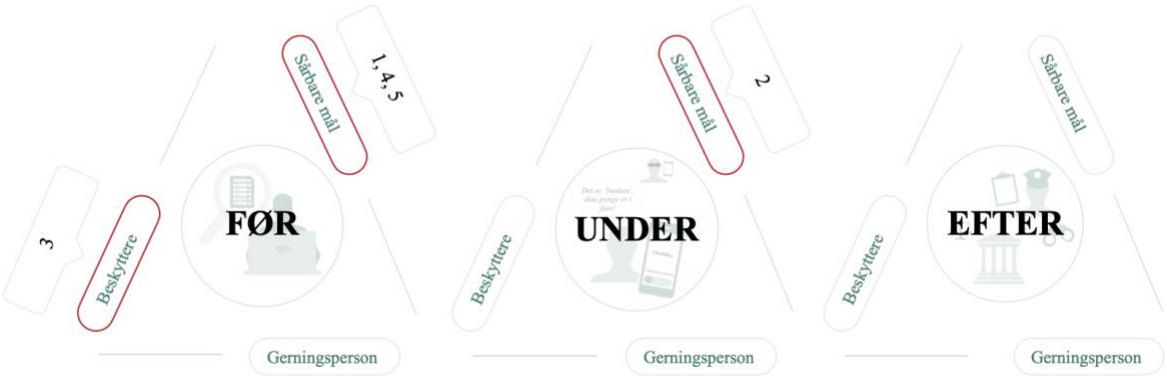
Vi har identificeret fem konkrete tiltag, som TI aktuelt har implementeret til forebyggelsen af vishing:

Tabel 5: *TIs tiltag*

Teleindustriens forebyggelsestiltag	
1	Spoofingbeskyttelse af virksomheders afsender-ID på SMS'er
2	Spoofingbeskyttelse af banker, politi og myndigheders fastnettelefonnumre
3	Blokering af farlige links
4	Anbefalinger til Ældresagen
5	Oplysningskampagner

Tiltag nr. 1, 4 og 5 har til formål at styrke (specifikke) borgeres evner til at identificere svindelforsøg, inden det udføres. Tiltag nr. 2 styrker ligeledes borgernes identificering af vishing, men under den aktive udførelse, da opkaldet, jf. afsnit 4.1, er den aktive del af udførelsen af et vishingforsøg. Tiltag nr. 3 er et teknisk tilbud til teleselskaberne, der gør dem bedre i stand til at stoppe gerningspersonens forsøg på at få potentielle mål til at tage kontakt. Blokering af links er således et tiltag, der kan øge teleselskabernes kompetencer i at beskytte deres kunder, før kriminaliteten udføres.

Figur 10: *Opsummering - Teleindustrien*



Note: Egen illustration

Finans Danmark

Vi har valgt at inddrage Torben som informant på vegne af Finans Danmark (FD), fordi FD har en central rolle i finanssektoren, hvor de er interesse- og arbejdsgiverforening for bl.a. banker, investeringsfonde, datacentraler, it- og fintechvirksomheder (Finans Danmark, n.d. *b*). Torben er kontorchef for FDs digitaliseringsområde og beskæftiger sig primært med fraud og cybersikkerhed (Bilag 5: 1). Hans arbejdsopgaver omhandler et af FDs seks kerneområder i deres vision om, at bidrage *"... til et sikkert og trygt Danmark gennem bekæmpelse af svindel og økonomisk kriminalitet*" (Finans Danmark, n.d. *b*). Torbens arbejdsopgaver omfatter både interne opgaver i FD, samarbejde mellem banker, koordinering med myndigheder samt andre nationale samarbejdspartnere såsom virksomheder og NGO'er. På internationalt plan, sidder Torben med i European Banking Federations (EBF) cyber ekspertgruppe i Bruxelles (Bilag 5: 1). EBF repræsenterer 33 europæiske bankforeninger og arbejder for at skabe en harmoniseret lovgivningsmæssig ramme i (European Banking Federation, n.d.). De fremmer initiativer til informationsdeling om cyberrisici og styrker cybersikkerhedsfærdighederne hos både bankansatte og kunder (European Banking Federation, 2018).

Torben sidder med andre ord med til bords, når FD implementerer nationale forebyggelsesinitiativer, der har til formål at bekæmpe forekomsten af digital svindel, herunder vishing. Han fortæller, at FDs forebyggelsestiltag både er tekniske sikkerhedsforanstaltninger og samarbejder om at overkomme regulatoriske begrænsninger samt oplysningskampagner rettet mod forbrugere og den almene borger.

Tekniske tiltag

Det første tekniske tiltag Torben fortæller FD har implementeret, er at sænke den daglige beløbsgrænse på overførsler fra 500.000 kr. til 50.000 kr. (Bilag 5: 9; Thorning, 2023). Det er det første initiativ fra Svindel Task Forcen. Derudover har FD, som en del af ejerkredsen, lanceret fornyelsen af NemID, MitID, for at øge sikkerheden ved overførsler (Bilag 5: 6; Digitaliseringsstyrelsen, n.d. *a*). De tekniske ændringer inkluderer brug af et selvvalgt brugernavn i stedet for CPR-nummer, fjernelse af push-notifikationer, to-faktor godkendelse og tilføjelse af en referencetekst ved alle betalinger. Bankerne arbejder også løbende på at styrke referenceteksten yderligere f.eks. vha. VOP (Verification of Payee), som kommer viser identiteten på modtagende kontonummer ved en overførsel (Bilag 5: 16). På trods af at FD kontinuerligt øger sikkerhedsforanstaltningerne, er den største udfordring for sikkerheden, "...

i virkeligheden, at man manipulerer ofrene til selv at gøre det" (Bilag 5: 4). FD arbejder derfor for, at bankerne i fremtiden må anvende *behavioural biometrics* (adfærdsanalyse) til at monitorere kundernes transaktionsmønstre (Bilag 5: 24-25). Herved vil det blive muligt for bankerne at analysere kundernes adfærd i netbanken; hvordan de flytter computermusen, hvad de kigger på, og hvilke handlinger de normalt foretager sig. Derudover ser Torben potentiale ved at ændre ved standardrettighederne i netbanken (Bilag 5: 30). Ved at skrue ned for services, mener han at bankerne vil kunne begrænse, hvad gerningspersonerne kan udnytte, hvis de får tilegnet sig informationer, der giver dem adgang til forurettedes netbank. For at styrke forebyggelsen gennem sikkerhedsforanstaltninger, samarbejder FD med nordiske banker i Nordic Financial Computer Emergency Response Team (NFCERT), hvor de holder hinanden opdaterede på det aktuelle trusselsbillede (Finans Danmark, 2017):

> *"... der bliver holdt ugentlige møder med fraud folkene fra alle bankerne, telefonmøder, hvor man tipper ind og deler viden ift., hvad det er de ser. Så man har et meget godt efterretningsbillede af udviklingen og trends rent fraudmæssigt"* (Bilag 5: 16).

På trods af de ugentlige opdateringsmøder, er bankerne udfordret af, at "*Modus ændrer sig hele tiden. Angrebene bliver mere sofistikerede, tekniske og målrettede*" (Bilag 5: 22). Bankerne er desuden udfordret af, at de ikke må dele alle relevante data med hinanden i henhold til Lov om Finansiel Virksomhed og GDPR. Det udmønter sig bl.a. i, at kriminaliteten er grænseoverskridende og bankerne ikke kan følge transaktionen ud af deres eget pengeinstitut. Samtidig ved de, at "*... hvis vi ikke får fat i modtagende bank inden for et kvarter. Så er det næsten lige meget. Det går så stærkt med at flytte ting elektronisk efterhånden*" (Bilag 5: 22). Det er tidligere blevet undersøgt af samtlige ministerier, om der kan opbygges en model for machine learning, til at styrke bankernes monitorering ved at se på hele bevægelsen af transaktionen (Bilag 5: 45). Torben fremhæver i forlængelse heraf, at den afprøvede model kan reducere falske positiver med omkring 80 eller 85 %. Det er dog ikke muligt at implementere modellen, da det vil være et brud på Data Privacy, at kigge ind i transaktionerne og finde sammenhænge (Bilag 5: 45).

Videndeling

Ifølge Torben er videndeling blandt bankerne vigtig for forebyggelsen, da de skal følge med kriminalitetsudviklingen for at kunne implementere velbegrundede tiltag. Der har tidligere

været et tilfælde, hvor en dansk bank, ud fra egne data, identificerede en stigning i svindelforsøg rettet mod en bestemt gruppe borgere i et bestemt område. Som svar på dette implementerede banken en teknisk løsning, der forhindrede borgergruppen i at lave straksoverførsler. *"Der kom forbrugerombudsmanden på gaden med det samme og sagde, "Det der er diskriminering"* (Bilag 5: 9).

Inden for landets grænser udfordres forebyggelsen af, at bankerne ikke har samme muligheder for at implementere de samme tekniske tiltag, idet de anvender forskellige datacentraler (Bilag 5: 10). Nogle af de store banker har egne datacentraler og kan implementere nye tekniske tiltag hurtigere end de mindre banker, som anvender fællesejede datacentraler. De fællesejede datacentraler er bygget på baggrund af et ønske om besparelser, men ulempen er, at de mindre banker først skal skaffe mandat blandt de andre banker på centralen, før noget nyt kan implementeres.

Flere af udfordringerne Torben fortæller om, er funderet i hvad bankerne lovgivningsmæssigt har lov til at indsamle, anvende og dele af data. Som han selv formulerer det, "*Der er nogle ønsker, som vi prøver at få igennem lovgivningen for at få øgede muligheder for at kunne dele flere relevante datapunkter. Det virker som om PSR kommer til at åbne lidt mere for*" (Bilag 5: 16). PSR (Payment Service Regulation) skal sammen med PSD3 (third Payment Service Directive) erstatte den nuværende PSD2, som er europæisk regulering af betalingstjenester (Nordea, 2024). Den nye regulering forventes færdigudviklet slut 2024/ start 2025, hvorefter EU-medlemslandene har 18 måneder til at implementere dem. PSD2 har bl.a. indført styrket autentifikation ved online betalinger, som i Danmark førte til implementeringen af MitID (Nordea, 2023). Derudover er princippet om *Open Banking* blevet indført for at gøre det lettere for tredjeparter at udbyde betalingstjenester, der muliggør integrering af online bank og andre finansielle applikationer, som f.eks. Mobilepay, der tilsammen kan skabe et sammenhængende og sikkert betalingssystem (Ibid.). Derudover er der indført nye regler for betalingstjenester, med det formål at gøre betalinger i andre EU-lande, lige så nemme og sikre som inden for landets egne grænser. Formålet med den nye PSD3 er bl.a. at skærpe kravene til de tekniske løsninger bag forbrugerautentifikation og reglerne for adgang til kundedata, som skal inkorporeres i national lovgivning (Nordea, 2024). PSR viderefører reguleringen af bankernes ansvarsområder og bliver automatisk lov for alle EU-medlemsstater. I PSR fastlægges et mål om, at udbydere af elektroniske kommunikationstjenester og betalingstjenesteudbydere

samarbejder, når der er mistanke om spoofing. Derudover skal de implementere tekniske tiltag, der styrker sikkerheden.

FD er positivt indstillet overfor, at der i PSR appelleres til større samarbejder på tværs af sektorer, men håber at det, i den endelige udgave, kan blive en forpligtelse frem for en opfordring (Bilag 5: 6). I et høringssvar til EU-specialudvalget for den finansielle sektor, beskriver FD: *"Da meget af svindelen opstår på internetplatforme og sociale medier, ønsker Finans Danmark, at ansvar og forpligtigelsen til at samarbejde, udbredes til andre sektorer, f.eks. udbydere af internetplatforme og sociale medier"* (Fjord, 2023: 2). FD håber således, at implementeringen af PSD3 og PSR, kan føre til at de platforme, hvor kontakten mellem gerningsperson og forurettede kan opstå, gøres ansvarlige for at regulere spredningen af svindelforsøg på deres kanaler, så forekomsten mindskes. Med den nuværende PSD2, er bankerne forpligtede til at indberette det svindel de opdager til Finanstilsynet (Bilag 5: 15). FD har besluttet at deres medlemmer ligeledes skal indberette til FD, så de kan danne et samlet billede af modus og udviklingen af samme, som de rapporterer tilbage til medlemmerne, så de alle har samme vidensgrundlag for forebyggelsesarbejdet.

Samarbejder

FD har, som beskrevet, oprettet Svindel Task Forcen i starten af 2024, der har implementeret deres første tiltag vedrørende beløbsgrænser. Task forcen er baseret på viden fra den Hvidvask Task Force, FD etablerede for 3 år siden (Bilag 5: 34). Her kortlagde de, hvordan hvidvask foregår og fandt derigennem løsninger til at identificere og begrænse det. Nu vil de gøre det samme med svindel (Bilag 5: 34-35). Målet er at Svindel Task Forcen skal afdække alle led i de kriminelle hændelser ved at styrke borgernes digitale dannelse, lave tekniske tiltag der forhindret svindel, evt. etablere AI baserede løsninger, forbedre sikkerheden i telenettet, styrke indsatsen mod svindel på sociale medier og digitale handelsplatforme samt øge politiets mulighed for at opklare det efterforskningsmæssige arbejde (Bilag 5: 35).

Eksternt, deltager FD bl.a. i FITs arbejdsgruppe om simswap og spoofing (Bilag 5: 31) og DKRs udvalg for Borgernes Digitale og Daglige Tryghed (Bilag 5: 33), der *"...forebygger kriminalitet ved at øge digitale dannelse og tryghed blandt voksne borgere"* (Det Kriminalpræventive Råd, 2024). Begge samarbejder er opstartet i 2024 og der er derfor ikke offentliggjort tiltag fra disse endnu.

Oplysningskampagner

FD udarbejder oplysningskampagner sammen med adskillige samarbejdspartnere, bl.a. Digitaliseringsstyrelsen, NCIK, DKR, Ældresagen, Forbrugerrådet Tænk og Teleindustrien (Bilag 5: 1+13+28+29). Derudover er der 'Cybersikkerhedsmåneden' i oktober (Bilag 5: 12). Generelt anser Torben kampagnerne som et forsøg på at øge befolkningens robusthed og derigennem reducere konsekvenserne af de svindelforsøg, bankerne ikke er i stand til at forhindre. Samtidig påpeger han at effekten af dem er kortvarig (Bilag 5: 12) og den måde kampagnerne aktuelt produceres og spredes på, virker kontraproduktivt: *"Vi ved også godt det med at oplysningskampagner ikke skal komme med for mange råd, fordi lige så snart man har sagt to ting, så kan folk ikke huske mere*" (Bilag 5: 12-13). Ifølge Torben vil det være mere produktivt, hvis kampagnerne spredes ud over året og at de gode råd samles ét sted, så borgerne ved, hvor de skal finde information (Bilag 5: 31).

Ifølge Torben vil forebyggelsen være mest effektiv, hvis der først og fremmest arbejdes på at reducere forekomsten af svindel: *"... den tekniske infrastruktur, det er selvfølgelig nr. 1, kan det overhovedet lade sig gøre at lave noget med mitigerende og begrænsende? Kan man få noget lovgivning på plads til at man kunne gå ned og kigge og filtrere i det? Det er nr. 2"* (Bilag 5: 40). Som beskrevet, er FDs evner til at implementere forebyggende eller forhindrende sikkerhedsforanstaltninger på nogle områder begrænset af lovgivning og de er dermed afhængige af brede samarbejder indenfor, og på tværs af sektorer: *"Nr. 3, det er det svindel der så kommer igennem. Der vil altid være nogen, der bliver ramt af noget, så skal man stadigvæk fortsætte med at fortælle folk, hvad de kan blive udsat for og hvordan de skal forholde sig, altså informere omkring det"* (Bilag 5: 40).

Opsummering

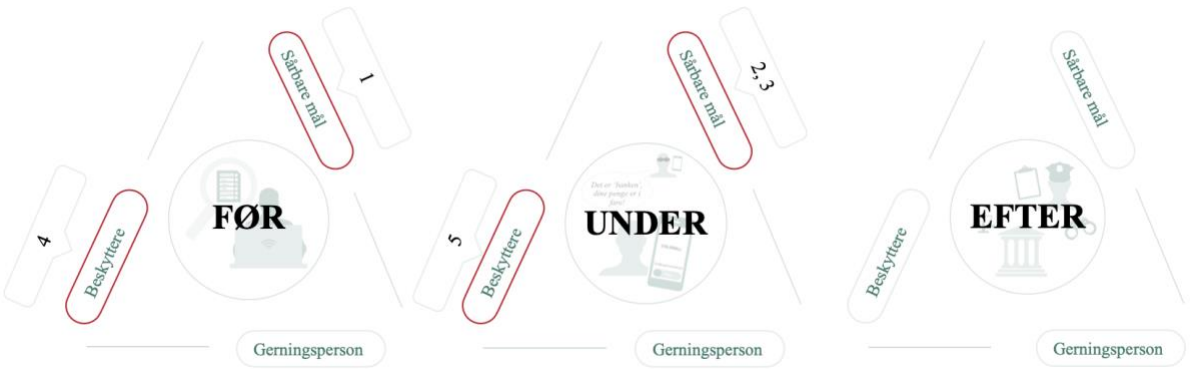
Vi har identificeret fem konkrete tiltag, der aktuelt er implementeret i FDs forebyggelse af vishing:

Tabel 6: *FDs tiltag*

Finans Danmarks forebyggelsestiltag	
1	Oplysningskampagner
2	Ny daglig beløbsgrænse
3	MitID
4	Diverse samarbejder
5	Videndeling i finanssektoren

Tiltag nr. 1, er ligesom ved TI, et tiltag der har til formål at styrke borgernes evner til at identificere forsøg på svindel, inden det udføres. Tiltag nr. 2 og 3 er tiltag orienterede mod de sårbare mål, men under udførelsen af kriminaliteten, idet de kommer i spil ved selve overførslen. Tiltag nr. 4 og 5 har begge til formål at styrke andre aktører i forebyggelsen, både på tværs af og inden for den finansielle sektor. De eksterne samarbejder fokuserer primært på oplysningskampagner eller teknologiske sikkerhedsforanstaltninger, der kan reducere forekomsten af svindel. Dermed placeres samarbejderne før vishing. Videndelingen inden for sektoren omhandler primært samarbejdet i NFCERT, som styrker bankernes evner til at kunne følge med i det aktuelle kriminalitetsbillede og tilpasse deres monitorering, hvorfor dette tiltag placeres under udførelsen af vishing.

Figur 11: *Opsummering – FD*



Note: Egen illustration

Banker

Vi har valgt at inddrage informanterne Pernille og Jesper fra Spar Nord (SN) samt Niels fra Danske Bank (DB) i vores undersøgelse, da de som fraud specialister i to større danske banker har erfaring med hverdagens praktiske del af finanssektorens forebyggelse.

Oplysningskampagner

Ligesom TI og FD, laver bankerne oplysningskampagner. Bankerne laver dog ikke deres kampagner i samarbejde med andre. De laves internt og udsendes primært i bankernes egne kanaler til kunderne. De udsender både generel informationsmateriale om digital svindel, men også specifikke advarsler til kunderne (Bilag 7: 4). Jesper udtrykker direkte, at han ikke er tilhænger af kampagnerne, men at det er en forventning til bankerne:

> *"Det er ekstremt generisk og det er ikke den form for forebyggelse, jeg er mest tilhænger af, fordi hvis du taler med en eller anden given person i Danmark og siger,* "Må du klikke på links eller må du snakke med mennesker du ikke kender om det her i telefonen?". *Så vil de sige nej, men når de står i situationen, så gør de det bare engang imellem alligevel"* (Bilag 6: 2).

På trods af skepsis, laver SN kampagner og kigger på, hvorvidt deres kunder anvender deres netbank, for at bedømme om den enkelte kunde skal have tilsendt informationen med posten eller i den elektroniske indbakke (Bilag 6: 9). Begge banker laver nogle få generelle anvisninger, som de sender ud til kunderne få gange om året, samt flere målrettede advarsler drypvis i løbet af året. Ifølge Jesper har de fleste banker et årshjul, som hjælper dem med at være opmærksomme på, hvornår på året de skal advare deres kunder om specifikke former for svindel, f.eks. svindel med udlejning af lejeboliger i forbindelse med studiestart (Bilag 6: 6).

Både Jesper og Niels fortæller, at de ikke kan sige noget om, hvor stor en effekt deres kampagner reelt har. For det første påpeger Jesper, at der er risiko for at store mængder af information om svindel bliver filtreret fra i kundernes bevidsthed (Bilag 6: 3). SN har leveret data til Jensen et al. (2024) undersøgelse om oplysningskampagnens effekt, der, som beskrevet i litteraturreviewet, viser at effekten er kortvarig. For det andet pointerer Niels, at der ikke er nogen der ved, hvor meget svindel der egentlig er i omløb og, både han og Jesper, pointerer at der ikke er nogen, der ved hvor meget af svindlen deres kunder ignorerer (Bilag 7: 10; Bilag 6:

16). For det tredje er det, ifølge Niels, svært at vurdere effekten af en kampagne, hvis banken samtidig har implementeret nogle tekniske kontroller i deres transaktionsmonitorering (Bilag 7: 9). Derudover kan det, ifølge Jesper, være kontraproduktivt for forebyggelsen at lave oplysningskampagner: "*Vi kan jo også høre, at svindlerne bruger vores egne informationskampagner imod os"* (Bilag 6: 9).

Modstykket til kampagner er, ifølge begge bankers fraud specialister, at forstyrre brugeroplevelsen af elektroniske overførsler ved at lave pop-up beskeder på skærmen undervejs. Beskederne gør kunden opmærksom på, hvad vedkommende er ved at foretage sig eller advarer f.eks. om specifikke svindeltyper, der er i omløb (Bilag 6: 3). For at styrke pop-up beskedernes effekt mener Niels at det vil være brugbart, hvis det undersøges, hvilke ord, der har den største effekt på kundernes bevidsthed (Bilag 7: 11).

Udover kampagner og pop-up beskeder, fortæller fraud specialisterne også, at de begge laver målrettet forebyggelse mod vishing i samarbejde med Ældresagen. SN har, sammen med Ældresagen og politiet, lavet informationsaftener for ældre, hvor de har fortalt dem, hvad de skal passe på og kan gøre, hvis de bliver udsat for vishing (Bilag 6: 8). DB har trænet frivillige i, at kunne træne medlemmerne i Ældresagens lokale klubber, i it-sikkerhed og derved styrke deres digitale færden (Bilag 7: 5).

Transaktionsmonitorering

Bankerne forsøger aktivt at stoppe svindlen, mens den udføres ved at monitorere transaktioner. Deres monitoreringer er baseret på, hvad SN kalder, 'beslutningstræer', *"... hvor du kører en transaktion ned igennem tragter, ift. at vurdere, om det kan være svindel. Hvis den falder ud skævt, så skal vi snakke med kunden"* (Bilag 6: 16). Tragtene består af koder, der beslutter, hvad monitorerne skal lede efter og reagere på. Koderne er udgjort af mavefornemmelser, samt lavpraktiske og logiske principper, såsom geografisk uoverensstemmelse mellem den computer vedkommende forsøger at logge på med MitID, og telefonen med MitID'et befinder sig på. Koderne er indtastet manuelt i beslutningstræerne og udvides kontinuerligt, som kriminalitets-form og modus udvikler sig.

Fraud specialisterne fra begge banker ser monitoreringen som deres mest effektive værktøj, *"... som bremser rigtig meget svindel, rigtig, rigtig meget svindel*" (Bilag 6: 13). "*Det er der hvor*

bankerne kan gøre rigtig, rigtig meget" (Bilag 7: 3). Samtidig forventer de, at de i fremtiden primært vil se svindelsager, hvor kunden er blevet manipuleret til selv at autorisere overførslen, hvilket vil udfordre monitoreringen: *"Det er der en soleklar årsag til. Det er nemmere at fange det, hvor den kriminelle laver det, fordi du har mange tekniske data. [...] Musehastighed, you name it"* (Bilag 7: 11). Anvendelsen af manipulation skaber således større krav til udvikling af bankernes monitorering og vores informanter giver udtryk for, at de ønsker at kunne gøre brug af machine learning og AI i fremtiden. Sådanne værktøjer vil gøre beslutningstræeerne i stand til selv at udvikle nye kodningstragter undervejs, som nye tendenser opstår (Bilag 6: 16). Derudover mener Niels, at bankerne i større grad vil blive afhængige af at kunderne indrapporterer det de bliver udsat for, som ikke fanges i bankernes monitorering (Bilag 7: 12). Den primære udfordring er således det manipulerende element, der gør, at kunderne, ifølge Pernilles oplevelse, ikke handler rationelt i situationen (Bilag 6: 3).

For at modarbejde kundernes irrationelle handlinger laver begge banker forstyrrelser i 'kunderejsen'. Det betyder at der undervejs, i en bankoverførsel, kommer beskeder frem, som advarer kunden eller spørger om de er sikre på at de vil lave overførslen (Bilag 7: 11). I SN er de enige med Niels i, at den uforstyrrede brugeroplevelse giver gerningspersonerne en fordel. Pernille påpeger dog, at bankerne heller ikke må forstyrre brugeroplevelsen for meget, da de samtidig har forpligtelser over for f.eks. Visa og MasterCard, om at begrænse antallet af falske positiver, så kunderne får en nem og gnidningsfri oplevelse (Bilag 6: 19). Dette indebærer, at bankerne skal begrænse antallet af falske positiver i deres monitorering.

Samarbejder

Jesper fortæller, at de i SN, generelt er lidt afventende med at indgå i forebyggende samarbejder, hvor der er aktører, som har en økonomisk interesse som f.eks. MasterCard. Ifølge Jesper er de bedste samarbejder SN indgår i, de samarbejder, hvor aktørerne er på lige fod og arbejder på samme måde (Bilag 6: 22). Hertil nævner Jesper NFCERT som et godt eksempel:

> *"Deres [NFCERTs] logo er sådan et puslespil, fordi når det kommer til fraud, så sidder vi med hver vores puslespilsbrik i sektoren og hos myndighederne. Men kun ved at vi taler sammen, kan vi se, hvad det fulde billede er…"* (Bilag 6: 11).

Niels påpeger at NFCERT også styrker de mindre banker, som ikke har lige så meget data at trække på, som f.eks. DB, der, udover Danmark, har filialer i Sverige, Norge, Finland og Nordirland og dermed har mulighed for at trække på egne data for digital svindel i andre lande. Der er således ikke et konkurrerende element blandt bankerne, når det kommer til bekæmpelsen af vishing og generel digital svindel. Tværtimod er der et fælles ønske om at samarbejde, så de ikke forflytter problemet til andre banker (Bilag 7: 13).

Da transaktionsmonitoreringen for nuværende er opstillet efter den manuelle kodning af beslutningstræet, giver SN udtryk for at være afhængige af NFCERT samarbejdet, så de kontinuerligt kan danne sig et fyldestgørende trusselsbillede. Udfordringen i NFCERT er dog, ligesom i monitoreringen, anvendelsen af data:

> *"I de fællesskaber, der kan vi tale om objektive indikatorer på svindlen. Vi må ikke komme langt ned. [...] Men vi må godt tale om, at vi ser en overvægt af ældre eller... Geografisk område, der er udsat for et eller andet…"* (Bilag 6: 11).

Især fraud specialisterne fra SN fortæller, at det er begrænsende for deres arbejde, at de kun må dele information om modus og tendenser for, hvilke strategier de kriminelle p.t. anvender, f.eks. om det er bestemte banker der overføres til. Begge banker er interesserede i at kunne komme til at dele flere informationer i fremtiden, fordi det, i deres optik, vil styrke forebyggelsen. Jesper fortæller f.eks., at det vil være behjælpeligt, hvis de kan få lov til at dele information om IP-adresser, telefoner, simkort og lign. med andre banker, når de opdager at sådanne anvendes til svindel. Hvis de måtte dele sådanne oplysninger vil de, ifølge Jesper, kunne få lukket ned for svindlen fra det pågældende device og derigennem beskytte forbrugerne mere effektivt: "*Men det må jeg ikke. Jeg må ikke engang sende en IP-adresse til en i Jyske Bank... På et Lebara taletidskort... Det er simpelthen så dumt"* (Bilag 6: 25).

Fraud specialisterne fortæller, at øgede muligheder for datadeling ligeledes vil kunne gavne deres samarbejde med andre sektorer. Niels fortæller f.eks. at det kan give bedre indsigt i det fulde omfang af vishing og andre former for svindel. De nuværende begrænsninger for datadeling gør det kun muligt for bankerne at have indsigt i, hvor stort et omfang af svindlen, der når til en egentlig transaktion. Derudover ved de heller ikke, som tidligere beskrevet, hvad effekten af kampagnerne mod vishing er, ift. deres transaktionsmonitorering: "*... er det noget data Teleindustri på en eller anden måde kunne have? I have no idea. Dette understreger*

vigtigheden af, at vi samarbejder for at forstå det fulde omfang" (Bilag 7: 10). I forlængelse heraf påpeger Jesper, at de heller ikke må handle på svindel, de kan se udfolde sig i realtid. Han beskriver, at de kan sidde og følge med i, at et betalingskort, som de ved, ikke længere er i ejerens varetægt, anvendes til at købe varer til afhentning hos Elgiganten De må dog ikke ringe til Elgiganten og bede dem om at tilbageholde varen, fordi de ikke må videregive kortoplysninger (Bilag 6: 12). Som Jesper pointerer, er SN ikke interesseret i at data deles ukritisk, men håber at de kan komme til at dele mere eller få samtykke fra kunderne om, at de må indhente risikodata fra f.eks.:

> "*... teleinfrastrukturen, fra NemKonto infrastrukturen, fra Apple og Google, fra MitID. Så det egentlig ikke er så meget MitID, der skal fortælle os, at en kunde er ved at blive svindlet, men de sender bare en masse data med, sammen med login'et og geolokation, IP-adresse osv."* (Bilag 6 : 15).

Begge bankers fraud specialister fortæller, at selvom de overordnet set er positivt stemte for samarbejderne i FIT, hvor de arbejder sammen med medarbejdere fra andre sektorer og dermed får input fra *"... forskellige dele af kæden*" (Bilag 6: 22), ser de også et potentiale for datadeling her, fordi FIT-samarbejdet ligeledes er hæmmet af lovgivningen. Ingen af specialisterne tilskriver FIT-samarbejdet nogen betydelig indflydelse på deres aktuelle forebyggelse af vishing. I stedet forklarer de, at det ofte er mere relevant at en repræsentant fra deres respektive datacentral deltager (Bilag 6: 21).

Udover at dele data med relevante aktører, ønsker DB og SN ligeledes, som FD har udtrykt i deres høringssvar til EU-Kommissionen om PSD3 og PSR, at flere relevante aktører pålægges ansvar for at være med til at bekæmpe digital svindel:

> *"Hvordan starter svindlen? Hvis det er en telefon, så vil Teleindustrien på en eller anden måde have en rolle. Hvis det er en artikel på Facebook, så må de have en rolle"* (Bilag 7: 4).

Specialisterne fra SN er enige med Niels i, at flere aktører skal kunne pålægges et ansvar for spredningen af digital svindel:

> "*Det er også en af de her bagtanker i PSD3; Hvis du er en del af værdikæden for svindel, så skal du også hjælpe os, der er udsat for det"* (Bilag 6: 7).

På trods af at begge banker primært er positivt stemt over for samarbejder på tværs af sektorerne, efterspørger de, at disse styrkes yderligere i fremtiden. Niels oplever samtidig sektorernes forskellige kategoriseringer af svindeltyper, som en udfordring i samarbejderne. De forskellige kategoriseringer skaber, ifølge Niels, forskellige trusselsbilleder, der gør det svært at sammenligne på tværs af sektorer (Bilag 7: 8).

Vidensgrundlag

Begge banker har, som beskrevet i det foregående afsnit, en fordel pga. deres størrelse og dertilhørende interne mængder af data, de hver især besidder. Det styrker deres daglige arbejde med svindelbekæmpelse, da deres datasæt er store nok til at de kan lave generaliseringer foruden NFCERT. Jesper fortæller dog, at de i SN er afventende med at reagere på nye tendenser ud fra egne data, fordi de gerne vil undgå at implementere tiltag på spinkle grundlag, der leder til falske positiver: "*Vi prøver på ikke at løbe efter ting, der ikke rigtigt har manifesteret sig endnu. Og det kan faktisk godt være noget af det sværeste synes jeg"* (Bilag 6: 18). De venter således på, at tendenser enten manifesterer sig i datamaterialet, eller til de hører, at tendensen opleves bredt i NFCERT.

Både SN og DB fortæller, at de særligt retter deres opmærksomhed mod England og Sverige, fordi bankerne har observeret, at nye typer af digital svindel, oftest opstår på de kanter og efterfølgende vandrer til Danmark (Bilag 6: 19). Ifølge Jesper er grunden til, at de ser nye svindeltyper vandre på den måde, at:

> *"... de har de største bander, Sverige, og så starter de jo en ny gruppering op i et nyt land. Så kører de tit bare lige over Øresund og så plejer det at slutte i Norge. Vi har også set rimelige klare indikationer i nogle sager på, at det er det samme persongalleri, og at der er nogen, der skal læres op af nogen, som man godt kendte i forvejen, fra andre grupperinger. Det er organiseret kriminalitet. Og så forplanter det sig bare"* (Bilag 6: 19).

Denne observation afspejles i fundene fra Choi et al.s (2016) og Lee's (2020) studier, som begge peger på, at der sker en oplæringsproces inden vishing kan udføres. Hvor der skal rekrutteres "medarbejdere", som oplæres i, enten at foretage telefonsamtalerne eller til at hæve kontanter fra forurettedes bankkonto. Samtidig fremgår det af begge studier, at handlingerne er organiseret i en hierarkisk struktur, hvor opgaverne fordeles mellem gerningspersonerne.

Derudover henter DB og SN inspiration fra det forebyggende arbejde, der udføres i UK. Som Niels beskriver det, er disse lande langt foran Norden på forebyggelsesområdet, fordi de ikke er bundet af de samme reguleringer vedrørende datadeling som medlemmer af EU (Bilag 7: 21). I UK har de derfor andre muligheder for at implementere tekniske løsninger, der går på tværs af systemer og kan dermed nemmere dele viden på tværs af sektorer.

Tilbageførsel af svindeltransaktioner

Hvis et svindelforsøg slipper igennem monitoreringen uopdaget, og de kriminelle lykkes med vishingforsøget, forsøger banken at få det mistede beløb tilbage til forurettede. Det er dog en opgave, der især er besværet af at kriminaliteten foregår på tværs af landegrænser og, som Jesper beskriver, at det går meget hurtigt med at flytte ting elektronisk: "*Af de penge, der forlader banken via kort og kontooverførsler. Der er det, måske 10 %, vi får hjem. Hvis tingene først har forladt banken, er det ikke nemt"* (Bilag 6: 14). Når svindlen er foregået på tværs af landegrænser forsøger banken, gennem det pågældende lands lovgivning, at sørge for at de kriminelle ikke får råderet over pengene, men det kræver at en retsanmodning fra Danmark, hvilket er tidskrævende (Bilag 6: 13). Pernille og Jesper kalder det for "brandslukning", da det er det sidste, de kan gøre, for at sikre at pengene ikke overgår til gerningspersonen. Hertil ser de en fremtidig udfordring ved, at PSD3 og PSR søger at optimere brugeroplevelsen. Da det kan fremmer konkurrencen i den finansielle sektor, på internationalt plan, og øger efterspørgslen på at kunne straksoverføre på tværs af landegrænser:

> *"Vi kan altid ringe til Danske Bank og så sige, "*Vil I bremse det her?*". Vi kan ikke ringe til en lokal spansk bank, dem har vi ikke noget samarbejde med. Så lovgivningen og den evige søgen efter, at forretningsudviklingen for finansielle institutioner skal gå så hurtigt, og det helst skal være uden menneskelig kontakt - den her friktionsløse brugeroplevelse gør, at det er svært at bremse svindel"* (Bilag 6: 14).

Håndtering af kunder

Hvis banken har opdaget svindlen, inden en overførsel er gået igennem, ringer banken forurettede op for at undersøge, hvorvidt det er en legitim overførsel eller ej. Hvis svindlen er gået igennem sikkerhedsforanstaltningerne og monitoreringen ikke har fanget det, ringer kunden selv til banken, såfremt kunden selv opdager svindelen. I kontakten med en kunde, der har været udsat for svindel, oplever både DB og SN, at vedkommende kan være i tvivl om det nu er den rigtige bank de taler med, eller om det er andre kriminelle, der har ringet dem op (Bilag 6: 5; Bilag 7: 5). Begge banker forsøger at forsikre kunden om bankens legitimitet ved at henvise kunden til bankens hovednummer og bede om at blive stillet om til den afdeling, rådgiveren oplyser de sidder i, eller direkte til den pågældende rådgiver, der har kunden i røret. Derudover forsøger bankerne ligeledes at sikre, at det er den rigtige kunde de taler med ved at stille nogle kontrolspørgsmål, der både kan være bankrelaterede eller omhandle andre ting, som farven på kundens hus (Bilag 6: 5).

Når kunden og banken er forsikret om, at de begge taler med den korrekte person, laver rådgiveren en individuel vurdering af, hvad den pågældende kunde har brug for af rådgivning (Bilag 7: 18; Bilag 6: 27). Rådgiveren vurderer kundens behov ud fra selve samtalen med kunden, hvor nogle er rystede ovenpå oplevelsen og andre bare efterspørger en 'køreplan' for den videre proces med anmeldelse og dækning af tabet (Bilag 6: 27). Pernille, Jesper og Niels fortæller alle tre, at de ikke behandler kunder, der har været udsat for svindel, efter en standardprocedure. De går op i at være fleksible, så de kan give kunden den rådgivning og hjælp vedkommende har brug for. Uanset, hvad kunden har brug for, bliver de oplyst, både mundtligt og skriftligt, om at de kan opleve at blive udsat for ny svindel (Bilag 7: 3; Bilag 6: 26). Den forurettede kan risikere at deres kontaktinformationer bliver solgt videre til andre gerningspersoner, der udsætter dem for vishing på ny, eller at de samme gerningspersoner ringer igen og forsøger at gennemføre et *recovery scam:*

> *"Efter noget tid kommer svindleren tilbage. De kan udgive sig for at være nogle andre og sige, "*Vi ved godt du er blevet udsat for svindel, skal vi hjælpe med at få pengene tilbage?*". Der har vi jo, som bank, allerede forsøgt os med at få pengene tilbage, men gerningspersonerne binder kunden en løgnehistorie på om, at de f.eks. er verdens bedste til det, at de ved at pengene gik til Kina og der er de eksperter i at få pengene*

> *tilbage fra. De skal bare lige have et fee up front. Så er du blevet svindlet to gange"* (Bilag 7: 3).

I de sager, hvor det udelukkende er kunden, der har lidt et tab, rådgiver bankerne kunden om at lave en politianmeldelse. Hvis banken også har lidt et tab, anmelder de både eget og kundens tab (Bilag 6 : 27; Bilag 7: 18).

Betalingsloven § 100

Fraud specialisterne fra begge banker fortæller, at ansvaret for tabet afhænger af, hvem der har 'trykket på knapperne' (Bilag 6: 28; Bilag 7: 19). I de tilfælde hvor gerningspersonen har tilegnet sig kundens oplysninger eller kreditkort og dertilhørende kode, og autoriserer overførsel eller laver kontanthævning, hæfter banken for tabet. I de tilfælde hvor kunden selv har udført overførslen eller hævningen, hæfter kunden for tabet. Det er ikke noget bankerne har besluttet, det er praksis jf. betalingsloven § 100. Ifølge Niels vil der i fremtiden være flere af de forurettede, der har været udsat for vishing, der kommer til at hæfte for hele tabet selv, fordi han, som tidligere beskrevet, forventer at de kriminelle i højere grad vil manipulere de forurettede til at autorisere overførslen selv (Bilag 7: 20).

Det er dog noget PSD3 og PSR kan få indflydelse på: "*Og det er svært lige nu at vide, om det vil være i forbrugernes favør, eller om det ville være i vores favør, hvis man kan stille det sådan op"* (Bilag 6: 28). Som PSR er lagt ud lige nu, kommer banken til at hæfte for hele beløbet første gang en kunde manipuleres til at gennemføre en overførsel, hvor spoofing er anvendt til at få kunden til at tro, at det er banken de har talt med, og kun hvis kunden ikke har handlet svigagtigt eller groft uagtsomt (Økonomiministeriet, 2024). En udfordring for bankerne er, at det således kun er betalingstjenesteudbyderne, som dem selv, der hæfter for hele beløbet ved disse specifikke sager. De danske forbrugere er derfor bedre stillede med EU-kommissionens nuværende udspil til PSR, end de er i betalingsloven (Ibid.). Som det er beskrevet i FDs høringssvar til EU-specialudvalget formodes det, at forekomsten af svindel vil stige, hvis forbrugerne stilles bedre, fordi det kan medføre mindre agtpågivenhed hos forbrugeren (Fjord, 2023: 2+9). Dette kan udgøre en risiko for at forekomsten af svindel stiger og at bankerne dermed må hæfte for mere. SN og DB bakker således op om FDs høringssvar, der appellerer til at andre sektorer holdes ansvarlige for at opdage og stoppe svindlen, så bankerne fremadrettet ikke kommer til at hæfte for lige så mange økonomiske tab.

Opsummering

Vi har identificeret syv forskellige tiltag, som SN og DB p.t. udfører i deres forebyggelse mod vishing:

Tabel 7*: SN og DBs tiltag*

Spar Nord og Danske Banks forebyggelsestiltag	
1	Oplysningskampagner
2	Forstyrrelser i brugeroplevelsen af overførsler
3	Informationsaftener for, og it-træning af Ældresagens medlemmer
4	Transaktionsmonitorering
5	Videndeling i NFCERT
6	Tilbageførsel af svindeltransaktioner
7	Rådgivning af kunder

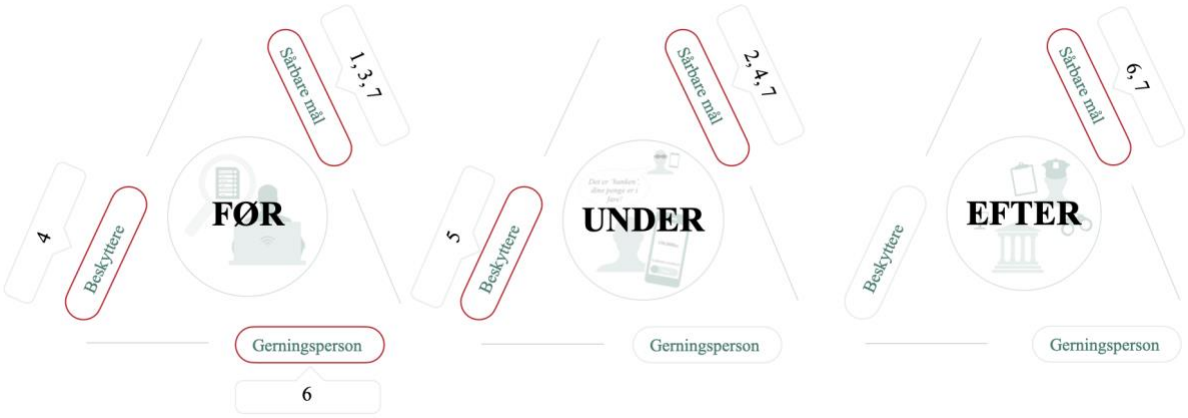
Tiltag nr. 1 og 3, søger begge at øge borgernes evner til at genkende svindelforsøg, før de bliver udført og indgår således i forebyggelsen, der finder sted før vishing. Tiltag nr. 3 er derudover målrettet en specifik borgergruppe.

Tiltag nr. 2 og 4 har til formål at (identificere og) beskytte kunden, der er ved at blive svindlet. Disse tiltag indgår således under udførelsen af vishing. Tiltag nr. 5 udføres på baggrund af bankernes individuelle observationer, hvilket gensidigt kan styrke deres kodning bag transaktionsmonitorering af de aktive svindelforsøg. NFCERT-samarbejdet styrker således bankernes kompetencer til at beskytte deres kunder under udførelsen af vishing.

Tiltag nr. 6 udføres efter at svindlen har fundet sted og har til formål at mindske forurettedes tab. Således er dette tiltag med til at forhindre gerningspersonen i at få udbytte fra den kriminelle handling. Vi argumenterer for, at dette muligvis kan være med til at mindske gerningspersonens motivation for at udsætte andre for vishing i fremtiden, hvorfor vi mener, at dette tiltag både kan indgå i forebyggelsen efter det oprindelige svindelforsøg og inden udførelsen af et nyt. Tiltag nr. 7 udføres, ligesom tiltag nr. 6, efter vishing er udført. I rådgivningen er der fokus på at hjælpe forurettede med at anmelde, samt informere

vedkommende om risikoen for at blive forsøgt svindlet igen. Bankerne forsøger dermed at forberede vedkommende på fremtidige svindelforsøg og derigennem ruste dem til at være mindre sårbar i lignende situationer i fremtiden. Selvom kunderådgivningen finder sted efter svindlen er udført, hjælper dette initiativ med at ruste kunden til at forholde sig mere kritisk over for både smishing og phishing, som finder sted inden kriminaliteten udføres, samt direkte opkald fra gerningspersoner under forsøget på et nyt vishingforsøg. Kunderådgivning kan således reducere den forurettedes sårbarhed før og under nye svindelforsøg.

Figur 12: *Opsummering – Banker*



Note: Egen illustration

8.1.3 Efter vishing

Efter vishing er udført og den kriminelle har tilegnet sig den forurettedes penge, kan det, som ved alle andre kriminelle hændelser, anmeldes til politiet, der igangsætter en efterforskning. Som vi har beskrevet i afsnit 2.2, modtager NCIK hele landets anmeldelser om vishing og andre former for kontaktbedrageri, som i stigende grad henlægges (mere end halvdelen af sagerne i 2022) (Bilag 1). NCIK er dermed, i mange sager, afhængige af at involvere udenlandske politimyndigheder i efterforskningen, hvilket kræver en rimelig formodning om, at en gerningsperson kan udleveres og at der er tale om gentagen eller alvorlig kriminalitet, som vil medføre en straf ved domfældelse (Retsudvalget, 2022: 4-5). På trods af, at antallet af både anmeldelser og henlæggelser af sager om vishing stiger, er der få sager der fører til domfældelse. I 2022 faldt der kun dom i 5 ud af 750 anmeldelser om vishing (Kirkebæk-Johansen & Jorsal, 2023). Det tyder på, at det digitale, grænseløse element i sager om vishing,

udfordrer politiets efterforskning og dermed en efterfølgende retsforfølgelse. Hvis en sag om vishing retsforfølges, kan der straffes efter straffelovens § 279 om bedrageri eller § 279a. Straffelovens § 279 om bedrageri anvendes i sager, hvor gerningspersonen har bragt forurettede i en vildfarelse, der har fået forurettede til at udføre en overførsel eller kontanthævning til gerningspersonen. § 279a om databedrageri anvendes i sager, hvor gerningspersonen uberettiget har tilegnet sig forurettedes informationer og gerningspersonen således selv har foretaget overførslen eller kontanthævningen.

En anmeldelse om vishing indebærer den forurettede og gerningspersonen, der har udsat den forurettede for forbrydelsen. Sammen med politiet og retssystemet udgør de aktører, der involveres efter vishing er udført. Da det danske retssystem ikke iværksætter deciderede forebyggelsestiltag, vil vi i dette afsnit udelukkende præsentere NCIKs forebyggelse af vishing. Hertil inddrager vi informanten, Sofie, som arbejder i NCIK og er ansvarlig for FIT-samarbejdet.

Politi

NCIK varetager politiets *"... nationalt koordinerende forebyggende indsats for it-relateret økonomisk kriminalitet*" (Politi, n.d. *c*), herunder vishing. Sofie fortæller at sektionen for analyse og forebyggelse i NCIK, overordnet har tre forskellige arbejdsområder: 1) databehandling og dataanalyse, 2) kommunikation og awareness og 3) strukturelt forebyggelsesarbejde, hvor FIT er kerneelementet (Bilag 8: 2-3).

FIT

FIT består af ca. 90 organisationer og 150 medlemmer, som er en blanding af private og offentlige organisationer, der samarbejder; *"... konstruktivt og målrettet for at forebygge og mindske it-relateret økonomisk kriminalitet"* (Politi, n.d. *a*). Samarbejdet er forankret i fem interessegrupper, og én fokuseret arbejdsgruppe med højere krav til fremdrift og resultater, der arbejder med hver deres problemfelt i minimum et år ad gangen (Bilag 8: 8-9). Der er som minimum en styregruppere præsentant i hver gruppe. Styregruppen består af udvalgte medlemmer af FIT, som har meldt sig i en toårig periode. Årshjulet for FIT består, foruden gruppearbejdet, af 2-3 faglige 'gå-hjem-møder', en temadag midt på året og afsluttes med et årsmøde, hvor grupperne præsenterer resultaterne af deres samarbejder (Bilag 8: 11-12). Efter

årsmødet kigger NCIK på, hvilke grupper der er relevante at etablere eller videreføre i det nye år, baseret på de problemfelter FIT mener er relevante at fokusere på. NCIK udpeger nogle af de medlemmer, de mener skal udgøre grupperne, for at sikre de rette kompetencer (Bilag 8: 8). Derudover kan andre med interesse for problemfeltet tilslutte sig. Interessegrupperne har selvbestemmelse over, hvilke resultater deres arbejde skal munde ud i. Det kan eksempelvis være videndeling, at opbygge netværk på tværs af sektorer eller specifikke løsninger (Bilag 8: 9). I år hedder de fem interessegrupper hhv. 'AI og deep fakes', 'Efterforskningsgruppen', 'Fragtrelateret fraud', 'MitID risikodata' og 'Influencer kampagnegruppen' (Bilag 8: 9). Den fokuserede arbejdsgruppe hedder 'Spoofing og misbrug af e-Sim'.

> "*E-Sim er et digitalt simkort. Du kan logge ind ved din teleoperatør og købe et e-Sim, som du installerer på din telefon uden at have et fysisk simkort i telefonen. [...] Det er der nogle fordele ved, men i svindeløjemed, er der også ulemper*" (Bilag 8: 10).

På tidspunktet for interviewet var de fleste arbejdsgrupper nye. Influencer kampagnegruppen, er dog en videreførelse fra sidste år. Sofie kunne således kun fortælle om det forventede slutprodukt af influencer kampagnegruppen; *"som er en awareness gruppe, der laver kampagner og arbejder på at få nogle midler til, at influencere skal ud og promovere det"* (Bilag 8: 9).

Arbejdsgruppernes problemfelter er relativt afgrænsede, for at få de medlemmer med i grupperne, som i særlig grad kan bidrage til den givne problemstilling (Bilag 8: 10). Ifølge Sofie er denne opdeling medvirkende til, at medlemmerne lettere kan komme i gang med at tale med hinanden om konkrete udfordringer og ideer til løsninger. Hvis arbejdsgrupperne oplever lovgivningsmæssige udfordringer for konkrete forebyggelsestiltag, overkommer de disse ved f.eks. at se mod de andre nordiske og europæiske lande, som har stået med lignende juridiske udfordringer (Bilag 8: 17). Disse observationer kan i visse tilfælde videreformidles til de relevante sektorer og ministerier, der kan føre det videre i Folketinget: *"Det er ikke sådan at vi går ud som politiet og siger, at vi er uenige i lovgivningen på området, men man kan adressere nogle konkrete udfordringer og prøver at aktivere nogle af de aktører på området, som rent faktisk kan gøre noget"* (Bilag 8: 17). Det er de bl.a. i gang med på spoofingområdet.

Sofie har indtryk af, at FIT skaber nye netværksmuligheder blandt medlemmerne. FIT synliggør mulige samarbejdspartnere for aktørerne og er en god måde at bringe de relevante aktører sammen om komplekse problemstillinger. Da disse ofte kræver forskellige kompetencer og fælles opbakning (Bilag 8: 13).

Datadeling

På trods af, at de i FIT taler om konkrete problemstillinger, uden at skulle dele personfølsomme data, fortæller Sofie, at;

> "*Nu hvor AI er kommet på banen, og da det går så superhurtigt med it-kriminalitet, så bliver det rigtig, rigtig svært at kunne følge med, hvis man ikke også begynder at dæmme lidt op for, hvordan man må udveksle oplysninger blandt de aktører, der har en rolle i at bekæmpe det. Det er allerede en meget vanskelig opgave at følge med*" (Bilag 8: 24-25).

FIT må ikke dele oplysninger, på samme måde, som de f.eks. har hjemmel til i ODIN-netværket, som også er et samarbejde mellem offentlige og private aktører, men som forebygger og bekæmper hvidvask og terrorfinansiering (Politi, n.d. *b*). Forskellen på de to forebyggelsesnetværk er, at ODIN har en specifik lovhjemmel til at udveksle oplysninger mellem visse sikkerhedsgodkendte parter, og at ODIN er et mindre og mere specifikt samarbejdsnetværk: "*...det er en helt anden situation at sige at 90 private/offentlige aktører bare må dele data, kontra 7-8 udvalgte aktører"* Bilag 8: 24). FITs brede involvering af aktører, udfordrer således implementering af en lignende lovhjemmel.

Grænseoverskridende kriminalitet

Selvom det grænseoverskridende element ved vishing udfordrer efterforskningsarbejdet, er det, ifølge Sofie, ikke nødvendigvis en udfordring for forebyggelsesarbejdet:

> *"... det forebyggelse man laver, laver man uagtet om det [svindelforsøget] kommer fra nogen i Danmark eller fra nogen i udlandet. Det handler mere om, at folk ikke falder i,*

> *eller at minimere det tab, de har, når de falder i [...] Hvis man går ud og advarer, med eksempelvis kampagner som 'Smæk røret på', så er det et forebyggelsestiltag, som er lige relevant, uanset om bagmanden sidder i Danmark eller i udlandet"* (Bilag 8: 30-31).

Hun fortæller at uanset om en gerningsperson sidder i Danmark eller udlandet og spoofer et opkald til en dansk person, går opkaldet igennem det danske telenetværk, som giver teleoperatørerne mulighed for potentielt at blokere det. Dette er dog modstridende med Jakobs udtalelse om at spoofingbeskyttelsen på fastnettelefonnummer, er baseret på en antagelse om, at de spoofede opkald kommer fra udlandet (Bilag 4: 14)[3].

Vidensgrundlag

Udover at facilitere netværksmuligheder og videndeling blandt de aktører, hvis arbejde er berørt af digital svindel, udvider FIT også NCIKs viden; "*...med viden fra deres [medlemmernes] bagland og deres kanaler"* (Bilag 8: 19). Derudover analyserer sektionen for analyse og forebyggelse, qua arbejdsområdet, der udfører databehandling og dataanalyse, på intern data og orienterer sig i rapporter fra andre lande. De deltager også i både nordiske samarbejder og i Europolsamarbejdet, *"...hvor man bl.a. laver erfaringsudveksling og deler viden om problematikkerne. Så det er nogle af de mere formelle fora vi er med i*" (Bilag 8: 19). Sektionen advarer også organisationer, myndigheder og virksomheder, hvis de ser en konkret problematisk udvikling på den pågældende aktørs område. Sofie fortæller eksempelvis at de på et tidspunkt så, at der blev sendt e-mails ud fra nogen, der udgav sig for at være Sygeforsikringen "danmark", der bad kunden om at opdatere betalingsoplysninger via et link. I dette tilfælde tog NCIK kontakt til Sygeforsikringen "danmark": "*Der har været et samarbejde med dem, som helt konkret gør, at de f.eks. har fjernet flere links i de mails de sender ud og har et andet introskriv på deres hjemmeside, hvor de advarer mod svindel*" (Bilag 8: 22).

[3]*NCIK har inden specialets aflevering gjort opmærksom på, at de tekniske mekanismer er komplekse, og kan variere afhængigt af, om det spoofede opkald starter i Danmark eller udlandet. NCIK er derfor ikke enige i specialets fortolkning af, at Teleindustrien og NCIK har forskellige opfattelser af, hvornår et spoofet opkald kan identificeres*.

Sektionens viden om aktuelle problemstillinger kan også understøtte efterforskningen på området,

> "*... hvis de oplever at der er nogen, [...] der f.eks. er lidt dårlige til at udlevere de oplysninger, der skal bruges, så kan vi eksempelvis række ud til aktøren og forsøge at gå i dialog med dem, eller eventuelt rette henvendelse til den brancheorganisation eller myndighed, de er underlagt.* (Bilag 8: 22).

Opsummering

Vi har identificeret fire konkrete forebyggende elementer ved arbejdet i NCIKs sektion for analyse og forebyggelse:

Tabel 8: *NCIKs tiltag*

NCIKs forebyggelsestiltag	
1	Facilitering af tværsektoriel videndeling og samarbejde i FIT
2	Varsling om akut problemstilling til berørte aktør
3	Viden- og erfaringsudveksling blandt politimyndigheder
4	Oplysningskampagner

Tiltag nr. 1 muliggør videndeling blandt aktører fra forskellige sektorer, hvilket hjælper dem med at danne et mere fuldkomment trusselsbillede, samt udvikle konkrete løsninger i fællesskab. FIT bidrager således til at styrke kompetencerne for forebyggelsesaktører både før og under udførelsen af kriminalitet. Det samme gør sig gældende for tiltag nr. 2. Tiltag nr. 3 bidrager til gensidig forøgelse af myndighedernes viden om aktuelle problemstillinger, hvilket styrker deres efterforskningsmæssige kompetencer og placeres i nedenstående figur 13, efter vishing. Foruden kampagnerne, der bliver udviklet i influencer kampagnegruppen, under FIT-samarbejdet, skaber sektionens kommunikations- og awareness-medarbejdere også oplysningskampagner, tiltag nr. 4, hvor politiet er afsender. Disse kampagner øger, ligesom kampagnerne fra andre aktører, borgernes bevidsthed om risikoen for svindel, før det sker.

Figur 13: *Opsummering - Politi*

Note: Egen illustration

8.2 Delkonklusion 1

Aktører

Gennem undersøgelsen af aktører, der fremstår som oplagte forebyggelsesaktører mod vishing, enten som en del af processen før, under eller efter de kriminelle handlinger udføres, er det tydeligt at det reelle forebyggelsesnetværk er ekstremt bredt. Ved at inddrage aktører, der repræsenterer cybersikkerhed, telesektoren, finanssektoren og politiet, samt ikke-menneskelige aktører, såsom dokumenter, (bl.a. lovgivning, direktiver, forordninger og høringssvar) teknologiske løsninger (f.eks. transaktionsmonitorering og MitID) og enheder som computere og telefoner i analysen, fremstår netværket allerede bredt.

I ekspertinterviewene blev 100+ nye aktører nævnt som værende en del af netværket. Flere af disse nye aktører, som eksempelvis Sygeforsikringen "danmark", fremstod ikke som oplagte aktører i forebyggelsen af vishing forinden undersøgelsen. Disse aktører er bl.a. nævnt som eksempler på platforme, der udnyttes til at initiere kontakten mellem gerningsperson og forurettede. Alle platforme for officielle institutioner, virksomheder, organisationer og myndigheder kan udnyttes, hvilket udvider netværket for potentielle aktører og gør listen uudtømmelig. Selvom de 100+ nævnte aktører ikke er blevet identificeret som nøgleaktører i netværksanalysen, formodes de at have en translaterende rolle (Latour, 2008: 64). I og med at de f.eks. implementerer tiltag på baggrund af henvendelser fra NCIK, interagerer de med deres brugere og får dem til at handle anderledes ved f.eks. at advare dem om spoofede beskeder og at fjerne skadesfulde links. Til gengæld blev cybersikkerhedseksperter oprindeligt betragtet som centrale aktører i undersøgelsen, men gennem analysen har det vist sig, at deres rolle

primært er formidlende, da det endnu ikke kan konkluderes, hvilke direkte tiltag, deres involvering i netværket bidrager til.

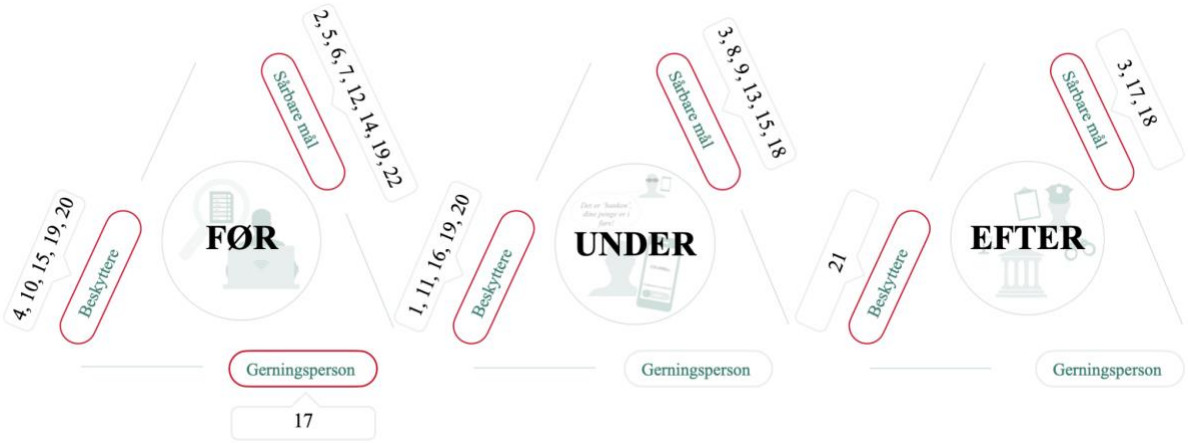
Overordnet består forebyggelsesnetværket mod vishing af:

- Digitale enheder
- Aktører, hvis digitale løsninger udnyttes til at udføre svindlen
- Politi - anmeldelser og efterforskning
- Domæner, der kan udnyttes til spoofing
- Regulering, politik og dertilhørende instanser
- Teknologiske sikkerhedsforanstaltninger
- Videndeling
- Oplysningskampagner
- Samfundets digitale robusthed

Forebyggelsestiltag

Gennem analysen har vi identificeret 22 individuelle forebyggelsestiltag, der aktuelt udføres af det undersøgte netværk. Overordnet dækker tiltagene over borgerrettet information, videndeling og samarbejde i, og på tværs af sektorer, teknologiske sikkerhedsforanstaltninger, akut orientering af andre aktører og facilitering af netværk for samarbejde. I nedenstående figur 14 visualiseres, hvordan de 22 tiltag fordeler sig før, under og efter kriminaliteten udføres og, hvorvidt tiltaget, iht. rutineaktivitetsteorien (Cohen & Felson: 1979), forsøger at eliminere forbrydelsen ved at ruste sårbare mål, øge beskytternes kompetencer eller mindske de kriminelles motivation.

Figur 14: *Netværkets forebyggelsestiltag*



Note: Egen illustration
Cyber: *1) Identificering af mulige tekniske indsatsområder*
Teleindustrien*: 2) Spoofingbeskyttelse af virksomheders afsender-ID på SMS'er. 3) Spoofingbeskyttelse af banker, Politi og myndigheders fastnettelefonnumre. 4) blokering af farlige links. 5) Anbefalinger til Ældresagen. 6) Oplysningskampagner.*
Finans Danmark*: 7) Oplysningskampagner. 8) Ny daglig beløbsgrænse. 9) MitID. 10) Diverse samarbejder. 11) Videndeling i finanssektoren.*
Spar Nord og Danske Bank*: 12) Oplysningskampagner, 13) Forstyrrelser i brugeroplevelsen af overførsler. 14) Informationsaftener for, og it-træning af Ældresagens medlemmer. 15) Transaktionsmonitorering. 16) Videndeling i NFCERT. 17) Tilbageførsel af svindeltransaktioner. 18) Rådgivning af kunder.*
NCIK: *19) Facilitering af tværsektoriel videndeling og samarbejde i FIT. 20) Varsling om akut problemstilling til berørt aktør. 21) Viden- og erfaringsudveksling blandt politimyndigheder. 22) Oplysningskampagner.*,

Figur 14 tydeliggør at det undersøgte netværk, implementerer tiltag før, under og efter kriminaliteten udføres, og primære søger at gøre sårbare mål mere robuste eller øge beskytternes kompetencer til at afværge forsøg på vishing (og andre former for digital svindel). Det er kun bankernes tilbageførsel af svindeltransaktioner, som formodes at kunne mindske gerningspersonernes motivation for at begå ny kriminalitet. Udover at bankerne umiddelbart er de eneste aktører der implementerer forebyggelsestiltag rettet mod gerningspersoners motivation, er bankerne ligeledes de aktører der implementerer flest forskellige forebyggelsestiltag på tværs af udførelsesstadierne. NCIK er den eneste anden aktør, der også implementerer tiltag på tværs af alle stadierne, dog færre end bankerne. Fælles for hele netværket er, at alle aktørerne implementerer flest tiltag før og under svindelforsøget. Ud fra rutineaktivitetsteorien (Cohen & Felson, 1979) fokuserer den nuværende danske forebyggelse primært på at reducere forekomsten af vishing ved at ruste de sårbare mål eller styrke beskytternes (forebyggelsesaktørernes) kompetencer yderligere.

Da de kriminelle kan udnytte forskellige platforme til at initiere vishing, og derigennem anvende forskellige former for social engineering, er der adskillige former for dagligdags aktiviteter der kan udnyttes af de kriminelle. Der er således et utal af rutineaktiviteter hvor forebyggelsen kan implementeres, hvilket kræver at de relevante aktører i hver rutineaktivitet er bevidste om mulighedsskabende elementer for vishing og deres ansvar for at reducere disse.

Forebyggelsesarbejdet

Aktørerne udfører både intern og ekstern forebyggelsesarbejde, som varierer fra aktør til aktør. F.eks. implementerer bankerne tiltag, der sigter mod at forbedre opsporingen af mistænkelige overførsler, mens politiet fokuserer på videndeling og faciliterer samarbejde. Hver aktør udgør derfor sit eget netværk inden for det samlede forebyggelsesnetværk.

Den første analysedel har afdækket, at hver aktør kun ved præcis, hvad deres eget netværk bidrager med af forebyggelse og hvilke udfordringer de står overfor. På trods af de mange (overlappende) samarbejder på tværs af aktørerne, hvor der primært udveksles viden, har aktørerne ikke fuld indsigt i hinandens arbejde. Eksempelvis mener Sofie ikke, at forebyggelsen af vishing er begrænset af landegrænser, da TI kan identificere alle spoofede opkald, der modtages på telefoner i Danmark. Samtidig fortæller Jakob, at det kun er muligt for TI at identificere spoofede opkald til telefoner i Danmark, hvis opkaldet kommer fra udlandet[4]. Der er også aktører som cybersikkerhedseksperter, hvis fulde potentiale endnu ikke udnyttes i forebyggelsen. Dette skyldes enten, at de opfattes som en black box af de andre aktører eller at de endnu ikke har formået at etablere sig som mediator i forebyggelsesnetværket. Den begrænsede indsigt og misforståelser om hinandens arbejde udgør potentielle udfordringer for forebyggelsen. Det kan forvride opfattelsen af, hvordan forebyggelsen reelt fungerer som helhed og dets begrænsninger, hvilket i sidste ende kan fordreje opfattelsen af trusselsbilledet.

[4]*NCIK har inden specialets aflevering gjort opmærksom på, at de tekniske mekanismer er komplekse, og kan variere afhængigt af, om det spoofede opkald starter i Danmark eller udlandet. NCIK er derfor ikke enige i specialets fortolkning af, at Teleindustrien og NCIK har forskellige opfattelser af, hvornår et spoofet opkald kan identificeres.*

Udfordringer

Aktørerne påpeger selv, at deres opfattelse af trusselsbilledet udfordres yderligere af GDPR. Selvom TI, FD og bankerne deltager i diverse samarbejder og deler deres observationer af udviklingen af modus, påpeger de alle behovet for fremtidig datadeling, gerne i realtid. Den konstante udvikling af kriminalitetsformen og det grænseoverskridende, samt det digitale element ved vishing gør det vanskeligt for aktørerne at følge med og forhindre forekomsten. Muligheden for datadeling vil bl.a. kunne styrke bankernes monitorering, fordi det potentielt kan gøre dem i stand til at sammenholde en pauseret transaktion med geolokation på MitID og IP-adresse på enheden, vedkommende forsøger at logge ind på.

På trods af at der, som beskrevet i starten af delkonklusionen, allerede indgår et væld af aktører i forebyggelsesnetværket, er der generelt efterspørgsel på, at techgiganter som Meta, Google og lign. inddrages. I det nuværende netværk er der en opfattelse af, at techgiganterne ikke holdes ansvarlige for at forhindre delingen af materiale, der på falske præmisser får personer til at kontakte, hvad de fejlagtigt tror er en legitim service, myndighed eller lignende, men som i virkeligheden fører dem til en gerningsperson, der derefter udsætter dem for vishing. Forebyggelsesaktørerne håber således at den nye PSD3 og PSR, pålægger disse giganter noget ansvar for at være med til at stoppe spredningen gennem deres kanaler.

8.3 Delanalyse 2 - Forebyggelsesmekanismer

I denne delanalyse specificerer vi først Bjørgo's (2016) helhedsorienterede forebyggelses-model til vishing ved at analysere, hvilke forebyggelsesmekanismer de 22 identificerede tiltag fra delanalyse 1 aktiverer. Da aktørerne implementerer flere af de samme tiltag, opstilles denne del af analysen efter de overordnede grupperinger af tiltagene; borgerrettet information, teknologiske sikkerhedsforanstaltninger, videndeling og samarbejde i og på tværs af sektorer, facilitering af netværk for samarbejde og akut orientering af andre aktører. Efterfølgende undersøger vi, hvordan de igangsatte mekanismer kan styrkes og diskuterer mulighederne for at aktivere andre mekanismer.

8.3.1 Borgerrettet information

Den borgerrettede information dækker over oplysningskampagner, anbefalinger til bl.a. Ældresagen, informationsaftener for, og it-træning af, Ældresagens medlemmer, samt rådgivning af bankkunder.

Oplysningskampagner

Samtlige inddragede forebyggelsesaktører (på nær cybersikkerhedseksperten) laver oplysningskampagner om vishing. Som beskrevet adskillige gange i delanalyse 1, sigter kampagnerne mod at øge den danske befolknings bevidsthed om risikoen for at blive udsat for vishing og hvordan de kan undgå det. Formålet med kampagnerne er at styrke borgernes modstandskraft og dermed mindske de kriminelles muligheder for at udføre vellykkede vishingforsøg. Kampagnerne udløser dermed mekanismen, 'beskyttelse af sårbare mål', som kan hindre udførelsen af svindel og medføre mekanismen, 'afværgelse' (Bjørgo, 2016: 23+26). Jesper fra SN påpeger imidlertid, at kampagnerne kan have en kontraproduktiv effekt, idet de kriminelle kan anvende den offentligt tilgængelige information til at forbedre deres svindelmetoder, hvilket potentielt kan underminere forebyggelsesindsatsen (Bilag 6: 9). Derudover kan en aktørs kampagne forskyde problemet (Bjørgo, 2016: 27) ved f.eks. at advare om, at et bestemt domænenavn anvendes til vishing, fordi det ligeledes advarer de kriminelle, som kan skifte til et andet domænenavn, og dermed rykke problemet til en ny aktør.

De samme mekanismer aktiveres ved anbefalinger, informationsaftener og it-træning for medlemmer af Ældresagen. Disse tiltag fokuserer specifikt på ældre borgere og leverer primært kampagnebudskaber gennem fysiske møder. Det kan eliminere risikoen for den kontraproduktive effekt af, at de kriminelle får indsigt i forebyggelsen og kan modarbejde den.

Rådgivning af bankkunder

Tiltaget dækker, som tidligere beskrevet, over at bankerne ringer deres kunder op, og rådgiver om hvordan kunden skal forholde sig, hvis banken mistænker at vedkommende er ved at blive eller er blevet udsat for svindel. Derudover gør de kunden opmærksom på risikoen for at blive udsat for ny svindel. I de tilfælde, hvor banken når at kontakte kunden inden transaktionen gennemføres, er dette tiltag med til at afværge kriminaliteten. Uanset om banken når at stoppe transaktionen eller ej, gør rådgiveren kunden opmærksom på risikoen for ny svindel. Herved

er tiltaget med til at beskytte sårbare mål, her er det dog mod gentagen viktimisering. Anmeldelserne bør ideelt set fordre efterforskning samt retsforfølgelse, hvilket kan udløse reaktiv uskadeliggørelse i form af straf, som kan reducere gevinsten ved den kriminelle handling og føre til individualpræventiv afskrækkelse (Bjørgo, 2016: 21+24-25+29-30). Idet vi fra NCIKs statistikker og henlæggelsesdata, som beskrevet i afsnit 2, kan se, at mange sager henlægges og at få sager fører til domfældelser, vil vi dog argumentere for at disse mekanismer ikke aktiveres af dette tiltag.

8.3.2 Teknologiske sikkerhedsforanstaltninger

De teknologiske sikkerhedsforanstaltninger omfatter TIs spoofingbeskyttelse på virksomheders afsender-ID på SMS, spoofingbeskyttelse af banker, politi og myndigheders fastnettelefonnumre, blokering af farlige links, FDs reducering af den daglige beløbsgrænse på overførsler og implementeringen af MitID, samt bankernes transaktionsmonitorering og tilbageførsel af svindeltransaktioner.

Spoofingbeskyttelser, blokering af links, samt transaktionsmonitorering er tiltag, der har til formål at opspore forsøg på svindel, hvilket er med til at afværge nogle af de kriminelle handlinger. Tofaktor-godkendelsen på MitID bidrager til at forhindre svindel ved at gøre det sværere for gerningspersoner at misbruge forurettedes oplysninger, som de ellers kunne bruge til at autorisere overførsler o.l. Selvom disse tiltag afværger nogle af svindelforsøgene, er det udfordrende for aktørerne at afværge alt, når gerningspersonerne får forurettede til selv at autorisere overførslen, idet gerningspersonerne herved kan omgå sikkerhedsforanstaltningerne.

Beløbsgrænsen på daglige overførsler og tilbageførsel af svindeltransaktioner er begge tiltag, der begrænser beløbsstørrelsen, der kan gå igennem sikkerhedsforanstaltningerne inden banken eller kunden selv bliver opmærksom på svindlen. Tiltagene er medvirkende til at 'reducere skadevirkninger' ved den kriminelle handling, samt 'reducere gevinsten' for gerningspersonen (Bjørgo, 2016: 28-30).

8.3.3 Videndeling og samarbejde i og på tværs af sektorer

I delanalyse 1 er det tydeliggjort at alle aktørernes samarbejder i netværket mod vishing, i høj grad består af gensidig videndeling om aktuelle trusselsbilleder og modi. Videndeling anvendes

til enten at forbedre de teknologiske sikkerhedsforanstaltninger eller orientere borgere om risici. Da videndelingen er med til at styrke aktørernes teknologiske sikkerhedsforanstaltninger, bidrager videndelingen til afværgelsen af vishing, som kan medføre reducering af skadevirkningerne og de kriminelles gevinster. Videndelingen der anvendes til at orientere borgere om risici er, som tidligere beskrevet, med til at beskytte sårbare mål.

NCIKs og FDs facilitering af de afgrænsede forebyggelsesfora, FIT og Svindel Task Forcen, er med til at aktivere de samme mekanismer. Udover videndeling, udarbejder de bl.a. nye teknologiske sikkerhedsforanstaltninger, som f.eks. reduceringen af den daglige beløbsgrænse, der er resultat af Svindel Task Forcen.

8.3.4 Akut orientering af andre aktører

Udover at deltage i den generelle videndeling blandt aktørerne, foretager bankerne og NCIK akutte orienteringer til andre aktører. I forbindelse med transaktionsmonitorering kan bankerne, i samarbejde, bremse udbetalinger af overførsler imens/umiddelbart efter svindlen finder sted (Bilag 6: 14). NCIK orienterer andre aktører, når de identificerer, at deres domæne udnyttes til at initiere svindel. Derudover hjælper NCIK den interne efterforskning ved at underrette om aktuelle trusler. Den akutte orientering er med til at afværge vishing og derigennem beskytte sårbare mål. Den interne orientering til politiets efterforskning, kan yderligere medføre både proaktiv og reaktiv uskadeliggørelse, hvis det leder til identificering af en eller flere gerningspersoner (Bjørgo, 2016: 24-25).

Opsummering af forebyggelsesmekanismer

De aktuelle tiltag i det identificerede netværk aktiverer primært mekanismerne 'Afværgelse' og ‘Beskyttelse af sårbare mål’, som kan medføre mekanismerne, ‘Uskadeliggørelse’, ‘Reducering af skadevirkninger’ og ‘Reducering af gevinster ved kriminelle handlinger’. Det aktuelle netværk mod vishing aktiverer således fem ud af ni forebyggelsesmekanismer i Bjørgo’s (2016) helhedsorienterede forebyggelsesmodel. Nedenstående tabel visualiserer fordelingen af de aktiverede mekanismer, og dermed også hvilke der ikke aktiveres. Tiltag fremgår i sort skrift ved den mekanisme, tiltaget primært aktiverer. Den grønne skrift indikerer hvilke andre mekanismer, de primært aktiverede mekanismer kan medføre. Tabellen er opstillet efter Bjørgo’s (Ibid.: 15) tre kronologiske grupperinger af mekanismer: 1) Mekanismer der

søger at forebygge at kriminelle handlinger sker, 2) Mekanismer ved kriminelle handlinger, der allerede er sket og 3) Mekanismer, der søger at forebygge at kriminelle handlinger gentages. Med denne opstilling gentages mekanismerne 'Uskadeliggørelse' og 'Afskrækkelse' i grupperingerne, da der skelnes mellem proaktiv og reaktiv uskadeliggørelse, samt generel- og individualpræventiv afskrækkelse.

Tabel 9: *Aktiverede forebyggelsesmekanismer*

Mekanismer	**Tiltag**	**Aktører**
Mekanismer der søger at forebygge at kriminelle handlinger sker		
Opbygge moralske barrierer mod at begå kriminelle handlinger		
Reducere rekruttering til kriminelle sociale miljøer og aktiviteter		
Afskrækkelse ved trussel om straf (Generalpræventiv)		
Uskadeliggørelse ved at fratage gerningspersoner evnen til at begå lovbrud (Proaktiv)	Akut orientering	
Afværgelse af kriminalitet ved at opdage og standse handlinger før de sker	Teknologiske sikkerhedsforanstaltninger Videndeling Akut orientering Borgerrettet information	TI, FD og banker Alle Politi og banker
Beskytte sårbare mål	Borgerrettet information Teknologiske sikkerhedsforanstaltninger Videndeling Akut orientering	Alle (minus cybereksperter)
Mekanismer ved kriminelle handlinger, der allerede er sket		
Uskadeliggørelse ved at fratage gerningspersoner evnen til at begå lovbrud (Reaktiv)	Akut orientering	
Reducere skadevirkninger	Teknologiske sikkerhedsforanstaltninger Videndeling	
Mekanismer, der søger at forebygge at kriminelle handlinger gentages		
Afskrækkelse ved trussel om straf (Individualpræventiv)		
Uskadeligegørelse ved at fratage gerningspersoner evnen til at begå lovbrud (Proaktiv)		
Reducere gevinster ved kriminelle handlinger	Teknologiske sikkerhedsforanstaltninger Videndeling	
Afholdenhed og rehabilitering		

Tabellen viser, som det ligeledes er påvist i delanalyse 1, at det nuværende netværk forsøger at eliminere forekomsten af vishing ved primært at styrke de kompetente beskyttere og ruste de

sårbare mål (Cohen & Felson, 1979). De tiltag, der kan udløse reaktiv uskadeliggørelse, reducering af gevinster og individualpræventiv afskrækkelse, er udfordret af at vishing er en grænseløs kriminalitetsform, der udføres gennem manipulation. Tilsammen udfordrer disse to elementer efterforskningen i en sådan grad, at der i den nuværende danske forebyggelse af vishing, må konkluderes at være utilstrækkelige muligheder for at forebygge gerningspersonernes motivation.

8.3.5 Muligheder for at styrke forebyggelsen

Vishing kan udføres på utallige måder, hvorfor den største udfordring, vi indtil videre har identificeret, er at fratage gerningspersonerne evnen til at udføre vishing. Med få domfældelser er der få eksempler, der kan have en generalpræventiv effekt og vishing kan derfor fremstå som en risikofri kriminalitetsform pga. den lave opdagelsesrisiko. Med det lave antal domfældelser er det ikke muligt at afdække, hvorvidt det pågældende strafniveau har en individualpræventiv effekt. I det afsluttende afsnit undersøger vi, hvilke indsatsområder aktørerne peger på, potentielt kan styrke forebyggelsen yderligere.

Led i kæden

I den nuværende forebyggelse oplever aktørerne at de primært har mulighed for at implementere tiltag, der styrker borgernes robusthed før vishingforsøget, eller styrke andre aktørers kompetencer til at opspore kriminelle handlinger som de sker, eller reducere skadevirkningerne heraf. Aktørerne nævner, at vishing blot er ét led i den samlede 'kæde' af handlinger fra planlægning til domfældelse og peger på forskellige indsatsområder i kæden, hvor det er muligt at styrke forebyggelsen. Det næste led i kæden, efter vishing, er hvidvask af det tilegnede beløb, som Niels, Torben og Jakob mener er et muligt indsatsområde, der kan styrke den nuværende forebyggelse mod vishing (Bilag 7: 21; Bilag 5: 35; Bilag 4: 39). Jens og Lene, peger i stedet på, at det vil styrke forebyggelsen at kigge på det sidste led, nemlig politiets efterforskningsmuligheder (Bilag 3: 26-27; Bilag 9: 17-18).

Hvidvask

Jakob, Jesper og Torben nævner at de i deres respektive arbejder, observerer indikationer på at kriminaliteten er organiseret (Bilag 5: 3; Bilag 6: 19; Bilag 4: 39). Det understøttes af de enkelte domfældelser, hvor f.eks. en gruppe på fire personer er blevet dømt for, i forening, at udsætte

455 personer for forsøg på vishing (Østjyllands Politi, 2023). Desuden nævner Sofie, at de i NCIK ofte oplever, at vishingforsøgene udspringer af organiserede grupper (Bilag 8: 25). Det der, i Sofies optik, adskiller vishing fra andre typer af it-relateret økonomisk kriminalitet, er den direkte mundtlige kommunikation mellem gerningsperson og forurettede. Det gør i nogen grad udførelsen af vishing afhængig af dansktalende personer, som både kan befinde sig i Danmark, eller rekrutteres til at sidde og arbejde fra udlandet (Bilag 8: 29). Ifølge Lene kan de rekrutterede danskere betegnes som muldyr:

> *"I gamle dage ville man kalde dem muldyr, hvis de havde en eller anden fordækt rolle og måske fik penge ind på deres egen konto. Men det her kunne jo godt være nogen, som tror, at de bare er ansat af et stort firma i udlandet*" (Bilag 9: 12)

Netop anvendelsen af muldyr, er noget som primært Niels, Torben og Jakob ser som særligt udfordrende for forebyggelsen. Som beskrevet i delanalyse 1, indhenter bankerne viden fra deres filialer. Niels ved fra DBs filialer i Nordirland, at der derovre er kommet større politisk fokus på forbrugerbeskyttelse, som medfører at bankerne kommer til at hæfte for en større andel af de svindlede beløb. Det er dog både afsendende og modtagende bank, der skal hæfte for tabet, hvilket, ifølge Niels, tyder på at muldyrsproblematikken anerkendes som en reel problemstilling (Bilag 7: 20-21). Torben ser den samme udvikling i UK, og nævner at der, udover at blive sat fokus på begge ender i en transaktion, ligeledes fokuseres på at ansvarliggøre de platforme, som udnyttes til at sprede svindlen (Bilag 5: 21+24). Derudover mener han, at det danske politis målrettede aktion overfor muldyr i januar 2023 var en succes (Bilag 5: 21). Aktionen gik ud på at 600 politifolk på samme tidspunkt tog ud og anholdte 150 mistænkte muldyr på tværs af landet, som havde, *"... ringet til personer, udgivet sig for at være fra politiet og fortalt dem, at deres bankkonto enten var ved at blive hacket, eller at der var optaget lån i deres navne*" (Ritzau, 2023). Jakob, Niels og Torben er enige om, at det vil kunne styrke forebyggelsen, hvis der sættes ind over for muldyrene. Som Jakob beskriver det; "*...det her [vishing] ville jo ikke kunne lade sig gøre, hvis du ikke havde muldyrene*" (Bilag 4: 39). Det tyder på, at fortalerne for denne løsning, vurderer at hvis der efterforskningsmæssigt sættes ind på at finde og uskadeliggøre muldyr, vil vishing kunne afværges og føre til en moralsk afvejning af fordele og ulemper ved de kriminelle handlinger. Der er dog andre aktører, som mener det er en uhensigtsmæssig løsning. Jesper fortæller f.eks. at idet kriminalitetsformen er grænseløs, kan de organiserede bagmænd blot rekruttere danske muldyr til udlandet i stedet, og så vil efterforskningen fortsat være udfordret (Bilag 6: 14). Jens og Lene bemærker

yderligere, at selv hvis nogle muldyr bliver uskadeliggjort, vil det ikke føre til bagmændene, da kriminaliteten er struktureret på en måde, hvor de der er nederst i hierarkiet ikke kan afsløre bagmændene, fordi de ikke har adgang til væsentlig information (Bilag 3: 24-25; Bilag 9: 12).

Politiets ressourcer

Ifølge Jens og Lene vil det styrke forebyggelsen, hvis der allokeres flere ressourcer til politiets efterforskning af digital svindel. Ifølge Jens kræver effektiv efterforskning af disse sager meget 'gravearbejde', og han understreger, at det er nødvendigt at prioritere politisk; "*...fordi ellers så kommer vi til det der politiløse, retsløse samfund og det kan vi ikke leve med* (Bilag 3: 27). Den nuværende lave opdagelsesrisiko kan, ifølge Jens, føre til mistillid i samfundet, hvor det bliver vanskeligt at skelne mellem ægte og falske identiteter. Øgede ressourcer i form af cybersikkerhedskompetencer, vil i Jens' optik øge muligheden for at retsforfølge, og dermed uskadeliggøre, flere gerningspersoner, hvilket potentielt kan afskrække både individual- og generelpræventivt og derigennem styrke de moralske barrierer mod at begå disse former for kriminalitet.

Andre aktører argumenterer for, at forebyggelsen af vishing kan forbedres ved at intervenere tidligere i kæden end politiets efterforskning, hvilket potentielt kan reducere behovet for at øge politiets ressourcer. I den forbindelse påpeger Torben, at selvom han mener at det er vigtigt at øge politiets ressourcer, mener han ikke at det i sig selv er nok og fremhæver at:

> "*... politiet er jo først på til sidst i kæden [...] når svindlen er sket. Det er selvfølgelig sådan for vores allesammens retfærdighedsfølelse, at når der er nogen, der har gjort noget kriminelt, og så bliver taget i det, så skal de jo også gerne dømmes hurtigt, i stedet for at de går rundt på gaden"* (Bilag 5: 35).

Det er således, i Torbens optik, vigtigt, at forebyggelsen er proaktiv og prioriterer at afværge kriminaliteten. Han fremhæver, at politiets muligheder for efterforskning er vigtig for de forurettedes retfærdighedsfølelse, men ved at anlægge en mere proaktiv forebyggelse, vil den kriminelle handling kunne afværges. Andre aktører mener at en prioritering af politiets ressourcer kan have en afskrækkende effekt, der potentielt medfører en mindre forekomst af vishing. Som Lene beskriver det, er diskussionen om, hvor i kæden det vil være mest effektivt at styrke forebyggelsen; "*... sådan lidt om det er hønen eller ægget"* (Bilag 9: 17). Det tyder

således på, at alle aktørerne er enige om, at der kan gøres noget for at styrke forebyggelsen yderligere, omend det er proaktivt eller ift. at øge politiets ressourcer.

Datadeling

Alle informanter er enige om, at det, der udgør den største udfordring for deres forebyggelses-arbejde, er den begrænsede mulighed for datadeling:

> "*Der er ingen tvivl om at datadeling og udveksling af oplysninger, også på tværs af nogen, der godt kunne være private aktører også, er da noget som kan have en positiv effekt ift. at minimere it-kriminalitet. [...] det går så superhurtigt med it-kriminalitet, så hvis ikke at man på et tidspunkt måske også begynder at dæmme lidt op for, hvordan man må udveksle oplysninger imellem dem, der forsøger at bekæmpe det, så bliver det rigtig svært at kunne følge med det. Det er det som udgangspunkt allerede*" (Bilag 8: 24-25).

Flere af forebyggelsesaktørerne mod vishing, inspireres af forebyggelsen på hvidvaskområdet. FDs Svindel Task Force er f.eks. inspireret af deres tidligere Hvidvask Task Force. Derudover er der, som beskrevet i afsnit 2, lavet en tilføjelse i retsplejeloven, der gør det muligt for aktører i forebyggelsen af hvidvask- og terrorfinansiering at dele fortrolige oplysninger (Justitsministeriet, 2021). Ifølge Lene og Sofie vil det kun være muligt at implementere en lignende tilføjelse for svindelområdet, hvis der laves mere afgrænsede forebyggelsesnetværker, som ODIN netværket (Bilag 9: 17; Bilag 8: 24). ODIN netværket består af færre aktører i et specifikt forum, hvorimod de afgrænsede netværk for forebyggelse mod digital svindel, som f.eks. FIT er meget store. *"... der er det selvfølgelig nemmere at gå ind og dele data på et super afgrænset område. Og det er i sidste ende en politisk beslutning, da der i de fleste tilfælde er behov for at justere lovgivningen, hvis vi skal kunne dele data på den mest optimale måde ift. at forebygge og bekæmpe it-kriminalitet"* (Bilag 8: 25). Det er således essentielt, at der kommer en større politisk bevågenhed på digital svindel, hvis forebyggelsesaktørerne skal have mulighed for at dele flere (personhenførbare) data med hinanden i fremtiden.

Alle de inddragede aktører udtrykker et ønske om at kunne dele mere data med hinanden og særligt aktørerne fra finanssektoren understreger behovet for indsigt i data om specifikke personer og enheder i realtid. Det vil styrke bankernes monitorering og muligheden for at

advare andre om specifikke konti og personer, de identificerer som involveret i svindeloverførsler: "*vi ser måske nogle ting tidligere end politiet gør. [...] Hvordan kan man være med til også at dele viden omkring, er der noget sammenfald? Altså som man ikke ser det på sag for sag"* (Bilag 7: 3). Lene pointerer yderligere, at ønsket om at dele personhenførbare data, egentlig er et ønske om at dele oplysninger om 'skurke': *"... det er jo det vi har politiet til, så må man anmelde det, og så må politiet ligesom lave deres straffesager. Det er jo en eller anden form for privat efterforskning, at man sætter folk i registre"* (Bilag 9: 15). Bankerne påtager sig således et stort ansvar for forebyggelse af vishing, hvilket kan hænge sammen med, at det lige nu kun er bankerne og de forurettede, der hæfter for tabet af det. Det kan ligeledes fordre deres ønske om bedre muligheder for at dele viden om gerningspersonerne, så vishing kan afværges.

Som beskrevet i delanalyse 1, er bankerne de aktører, der implementerer flest forebyggelsestiltag før, under og efter svindelforsøgene. Det rejser spørgsmålet om, hvorvidt bankerne i den nuværende forebyggelse har påtaget sig en patruljerende rolle, fordi det er for udfordrende for politiet at efterforske, efter svindlen er udført.

8.4 Delkonklusion 2

De identificerede tiltag i det nuværende forebyggelsesnetværk fokuserer primært på at afværge vishingforsøg og beskytte sårbare mål, hvilket kan reducere skadevirkninger for de forurettede og minimere gerningspersonernes gevinster. Politiets interne videndeling kan yderligere styrke efterforskningsarbejdet og derfor kan den nuværende forebyggelse mod vishing aktivere fem ud af ni forebyggelsesmekanismer i Bjørgo's (2016) helhedsorienterede forebyggelsesmodel. De forebyggelsestiltag, der burde kunne udløse de fire resterende mekanismer, er udfordret af, at vishing er en grænseløs kriminalitetsform, som udføres af at de forurettede manipuleres til selv at autorisere betalinger. Disse faktorer gør efterforskningen særdeles vanskelig, hvilket fører til lave antal domfældelser.

Aktørerne ser muligheder for at styrke forebyggelsen i forskellige 'led i kæden' af vishing. Ifølge Niels, Torben og Jakob kan forebyggelsen styrkes ved at flere muldyr strafforfølges, da de mener det vil besværliggøre legitimering af de svindlede beløb, som formodentlig vil mindske gerningspersonernes motivationen for at udføre vishing. Jens og Lene peger på, at politisk prioritering af cyberkompetente ressourcer til politiet kan styrke forebyggelsen. Alle aktører er enige om, at de nuværende tiltag kan styrkes gennem øgede muligheder for

datadeling i netværket. Samtidig er efterspørgslen på datadeling en understregning af, at den nuværende forebyggelse er uligevægtig fordelt, fordi politiet netop mangler efterforskningsmæssige ressourcer, som muligvis overlader et større ansvar til bankerne.

9. Refleksionsafsnit

I dette afsnit vil vi nuancere besvarelsen af problemformuleringen ved at reflektere over udvalgte fund fra analysen. Først berører vi ansvarsfordelingen i den nuværende forebyggelse af vishing og et potentielt behov for en øget politisk prioritering af politiets ressourcer. Dernæst præsenteres vores observationer af anvendelsen af oplysningskampagner. Afslutningsvis reflekterer vi over de potentielle udfordringer ved implementeringen af EU-direktiverne PSD3 og PSR.

Gennem analysen er det blevet tydeligt, at bankerne ikke blot implementerer flest tiltag i forebyggelsen, men ligeledes er de eneste aktører, udover politiet, der implementerer tiltag før, under og efter vishing udføres. Dette understreger ansvarsfordelingen i netværket, og bankernes ønske om, at flere aktører, såsom techgiganter, gøres ansvarlige for at stoppe spredningen af svindelforsøg. Informanterne fra finanssektoren har under interviewene fortalt, at de har et godt 'efterretningsbillede' (Bilag 5: 16) og nogle gange ser kriminalitetsudviklinger 'inden politiet' (Bilag 7: 3), samt ønsker at få bedre muligheder for datadeling, så de f.eks. kan sammenholde informationer om IP-adresser, telefoner, simkort, geolokation, log-in osv. for at 'få lukket ned for svindlen' (Bilag 6: 25). Udover at bankerne vil beskytte deres kunder, handler ønsket om øgede muligheder for datadeling om, at de er de eneste, foruden forurettede, der kan komme til at hæfte for det økonomiske tab. I og med at det kun er et fåtal af anmeldelserne om vishing, der fører til domfældelse, er bankerne interesserede i at kunne følge ind- og udenlandske transaktionerne i realtid, så de kan få stoppet udbetaling i modtagerbanken og føre beløbet tilbage til den respektive kunde, hvilket de kun lykkedes med i ca. 1/10 af sagerne (Bilag 6: 14).

Finanssektors-informanternes udtalelser antyder, at bankerne, udover den forebyggende rolle, påtager sig en patruljerende rolle i den nuværende forebyggelse, fordi kriminaliteten, qua det digitale, og heraf grænseløse, element, udfordrer politiets efterforskning. Flere af vores informanter påpeger, at politiets efterforskningsmæssige udfordringer kan tilskrives, at politiet mangler ressourcer med ekspertise inden for cybersikkerhed. Da politiet er en politisk styret organisation, kan en nøglefaktor i at styrke forebyggelsen yderligere, være at politiets cyberkompetente ressourcer til bekæmpelse af digital svindel, prioriteres højere på den politiske dagsorden. En styrkelse af disse ressourcer vil potentielt kunne føre til, at flere anmeldelser kan retsforfølges og føre til flere domfældelser, hvilket vi i analysen argumenterer

for potentielt vil kunne have en afskrækkende effekt, og aktivere flere mekanismerne i Bjørgo's (2016) helhedsorienterede forebyggelsesmodel.

Vigtigheden af en øget politisk prioritering af politiets ressourcer forstærkes desuden i lyset af PSD3 og PSR. I og med disse udgør et EU-direktiv og regulativ, som skal implementeres i EU-medlemslandene, indgår disse dokumenter som internationale aktører i forebyggelses-netværket. Gennem ANT-analysen er det blevet tydeligt, at aktørerne i en dansk kontekst samarbejder med adskillige internationale aktører for at styrke den nationale forebyggelse. Dette har ført til refleksioner over, hvordan den endelige version af direktivet og regulativet vil påvirke den danske forebyggelse af vishing i fremtiden. PSD3 og PSR lægger op til at forbedre open banking-princippet, så der skabes en mere gnidningsfri brugeroplevelse af betalinger, på tværs af tredjeparter og europæiske landegrænser. Som Jesper fra SN påpeger, kan det udfordre bankernes evner til at bremse svindelforsøgene, fordi bankernes 'patruljering' i høj grad vil blive afhængig af samarbejde med udenlandske banker om at få overførsler stoppet og tilbageført (Bilag 6: 14). Med afsæt i rutineaktivitetsteorien kan der argumenteres for at forbedrede, gnidningsfrie brugeroplevelser på tværs af tredjeparter, potentielt kan skabe nye aktiviteter, som kan implementeres i de kriminelles social engineering strategier og dermed udvikle mulighederne for at udføre vishing. Det vil potentielt kunne udfordre politiets efterforskning yderligere, fordi Danmark med retsforbeholdet står uden for dele af det europæiske politisamarbejde (Heron, 2024). Danmark har en operationel samarbejdsaftale, hvilket betyder at dansk politi skal have en retskendelse fra de danske domstole, samt en retshjælpsanmodning fra Justitsministeriet, for at kunne anmode en anden europæisk domstol om hjælp til at efterforske en sag. Som beskrevet i afsnit 2, kræver det at efterforskningsmulighederne står i rimeligt forhold til alvorsgraden af forbrydelsen og det forventede udfald ved en eventuelt straffesag (Retsudvalget, 2022: 5). Da den endelige version af PSD3 og PSR endnu ikke er trådt i kraft, er der fortsat mulighed for at finanssektorens ønske om at ansvarliggøre techgiganterne for spredningen af svindelforsøg efterkommes, så forebyggelsesnetværkets fælles kompetencer for at reducere forekomsten af svindelforsøg styrkes.

Som pointeret i analysen, fokuserer den nuværende forebyggelse i høj grad på at beskytte sårbare mål gennem oplysningskampagner, der har til formål at gøre borgerne opmærksomme på, hvordan de kan beskytte sig selv mod svindelforsøg. Selvom kampagner fremhæves som et godt tiltag af samtlige aktører, har de ligeledes en bevidsthed om, at effekten af dem er

kortvarig. Med afsæt i vores informanters udtalelser, virker det dog ikke til at have betydning for den fremtidige brug af kampagner, idet samtlige aktører påpeger, at det er nødvendigt at lave oplysning, for at øge borgernes modstandsdygtighed. Undervejs i udformningen af specialet har vi desuden oplevet, at indsatsen med at implementere kampagner er intensiveret. Selvom litteraturen på området er sparsom, er det, med afsæt i Cross & Kellys (2016) studie muligt at argumentere for, at kampagnerne ikke nødvendigvis gør borgerne mere modstandsdygtige over for svindelforsøg, fordi kampagnerne ofte har en stor detaljegrad, der kan gøre det svært for borgerne at anvende viden derfra, når de udsættes for svindelforsøg, jf. afsnit 4.3. Eksempelvis er budskaberne i FDs kampagne 'Sikker bank - sammen' (Finans Danmark, n.d. *c*), korte, men indeholder informationer om forskellige svindeltyper, hvorfor kampagnen, med afsæt i Cross & Kellys (2016) studie, kan have en lav forebyggende effekt. Kampagnerne kan derudover have en kontraproduktiv effekt i form af at oplyse gerningspersonerne om, hvordan de skal tilpasse deres strategier. I forlængelse heraf vil den endelige implementering af PSD3 og PSR ligeledes kunne skabe brugbar viden for de kriminelle om, hvilke betalingstjenester, der kan være rentable for dem at anvende. Eksempelvis er e-wallets som ApplePay endnu ikke fuldt omfattet af direktivet og kan således potentielt anses som mulighedsskabende for de kriminelle handlinger.

Der er endnu mange usikkerheder ift. den endelige version af direktivet, og det forventes først endeligt implementeret i medlemslandene i løbet af 2026 (Nordea, 2024). Selvom en dansk politisk prioritering af politiets ressourcer ligeledes må formodes at tage lang tid at implementere, vil vi argumentere for, at det vil være fordelagtigt for forebyggelsen. Vi antager at det potentielt kan styrke det samlede forebyggelsesnetværk og dermed forhindre, at vishing bliver en risikofri kriminalitetsform, der vil kunne udgøre et decideret samfundsproblem.

10. Konklusion

Specialet belyser, *hvordan der aktuelt forebygges mod digital svindel, hvor vishing indgår som kontaktmodus i en dansk kontekst, og hvilke muligheder der kan være for at styrke forebyggelsen yderligere.* Ved at anvende Aktør Netværk Teori til at kortlægge det nuværende forebyggelsesnetværk, har vi afdækket et komplekst og mangfoldigt netværk af aktører, som kontinuerligt udvides. Den kontinuerlige udvikling af forebyggelsesnetværket skyldes, at vishing er en form for social engineering, der kan kombineres med andre social engineering strategier såsom smishing, phishing, spoofing og falske fortællinger. De kriminelle kan således udgive sig for at være nærmest hvilken som helst organisation, myndighed eller virksomhed, hvilket medfører at kriminaliteten konstant kan ændres. Det egentlige forebyggelsesnetværk kan således omfatte alle aktører, hvis domæner og/eller navne kan anvendes til at opbygge en falsk fortælling for at bedrage enkeltpersoner. I denne undersøgelse har vi foretaget syv ekspertinterviews med hhv. en professor i cybersikkerhed fra Aalborg Universitet, direktøren for Teleindustrien, kontorchefen for Finans Danmarks digitaliseringsafdeling, tre fraud specialister fra hhv. Spar Nord og Danske Bank, en medarbejder fra NCIK, der er tovholder på FIT-samarbejdet og en lektor i jura fra Aalborg Universitet, der forsker i cybercrime. Disse eksperter danner, sammen med diverse dokumenter, det empiriske grundlag for undersøgelsen og repræsenterer de centrale (menneskelige og ikke-menneskelige) aktører i forebyggelses-netværket. Gennem analysen af de centrale aktørers forebyggelsestiltag har vi identificeret, at netværket implementerer 22 forebyggelsestiltag før, under og efter vishing udføres. Tiltagene kan grupperes i fem kategorier; borgerrettet information, videndeling og samarbejde i og på tværs af sektorer, teknologiske sikkerhedsforanstaltninger, akut orientering af andre aktører og facilitering af netværk for samarbejde. Ud fra rutineaktivitetsteorien sigter størstedelen af tiltagene mod at beskytte sårbare mål ved at gøre borgerne opmærksomme på risici for at blive udsat for svindel, og hvordan de kan undgå dette. Dette gøres primært gennem oplysningskampagner. Ydermere sigter en stor andel af aktørernes tiltag mod at styrke egne og andre forebyggelsesaktørers kompetencer til at afværge svindelforsøg, gennem implementering af teknologiske sikkerhedsforanstaltninger og videndeling.

Ud fra Bjørgo's helhedsorienterede forebyggelsesmodel, formår det nuværende forebyggelses-netværk, at igangsætte mekanismer, der afværger svindelforsøg og beskytter sårbare mål. Dette kan medføre uskadeliggørelse af kriminelle samt reducere skadevirkninger og de kriminelles gevinster. Antallet af domfældelser på området er dog meget lavt ift. det stigende antal

anmeldelser. Efterforskningen udfordres af kriminalitetens geografiske grænseløshed og teknologiske udførelse, der gør det svært for politiet at opspore gerningspersonerne. Vi konkluderer derfor at det nuværende opklaringsniveau af vishingsager kan få de kriminelle handlinger til at fremstå relativt risikofrie og efterlader forebyggelsesnetværket ude af stand til at have en afskrækkende effekt, hvilket lægger et stort ansvar på aktørernes evner til at afværge svindelforsøg mens de udføres. Aktørerne mener selv, at disse evner kan styrkes yderligere, gennem bedre muligheder for at dele data på tværs af netværket, der kan afdække legitimiteten af en pengeoverførsel eller kontanthævning. Det vil dog kræve, at der etableres mere afgrænsede samarbejdsgrupper, som kan få lovhjemmel til at dele data med hinanden, eller at der søges om lov til specifikke datadelinger hos Datatilsynet. Aktørerne fremhæver ligeledes et behov for at inddrage flere relevante aktører i netværket, i form af techgiganter, og pålægge dem et medansvar for at stoppe spredningen af svindelforsøg på deres domæner. Desuden peger aktørerne på, at øget politisk prioritering af politiets efterforskningsmæssige ressourcer, formodes at kunne føre til flere domfældelser. Det kan potentielt aktivere flere af Bjørgo's opstillede forebyggelsesmekanismer, som netop afskrækkelse, der kan påvirke de kriminelles afvejning af fordele og ulemper ved de kriminelle handlinger, og dermed opbygge moralske barrierer hos de kriminelle mod at begå disse handlinger.

Litteraturliste

Abildgaard, M., Jensen, L. L., Sarbo, M. I., Lilleholt, L. C., & Rubin, M. (23. juni 2023). *Rigsrevisionens beretning afgivet til Folketinget med Statsrevisorernes bemærkninger Politiets efterforskning af digitale seksualforbrydelser og økonomisk it-kriminalitet.* Hentet 12. marts 2024 fra Folketinget Statsrevisorerne & Folketinget Rigsrevisionen: Rigsrevisionens beretning

Armstrong, M. E., Jones, K. S., & Siami Namin, A. (2023). How Perceptions of Caller Honesty Vary During Vishing Attacks That Include Highly Sensitive or Seemingly Innocuous Requests. *HUMAN FACTORS, 62*(2), pp. 275-287. DOI:10.1177/00187208211012818

Ashfaq, S., Chandre, P., Pathan, S., Mande, U., Nimbalkar, M., & Mahalle, P. (2024). Defending Against Vishing Attacks: A Comprehensive Review for Prevention and Mitigation Techniques. *Cyber Security and Digital Forensics, 896*, pp. 411-422. DOI:0.1007/978-981-99-9811-1_33

Bengtsson, T. T., & Mølholt, A.-K. (2020). Anonymisering i kvalitative undersøgelser. I K. K. Petersen, & L. Ladefoged, *Forskning med børn og unge : etik og etiske dilemmaer* (1. udgave, s. 193-209). Hans Reitzel.

Bjørgo, T. (2016). Introduction: A Comprehensive Model for Preventing Crime. In T. Bjørgo, *Preventing Crime A Holistic Approach* (pp. 1-35). Palgrave Macmillan.

Bjørnholt, B., & Jakobsen, M. L. (2020). Kvalitativ analyse: kodning. I K. M. Hansen, L. B. Andersen, & S. W. Hansen, *Metoder i statskundskab* (3. udgave, s. 212-227). Hans Reitzel.

Brewer, R., de Vel-Palumbo, M., Hutchings, A., Holt, T., Goldsmith, A., & Maimon, D. (2019). Designing and Evaluating Crime Prevention Solutions for the Digital Age. In R. Brewer, M. de Vel-Palumbo, A. Hutchings, T. Holt, A. Goldsmith, & D. Maimon, *Cybercrime Prevention Theory and Applications* (1st edition pp. 125-146). Springer International Publishing. DOI:10.1007/978-3-030-31069-1

Center for Cybersikkerhed. (n.d.). *Center for Cybersikkerhed*. Hentet 11. Maj 2024 fra cfcs.dk: CFCS

Choi, K., Lee, J.-l., & Chun, Y.-t. (2016). Voice phishing fraud and its modus operandi. *Security Journal, 30*(2), pp. 454-466. DOI:10.1057/sj.2014.49

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *Approach. American Sociological Review, 44*(4), pp. 588-608. DOI:10.2307/2094589

Cross, C. (2015). No laughing matter: Blaming the victim of online fraud. *International Review of Victimology, 21*(2), pp. 187-204. DOI:10.1177/0269758015571471

Cross, C. (2016). Using financial intelligence to target online fraud victimisation: applying a tertiary prevention perspective. *Criminal Justice Studies, 29*(2), pp. 125–142. DOI:10.1080/1478601X.2016.1170278

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice, 20*(3), pp. 358–375. DOI:10.1177/1748895819835910

Cross, C., & Kelly, M. (2016). The problem of "white noise": examining current prevention approaches to online fraud. *Journal of Financial Crime, 23*(4), pp. 806–818. DOI:10.1108/JFC-12-2015-0069

Cullen, F. T., Agnew, R., & Wilcox, P. (2022). Understanding Criminological Theory: A Guide for Readers. In F. T. Cullen, R. Agnew, & P. Wilcox, *Criminological Theory: Past to Present* (7th edition, pp. 1-18). Oxford University Press.

Danmarks Statistik. (n.d. *a*). *Digitalisering*. Hentet 1. februar 2024 fra Dst.dk: Digitalisering

Danmarks Statistik. (n.d. *b*). *STRAF11*. Hentet 1. februar 2024 fra Statistikbanken.dk: STRAF11

Den Danske Ordbog. (n.d.). *Techgigant*. Hentet 1. juni 2024 fra Ordnet.dk: Techgigant

Det Kriminalpræventive Råd. (n.d.). *Ordliste*. Hentet 1. juni 2024 fra dkr.dk: Ordliste

Det Kriminalpræventive Råd. (14. maj 2024). *Udvalget for Borgernes Digitale og Daglige Tryghed*. Hentet 14. maj 2024 fra dkr.dk: Udvalget for Borgernes Digitale og Daglige Tryghed

Digitaliseringsstyrelsen. (n.d.). *Vejledning om databeskyttelse i den elektroniske kommunikationssektor*. Hentet 10. maj 2024 fra digst.dk: Vejledning om databeskyttelse

Digitaliseringsstyrelsen. (n.d.). *MitID - en sikker løsning*. Hentet 13. maj 2024 fra digst.dk: MitID - en sikker løsning

Erhvervsministeriet. (2023). *Faktaark digital svindel*. Hentet 13. marts 2024 fra em.dk: Faktaark digital svindel

European Banking Federation. (n.d.). *ABOUT US - EBF*. Hentet 12. maj 2024 fra ebf.eu: EBF - about us

European Banking Federation. (25. oktober 2018). *CYBERSECURITY - EBF*. Hentet 12. maj 2024 fra ebf.eu: Cybersecurity

Eurostat. (2024). *Individuals' level of digital skills (from 2021 onwards) [Digitale færdigheder i europæiske lande]*. Hentet 17. januar 2024 fra ec.europa.eu: Individuals level of digital skills

Finans Danmark. (10. april 2017). *Nordisk samarbejde i finanssektoren styrker kampen mod cyberkriminalitet*. Hentet 13. maj 2024 fra finansdanmark.dk: Nordisk samarbejde i finanssektoren

Finans Danmark. (december 2023). *Kampen mod digital svindel.* Hentet 12. marts 2024 fra finansdanmark.dk: Kampen mod digital svindel

Finans Danmark. (21. maj 2024 *a*). *Der er fuld fart på de digitale svindlere – alle gode ideer til at stoppe dem er i spil*. Hentet 25. maj 2024 fra finansdanmark.dk: Der er fuld fart på de digitale svindlere

Finans Danmark. (1. januar 2024 *b*). *Et år uden bankrøverier – for andet år i træk*. Hentet 12. marts 2024 fra ritzau.dk: Et år uden bankrøverier

Finans Danmark. (n.d. *a*). *Bank Vishing Opkald*. Hentet 1. juni 2024 fra finansdanmark.dk: Bank Vishing Opkald

Finans Danmark (n.d. *b). Om os*. Hentet 25. maj 2024 fra finansdanmark.dk: FD - Om os

Finans Danmark. (n.d. *c*). *Sikker Bank - sammen*. Hentet 12. maj 2024 fra finansdanmark.dk: Sikker bank - sammen

Finans Danmark. (n.d. *d*). *Svindel Task Force*. Hentet 11. maj 2024 fra finansdanmark.dk: Svindel Task Force

Fjord, L. (2023). *Finans Danmarks høringssvar vedrørende forslag til forordning om betalingstjenester i det indre marked og direktiv om betalingstjenester og e-penge i det indre marked*. Hentet 13. maj 2024 fra finansdanmark.dk: FD høringssvar

Folketinget. (3. marts 2021-22). *Forslag til Lov om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester. Vedtaget af Folketinget ved 3. behandling den 3. marts 2022*. Hentet 30. maj 2024 fra ft.dk: Lovforslag

Forbrugerrådet Tænk. (2017). *Mit digitale selvforsvar (Version 3.3.2) [Mobilapplikation software]*. Hentet 5. februar 2024 fra: Mit digitale selvforsvar

Forbrugerrådet Tænk. (2023 juli 2023). *Beskyt dig mod svindelbeskeder på sms*. Hentet 25. maj 2024 fra taenk.dk: Beskyt dig mod svindelbeskeder på sms

Forbrugerrådet Tænk. (n.d.). *Mit digitale Selvforsvar*. Hentet 5. februar 2024 fra taenk.dk: Om Mit digitale selvforsvar

Google. (n.d.). *RCS chats by Google FAQ - Google Message*. Hentet 10. maj 2024 fra support.google.com: RCS chats

Harrits, G. S., Pedersen, C. S., Halkier, B., & Møller, A. (2020). Indsamling af interviewdata. I K. M. Hansen, L. B. Andersen, & S. W. Hansen, *Metoder i statskundskab* (3. udgave, s. 180-211). Hans Reitzels Forlag.

Heron, T. (21. marts 2024). *De danske forbehold*. Hentet 30. maj 2024 fra eu.dk: Danske forbehold

Ingemann, J. H., Kjeldsen, L., Nørup, I., & Rasmussen, S. (2018). Forberedelse og udførelse af kvalitative interviews. (1. udgave, s. 147-194). Samfundslitteratur.

Jacobsen, A. V., Erenbjerg, A., Törnfelt, C., & Tassy, A. (2023). *It-anvendelse i befolkningen 2023.* Danmarks Statistik. Hentet 1. februar 2024 fra dst.dk: it-anvendelse i befolkningen

Jensen, R. I., Gerlings, J., & Ferwerda, J. (2024). Do Awareness Campaigns Reduce Financial Fraud? *European Journal on Criminal Policy and Research*, pp. 1-36. DOI:10.1007/s10610-024-09573-

Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Siami Namin, A. (2021). How social engineers use persuasion principles during vishing attacks. *Information and Computer Security, 29(2)*, pp. 314-331. DOI:10.1108/ICS-07-2020-0113

Justitsministeriet. (2020). *Aftale om politiets og anklagemyndighedens økonomi 2021-2023.* Hentet 6. marts 2024 fra Justitsministeriet.dk:
Aftale om politiets og anklagemyndighedens økonomi 2021-2023

Justitsministeriet. (2021). *Udkast: Forslag til Lov om ændring af retsplejeloven, hvidvaskloven og forskellige andre love (Etablering af National Enhed for Særlig Kriminalitet og styrkelse af indsatsen mod hvidvask m.v.).* Hentet 6. marts Justitsministeriet.dk:
Udkast: Forslag til lov om ændring af retsplejeloven, hvidvaskloven og forskellige andre love

Kejlberg, N. A. (19. september 2022). *Anders And og Rip, Rap og Rup går online!* Hentet 12. maj 2024 fra Center for Digital Pædagogik: Anders And

Kirkebæk-Johansson , L., & Jorsal, T. (31. august 2023). Sidste år blev der anmeldt mindst 750 sager om telefonsvindel. Der faldt dom i fem. Hentet 5. februar 2024 *DR.dk*: Sidste år blev der anmeldt mindst 750 sager om telefonsvindel

Kvale, S., & Brinkmann, S. (2015). *Interview: Det kvalitative forskningsinterview som håndværk* (3. udgave). Hans Reitzel.

Latour, B. (2008). *En ny sociologi for et nyt samfund: Introduktion til aktør-netværk-teori.* Akademisk.

LCIK. (2020). *LCIK Årsrapport 2019 [En rapport om it-relateret økonomisk kriminalitet anmeldt i 2019]*. Hentet 1. februar 2024 fra Politi.dk: Årsrapport 2019

LCIK. (2021). *LCIK Årsrapport 2020 [En rapport om it-relateret økonomisk kriminalitet anmeldt i 2020]*. Hentet 1. februar 2024 fra Politi.dk: Årsrapport 2020

Lee, C. S. (2020). A crime script analysis of transnational identity fraud: migrant offenders' use of technology in South Korea. *Crime, Law and Social Change, 74*(2), s. 201-218. DOI:10.1007/s10611-020-09885-3

Lynggaard, K. (2020). Dokumentanalyse. I S. Brinkmann, & L. Tanggaard, *Kvalitative metoder : en grundbog* (3. udgave, s. 185-202). Hans Reitzel.

NCIK. (2022). *NCIK Årsrapport 2021 [En rapport om it-relateret økonomisk kriminalitet anmeldt i 2021]*. Hentet 1. februar 2024 fra Politi.dk: Årsrapport 2021

NCIK. (2023). *NCIK Årsrapport 2022 [En rapport om it-relateret økonomisk kriminalitet anmeldt i 2022]*. Hentet 1. februar 2024 fra Politi.dk: Årsrapport 2022

NCIK. (2024). *NCIK Årsrapport 2023 [En rapport om it-relateret økonomisk kriminalitet anmeldt i 2023]*. Hentet 23. maj 2024 Politi.dk: Årsrapport 2023

NSK. (23. juni 2022). *Samhandel fylder fortsat mest i anmeldelser om it-kriminalitet.* Hentet 6. februar 2024 fra Politi.dk: Samhandel fylder fortsat mest i anmeldelser om it-kriminalitet

Nordea. (13. marts 2023) *What is PSD2?* Hentet 13. maj 2024 fra nordea.dk: What is PSD2?

Nordea. (15. marts 2024) *What are PSD3 and PSR?* Hentet 13. maj 2024 fra nordea.dk: What are PSD3 and PSR?

Olesen, F., & Kroustrup, J. (2007). ANT - Beskrivelsen af heterogene aktør-netværk. I C. Bruun Jensen, P. Lauritsen, & F. Olesen, *Introduktion til STS: science, technology, society* (1. udgave, s. 63-92). Hans Reitzel.

Pedersen, M. L., Hjarsen, C. F., & Balvig, F. (2023). *Udsathed for vold og andre former for kriminalitet. Offerundersøgelserne 2005-2022. Hovedtal.* Justitsministeriet. Udsathed for vold og andre former for kriminalitet

Politi. (n.d. *a*). *FIT - forum mod it-relateret økonomisk kriminalitet*. Hentet 18. maj 2024 fra politi.dk: FIT

Politi. (n.d. *b*). *Operativt Dansk Informations- og efterretnings Netværk (ODIN)*. Hentet 19. maj 2024 fra politi.dk: ODIN

Politi. (n.d. *c*). *Organisationen*. Hentet 18. maj 2024 fra politi.dk: Organisationen

Retsudvalget. (7. september 2022). *Politiets eksisterende muligheder for at prioritere sager [Retsudvalget 2022-23 (2. samling) svar på spørgsmål 754]*. Hentet 28. januar 2024 fra Justitsministeriet: Politiets eksisterende muligheder for at prioritere

Rigspolitiet. (22. august 2019). *Over 12.000 anmeldelser til politiets nye center for it-relateret økonomisk kriminalitet*. Hentet 28. januar 2024 fra politi.dk: Over 12.000 anmeldelser til politiets nye center

Rigspolitiet. (2021). *Co+creation Samskabelse med civilsamfundet [Co-creation casekatalog]*. Hentet 12. marts fra Politi.dk: Co+creation

Rigspolitiet og Rigsadvokaten. (6. februar 2020). *Økonomisk kriminalitet [Bilag 258 til retsudvalgets møde d. 6/2-20]*. Hentet 1. februar 2024 fra ft.fk: Bilag 258

Riis, O. (2012). Kvalitet i kvalitative studier. I M. H. Jacobsen, & S. Q. Jensen, *Kvalitative udfordringer* (1. udgave, s. 345-374). Hans Reitzel.

Ritzau. (5. januar 2023). *Over 135 mistænkte muldyr er anholdt i sag om svindel mod ældre*. Hentet 1. juni 2024 fra EkstraBlandet.dk: Over 135 mistænkte muldyr er anholdt i sag om svindel mod ældre

Tanggaard, L., & Brinkmann, S. (2020). Interviewet: samtalen som forskningsmetode. I S. Brinkmann, & L. Tanggaard, *Kvalitative metoder: en grundbog* (3. udgave, s. 33-64). Hans Reitzel.

Teleindustrien. (n.d.). *Teleselskabernes branchesamarbejde - Teleselskabernes Branchesamarbejde | Om TI*. Hentet 9. maj 2024 fra teleindu.dk: Teleindustrien

Thorning, C. (13. november 2023). *Finans Danmark er sammen med Forbrugerrådet Tænk, Teleindustrien, Ældre Sagen og Erhvervsministeriet nået til enighed om en række initiativer i kampen mod digital svindel. Der er blandt andet enighed om at sænke beløbsgrænsen for straksoverførsler pr. døgn*. Hentet 13. maj 2024 fra finansdanmark.dk: Initiativer i Svindel Task Force

United Nations. (2022). *United Nations E-Government Survey 2022: The Future of Digital Government.* United Nations. The future of digital government

Viano, E. C. (2016). Cybercrime: Definition, Typology, and Criminalization. In E. C. Viano, *Cybercrime, Organized Crime, and Societal Responses* (pp. 3-22). Springer International Publishing.

Wright, G. (n.d.). *Definition Signaling System 7 (SS7)*. Hentet 11. maj 2024 fra techtarget.com: Signalsystem 7

Økonomiministeriet. (1. februar 2024). *Samlenotat - Mandat til forhandling om forslag vedr. betalingstjenester (PSR og PSD3)*. Europaudvalget 2023-24 KOM (2023) 0367 Bilag 4. Hentet 28. februar 2024 fra eu.dk: Samlenotat

Østjyllands Politi. (15. december 2023). *Fire mænd idømt 23 års fængsel for omfattende telefonsvindel*. Hentet 14. marts 2024 fra Politi.dk: Fire mænd idømt 23 års fængsel