"Din pakke er klar til afhentning. Klik her og få franarret dine penge"

En crime script analyse af vishing, phishing og smishing i Danmark

Kandidatafhandling i Kriminologi
10. semester 6. juni 2023

Udarbejdet af:
Henry Phong Pham
Line El-Shakarji Nielsen

Vejleder:
Sune Qvotrup Jensen
Antal ord: 29.764

Abstract

This study aims to clarify the procedural stages/ approach of perpetrators of vishing, phishing and smishing in a Danish context.

To investigate this, we make use of semi-structured interviews and analysis of four cases. The semi-structured interviews were conducted with employees at Sydbank and the Police on Funen. The four cases are primary data, where the victims themselves report on their experience with vishing and smishing. Our theoretical perspective is focused on the routine activity theory, which makes it possible to examine the processes that must be present before the criminal act can take place. We use crime script analysis as an analytical framework for the study.

We find that two types of vishing occur. In the first type of vishing, the victims' cards are collected at their home address, after which the perpetrators withdraw cash from an ATM. The second type is safe account fraud. A great reason why vishing can occur is due to the great trust that the Danish population has in the authorities and not least in each other. In vishing, the perpetrators use a script from which they speak. The script makes the perpetrators appear professional and trustworthy. We also see a tendency for vishing to be coordinated and planned attacks with several perpetrators supporting each other when talking to the victims.

In phishing and smishing, the perpetrators make use of certain trends in society, which help to support their credibility. They broadcast mass communications, which are timed with major events in society. When sending mass communications, they have spoofed the e-mail or phone number from which they send the messages. The messages typically contain links that lead to fake websites where the victims share their personal information. Furthermore, we find cases where the perpetrators pretend to be an acquaintance of the victim.

As a final part of vishing, phishing and smishing, the stolen financial means must be converted into something tangible for the perpetrators. This takes place through four trends: 1) Withdraw the money from card machines after collecting the victim's card, 2) Convert the money into value, 3) Convert the money into bitcoin and other crypto-currency or 4) Through the use of mules.

At the end of the study, we include, among other things, Situational Crime Prevention for proposals for crime prevention.

Indholdsfortegnelse

Kapitel 1

Indledning

1. Indledning

"Har du en falsk (land)betjent i røret?". "PAS PÅ! Igen er vi ramt af tricktyve der ringer til primært ældre kvinder og franarrer dem penge." Sådan lyder nogle af de opslag, som det danske politi i øjeblikket deler på deres sociale medier. Svindelnumre med sigtet om økonomisk vinding er tiltagende, og opkald fra "landbetjente" og andre tricktyve er blot én af de mange metoder, som gerningspersoner anvender.

I en undersøgelse foretaget af FN i 2022 blev Danmark for tredje gang udpeget som det mest offentligt digitaliserede land i verden (Digitaliseringsstyrelsen, 2022). Den digitale udvikling har mange fordele, men kriminelle benytter den også til at udføre deres svindelnumre. Digitaliseringen muliggør, at de kriminelle kan udføre deres handlinger hjemmefra. Der er på den måde mindre risiko forbundet med den kriminelle handling, idet de ikke skal stå ansigt til ansigt med deres ofre. Dette betyder samtidigt, at de kan foretage flere kriminelle handlinger over kortere tid.

I 2021 modtog Politiets Nationale Center for It-Kriminalitet (NCIK) 26.588 anmeldelser om økonomisk kriminalitet foretaget online. 22.675 af dem blev anmeldt af privatpersoner (NCIK, 2022: 8, 17). NCIK påpeger en overordnet stigning i antal anmeldelser fra år 2019-2021. Fra 2020-2021 er der sket en stigning på 57% i sager med kontaktbedrageri[1] mod private – herunder vishing, phishing og smishing (begreber uddybes i afsnit 2.1). Tallene fra NCIK viser, at udbredelsen af økonomisk kriminalitet, herunder vishing, phishing og smishing, er stigende. Afhængigheden af teknologien betyder, at vores hverdagsliv og -rutiner i stort omfang er flyttet til de digitale platforme, hvilket ud fra en dansk kontekst kan være årsagen til, at flere og flere oplever disse angreb. Det er relevant at undersøge, hvordan de digitale platforme muliggør den kriminalitet, der kaldes vishing, phishing og smishing.

Formålet med følgende undersøgelse er gennem crime script analysis at belyse de processuelle stadier, som kriminelle anvender til at udføre nævnte kriminalitet – herunder inddragelsen af de digitale platforme.

[1] Det Kriminalpræventive Råd (DKR) beskriver kontaktbedrageri således: *"Kontaktbedrageri eller forskudsbedrageri er, hvis man overfører penge til en person, som man har fået kontakt til over internettet, og som senere viser sig at være en bedrager. Overførslen kan fx bestå af hjælp til rejseudgifter eller penge, man betaler i forskud for at modtage et større beløb. [...] Bedrageren kan både være en person, ofret ikke kender, en person, der udgiver sig for at være én, ofret kender, eller en person, ofret har mødt online, fx på et datingsite"* (DKR, 2022a)

NCIK definerer kontaktbedrageri som følgende: *"Kontaktbedrageri mod privatpersoner foregår ofte ved, at en gerningsperson tager kontakt til en person med henblik på at begå bedrageri og franarre vedkommende penge eller værdier [...] Kontakten kan både forekomme telefonisk eller over e-mail.* (NCIK, 2022: 38).

Kapitel 2

Problemfelt og problemformulering

2. Problemfelt og problemformulering

I dette kapitel introduceres problemfeltet for undersøgelsens forskningsområde. Første del af kapitlet er en begrebsafklaring af de termer, som er hovedelementerne af undersøgelsen. Derefter følger et afsnit, der præsenterer omfanget af vishing, phishing og smishing både på globalt og nationalt plan. Afslutningsvis præsenteres nogle af de eksisterende initiativer til bekæmpelse af databedrageri og hvidvask i Danmark.

2.1 Begrebsafklaring

I dette afsnit redegøres der for de relevante begreber inden for databedrageri, der inkluderes i undersøgelsen. Den juridiske definition for databedrageri står skrevet i retsplejelovens §279a og lyder som følger:

> *For databedrageri straffes den, som for derigennem at skaffe sig eller andre uberettiget vinding retsstridigt ændrer, tilføjer eller sletter oplysninger eller programmer til elektronisk databehandling eller i øvrigt retsstridigt søger at påvirke resultatet af sådan databehandling.* (Justitsministeriet, 2021).

I denne undersøgelse afgrænses databedrageri til at dække over phishing, smishing og voice phishing (vishing). I den forbindelse er det relevant først at introducere til *malware og social engineering.*

Malware og social engineering

Malware (malicious software) er software anvendt til digitalt indbrud gennem hacking. Dette kan eksempelvis opstå, hvis et offer får tilsendt en (phishing)mail og klikker på et link, der fører til en falsk hjemmeside, eller hvis vedkommende åbner en skadelig vedhæftet fil.
Social engineering *"omfatter sager, hvor brugeren lokkes til at afgive eller indtaste oplysninger (id, password og nøglekortkoder) til de it-kriminelle på baggrund af falske mails, SMS eller telefonopkald. Disse giver sig ud for at komme fra eksempelvis et velrenommeret selskab, en myndighed eller en ven."* (Finans Danmark, u.å.).

Social engineering anvendes i flere fagområder, men når det kommer til økonomisk kriminalitet er social engineering, når gerningspersonen forsøger følelsesmæssigt at manipulere med offeret ved at lokke vedkommende til at afgive personfølsomme oplysninger. Kontakten etableres gennem mails under falsk identitet, SMS og/ eller telefonopkald. Center for

Cybersikkerhed har ligeledes udarbejdet en definition af social engineering og beskriver det som en teknik, hvor gerningspersonen anvender psykologiske greb til at få offeret til at udføre en handling i god tro, som offeret ellers ikke ville have udført (Center for Cybersikkerhed, 2022: 6).

Malware og social engineering er begge teknikker, der kan anvendes ved phishing og smishing, mens social engineering i særdeleshed anvendes ved vishing, hvilket også fremgår af citaterne i nedenstående tabel. Formålet for gerningspersonen med vishing, phishing og smishing er det samme – at få et offer til at udlevere personlige oplysninger, som gerningspersonen kan udnytte til egen økonomisk vinding. Mere om dette vil blive præsenteret i kapitel 3.

Tabel 1: Begrebsafklaring for phishing, smishing og vishing

Phishing *"Phishing er et forsøg på at narre e-mailmodtagere til i god tro at videregive personlige eller andre beskyttelsesværdige oplysninger eller give uretmæssig adgang til bl.a. it-systemer. Ofte vil angriberen ved hjælp af simpel social engineering forsøge at få ofrene til at klikke på links til falske hjemmesider eller åbne inficerede filer. [malware]. Phishing e-mails sendes ofte bredt ud til mange tilfældige modtagere uden at være tilpasset den enkelte modtager."* (Center for Cybersikkerhed, 2020: 3)
Smishing *"Smishing er phishing forsøg, som foregår via sms. Sms'en vil typisk forsøge at narre modtageren til at gå ind på en hjemmeside for at bekræfte password eller kreditkortoplysninger eller lokke ofret til at downloade en skadelig app. Ofret kan også lokkes til at ringe til et telefonnummer, hvor gerningsmanden vil fortsætte sit svindelnummer."* (Center for Cybersikkerhed, 2020: 4)
Voice phishing (vishing) *"Vishing er phishing forsøg via telefonopkald. Gerningsmanden fortæller måske, at ofret har vundet en konkurrence, og skal udlevere personlige oplysninger for at modtage præmien. Gerningsmanden kan også påstå, at ofret har sikkerhedsproblemer med sin computer, betalingskort eller bankkonto og skal udlevere personlige oplysninger eller adgangskoder for at få løst problemet."* (Center for Cybersikkerhed, 2020: 4)

Muldyr og hvidvask

Som led i IT-kriminalitet er det relevant at nævne termen *'muldyr'*. Et muldyr betegnes som en person, der bevidst eller ubevidst hjælper kriminelle med at transportere ulovligt indhentede penge. Dette gøres ved, at muldyr sætter deres konto til rådighed, hvortil de kriminelle kan overføre de ulovligt indhentede penge for derefter at udbetale dem. Derved forbliver gerningspersonerne uopdagede, og pengenes oprindelsessted/ retlige ejer tilsløres. Dette kaldes også *'hvidvask'* (DKR, 2021: 21).

2.2 Vishing, phishing og smishing i tal

Dette afsnit præsenterer de nyeste tal inden for vishing, phishing og smishing. Afsnittet tager afsæt i udgivelser fra forskellige myndigheder og NGO'er, der beskæftiger sig med bekæmpelse af cyberkriminalitet. Yderligere præsenteres vishing, phishing og smishing i en dansk kontekst med opgørelser fra blandt andet Danmarks Statistik, Det Kriminalpræventive Råd, Hvidvasksekretariatet, NCIK og Finans Danmark.

Ifølge Finans Danmark optrådte netbankssvindel for første gang i Danmark i 2006, og siden har problemet været tiltagende (Finans Danmark, u.å.). Finans Danmark inddeler netbankssvindel i to kategorier: 1) Netbankssvindel gennem malware og 2) Netbankssvindel gennem social engineering. Data fra Finans Danmark er inddelt i halvår og omfatter 2020, 2021 og første halvår af 2022. Der ses en stigning i antallet af forsøg på netbankssvindel gennem social engineering for hele perioden. I første halvår af 2022 er der således registreret 1.551 tilfælde, og 623 af disse var med økonomisk tab til følge (ca. 40%). I første halvår af 2021 udgjorde det økonomiske tab også cirka 40%, mens det i første halvår af 2020 udgjorde lidt over 52% af det samlede antal sager om netbankssvindel gennem social engineering. Det samlede beløb på tab ved netbankssvindel gennem social engineering i første halvår af 2022 lød på næsten 30,3 mio. DKK (Finans Danmark, u.å.). Det lyder umiddelbart ikke af meget, men tabet ved netbankssvindel udgør 58,7% mere end ved eksempelvis kærlighedssvindel (med et samlet tab på 12,5, mio. DKK i første halvår af 2022) (Finans Danmark, u.å.).

I den seneste rapport fra den internationale koalition til bekæmpelse af cyberkriminalitet, Anti-Phishing Working Group (APWG), er der i tredje kvartal af 2022 observeret 1.270.883 phishing-angreb på globalt plan, hvilket er rekord. I august samme år blev 430.141 phishing-angreb registreret, hvilket er det højeste målte antal på en måned nogensinde (APWG, 2022a: 2). I tredje kvartal af 2022 var 23,3% af phishing-angrebene rettet mod virksomheder i

den finansielle sektor. Dette er et fald siden andet kvartal, hvor andelen af angreb mod den finansielle sektor lå på 27,6% (APWG, 2022a: 5). Generelt er antallet af phishing mod konkrete sektorer såsom sociale medier og e-handel/ detailhandel faldet fra andet- til tredje kvartal i 2022 (APWG, 2022a: 5; APWG, 2022b: 5).
I rapporten pointerer APWG desuden, at der er sket en stigning på 488% i responsbaserede-email-angreb (phishing) fra andet- til tredje kvartal i 2022 (APWG, 2022a: 9).

Det Kriminalpræventive Råd (DKR) inddeler it-kriminalitet i tre kategorier, hvoraf den ene – *computer-assisterede forbrydelser* – er relevant for denne undersøgelse (DKR, 2022a). DKR beskriver computer-assisterede forbrydelser som følgende:

> *"Disse forbrydelser har ofte et økonomisk sigte. Det er kendte kriminalitetsformer som tyveri og bedrageri, der begås ved hjælp af internetteknologi. Det er fx Nigeriabreve, phising* [phishing] *eller indbrud i en netbank."* (DKR, 2022a)

Digitaliseringsstyrelsen, KL med flere påpeger i en undersøgelse, at 52% af befolkningen mellem 16 og 89 år i 2020 oplevede at modtage phishing-e-mails. 30% oplevede svindel via SMS (smishing), mens 21 pct. oplevede svindel via opkald (vishing) en eller flere gange inden for det seneste år (Larsen et a., 2020: 12).
I Justitsministeriets offerundersøgelse påpeges det, at 3,7% af de adspurgte danskere mellem 16 og 74 år var udsat for it-kriminalitet i 2021 (ud fra 12.397 besvarelser). It-kriminalitet dækker over: *1) Misbrug af betalingskortoplysninger, 2) Samhandel på internettet, 3) Kontaktbedrageri, 4) Misbrug af personoplysninger* og *5) hadefulde ytringer* (Justitsministeriets Forskningskontor, 2022: 23). Vishing, phishing og smishing hører under kategorierne 1, 3 og 4.

Dette er et fald sammenlignet med 2020 (5%) og 2019 (4%) (med en gennemsnitlig svardeltagelse på cirka 12.000 respondenter for disse to år). I undersøgelsen påpeges det, at tallene fra år 2019 ikke er sammenlignelige med de efterfølgende år, idet der først er blevet spurgt ind til *'hadefulde ytringer'* fra år 2020, således at dette indgår i det samlede antal (Justitsministeriets Forskningskontor, 2022: 22).
Af offerundersøgelsen fremgår det, at den hyppigste form for it-kriminalitet er *'misbrug af betalingskortoplysninger'*, hvilket 1,6% af de adspurgte danskere i alderen 16-74 år var ofre for i 2021. Dette er et fald fra år 2019, hvor antallet af ofre for denne type it-kriminalitet lå på 2,6% (Justitsministeriets Forskningskontor, 2022: 22-23). En forklaring herpå kan være kravet om tofaktor-godkendelse ved aktiviteter på internettet, der blev pålagt fra år 2021.

Numerisk er 1,6% ikke et stort tal, men sammenlignet med en befolkning på cirka 6 mio. udgør dette trods alt 96.000 borgere. Mange er måske ikke bevidste om, at de har været udsat for vishing, phishing eller smishing, og en anden mulighed kan være, at hændelsen ikke er blevet anmeldt. Samtidigt skal det bemærkes, at afbrudte vishing-/ phishing-/ smishing-angreb ikke indgår i statistikken og muligvis slet ikke anmeldes. Der kan dermed være nogle mørketal, som gør, at man ikke får det reelle billede af disse databedragerityper i Danmark.

I en måling fra Danmarks Statistik af befolkningens it-anvendelse i Danmark fremgår det, at 45% af den danske befolkning mellem 16 og 74 år har oplevet at modtage phishing-mails i 2019 (Tassy, Nielsen & Jakobsen, 2020: 34). Her påpeges det samtidigt, at den tilsvarende andel for de andre adspurgte EU-lande ligger på 26%. Over halvdelen af de adspurgte EU-borgere i alderen 16-74 år mener ikke, de har været udsat for it-kriminalitet i 2019. Danmarks Statistik påpeger samtidigt, at den adspurgte del af Danmarks befolkning i 2019 giver mindre udtryk for bekymringer ved private aktiviteter på internettet (Danmarks Statistik, 2019). Det vil sige, at tilliden til it-sikkerheden er steget.

Center for Cybersikkerhed (2020) påpeger, at der i 2019 på globalt plan gennemsnitligt blev etableret 65.000 nye phishing-hjemmesider hver måned (Center for Cybersikkerhed, 2020: 14). Det bemærkes samtidigt, at phishing-mails fungerer i samspil med en hjemmeside, og ofte kan disse mails være harmløse, hvis hjemmesiden formås fjernet (Center for Cybersikkerhed, 2020: 15).

En rapport fra NCIK viser, at antallet af anmeldelser for phishing og smishing er steget fra 1.580 til 3.372 fra 2020-2021. Disse former for bedrageri er ifølge NCIK de mest anmeldte og anvendte ved misbrug af kortoplysninger (NCIK, 2022: 27). Det skal påpeges, at der ved 70% af sagerne ikke er oplyst et tab, men ud fra stigningen i antallet af anmeldelser om phishing og smishing på et år antages der, at svindlerne har øget fokus på sådanne kriminalitetsformer. Stigningen kan skyldes de mange falske hjemmesider, som fremstår troværdige og efterligner noget, som den almene borger kender.

2.3 Initiativer til bekæmpelse og forebyggelse af databedrageri og hvidvask

For at forstå fænomenet *'databedrageri'* ud fra et forebyggelsesperspektiv er det væsentligt at komme ind på, hvilke forebyggende indsatser der er blevet etableret for at bekæmpe denne kriminalitetstype. Nedenstående afsnit vil omhandle de danske indsatser og initiativer, som er målrettet databedrageri, herunder vishing, phishing og smishing. Yderligere vil de danske initiativer inden for hvidvask præsenteres, da hvidvask hænger sammen med it-relateret

økonomisk kriminalitet som vishing, phishing og smishing . I disse tilfælde er pengene allerede i det finansielle system, hvorfor der anvendes muldyr til at overføre det ulovlige udbytte til forskellige betalingstjenester for at sløre pengenes oprindelse (Hvidvasksekretariatet, 2022: 55).

Center for Cybersikkerhed har udgivet en vejledning i 2022, hvori de kommer med overordnede anbefalinger til, hvordan man kan reducere risikoen for phishing i en organisation (Center for Cybersikkerhed, 2022: 5). Denne vejledning fokuserer på phishing gennem e-mails og beskriver nogle af de kendetegn, som kan forekomme ved denne type af kriminalitet. Et af kendetegnene ved phishing er, at gerningspersonen forsøger at udnytte følelser som nysgerrighed, bekymringer og et ønske om at ville hjælpe offeret (Center for Cybersikkerhed, 2022: 7). Yderligere kommer vejledningen ind på, hvilke ting man skal være opmærksom på i forhold til phishing-mails i en organisation, hvilket ligeledes kan impliceres i private sammenhænge. Center for Cybersikkerhed kommer ind på, at man skal undgå mails, der indeholder links til websider, hvorfra der er direkte login med NemID og andre loginoplysninger (Center for Cybersikkerhed, 2022: 5). Derudover nævner de, at man skal installere antivirus på sine enheder, således at man kan bruge mail-filtre til at blokere eller filtrere uønskede mails, inden de kommer ind på brugernes indbakke. Center for Cybersikkerheds vejledning handler i høj grad om at reducere risikoen for phishing gennem e-mails hos organisationer, men den kan ligeledes implementeres ved private personer. Yderligere kommer vejledningen ind på, at hvis der er mistanke om afsenderens reelle identitet, skal man undgå at svare i samme tråd (Center for Cybersikkerhed, 2022: 7).

Forbrugerrådet Tænk, Det Kriminalpræventive Råd og Trygfonden har i 2018 udviklet en gratis app, der hjælper borgerne med at være sikre online. Appen hedder "mit digitale selvforsvar" og holder forbrugerne opdateret med de nyeste digitale trusler (Forbrugerrådet Tænk, u.å.). Nedenstående billede er fra app'en "mit digitale selvforsvar" og giver et eksempel på nogle af de typer af svindel, app'en advarer imod.

Kilde: Forbrugerrådet Tænk, u.å.

Formålet med app'en er at beskytte borgernes privatliv på nettet, hvor app'en også giver konkret viden til at undgå it-kriminalitet. App'en hjælper både med at forebygge, men den hjælper også brugeren med at løse problemet, hvis offeret er blevet svindlet.

I henhold til danske initiativer inden for hvidvaskområdet har Det Kriminalpræventive Råd i 2022 udarbejdet undervisningsmateriale omkring dette. Formålet med undervisningsmaterialet er at forebygge, at unge bliver brugt som kriminelle muldyr. Materialet belyser, hvordan unge vidende eller uvidende kan medvirke til at hvidvaske penge for kriminelle (DKR, 2022b: 3). Den primære målgruppe for dette undervisningsmateriale er unge i de højeste klassetrin på grundskoler, efterskoler og ungdomsuddannelser. Forebyggelsesindsatsen skal være med til at understøtte en dialog med de unge om hvidvask af penge og rollen som muldyr (DKR, 2022b: 3). Derfor har Det Kriminalpræventive Råd ligeledes lavet en minidokumentar, hvis formål er at skabe refleksioner om, hvad de unge selv skal gøre for at undgå at blive et muldyr, som i øvrigt kan medføre en plet på straffeattesten. På denne måde skal undervisningsmaterialet hjælpe unge med at identificere situationer, hvor potentielle gerningspersoner forsøger at overtale dem til at medvirke i at hvidvaske penge (DKR, 2022b: 3).

2.4 Opsummering og problemformulering

Ovenstående afsnit viser, at it-kriminalitet er et dansk såvel som globalt problem. Ud fra en dansk kontekst er phishing den form for it-kriminalitet, der fylder mest. Tallene inden for phishing og smishing indikerer svindlernes øgede fokus på denne form for it-kriminalitet. Tallene inden for phishing på et dansk og globalt plan viser vigtigheden af forebyggelse, da udbredelsen af denne kriminalitetsform er stor. Nyere tal i Danmark viser, at 30,3 millioner DKK er blevet tabt hos ofrene i første halvår af 2022, hvorfor forebyggelsesinitiativer inden for vishing, phishing og smishing er essentielle. Center for Cybersikkerhed og Forbrugerrådet Tænk er nogle af de få instanser, som har udarbejdet forebyggelsesinitiativer mod phishing. Center for Cybersikkerhed har udarbejdet en rapport, som er henvendt til organisationer, hvorfor vi finder det relevant at undersøge phishing hos privatpersoner ud fra en dansk kontekst. Dette leder til vores undersøgelse, hvor vi ønsker at belyse, hvilke metoder svindlere anvender i vishing, phishing og smishing til at overtale ofre til at videregive personfølsomme oplysninger. Vi vil gennem en crime script analysis beskrive og analysere de processer og stadier, som optræder ved disse databedragerityper, så vi derigennem kan klarlægge gerningspersoners sekventielle proces i disse angreb. Dette har ført til følgende problemformulering:

> ***Hvilke metoder anvender gerningspersoner til at gennemføre vishing, phishing og smishing, og hvilke processer indgår i denne kriminalitetstype?***

For at undersøge ovenstående er det relevant først at undersøge, hvilken forskning der allerede er foretaget inden for vishing, phishing og smishing. Dette vil blive præsenteret i det følgende kapitel (kapitel 3). Herefter følger en teoretisk afgrænsning og rammesætning af undersøgelsen (kapitel 4). I kapitel 5 præsenteres den metodiske fremgangsmåde i undersøgelsen, hvilket leder videre til selve undersøgelsen (analysen) i kapitel 6. Undersøgelsen afsluttes med en diskussion og en konklusion (kapitel 7 og 8).

Kapitel 3

Eksisterende forskning

3. Eksisterende forskning på området

Dette kapitel præsenterer noget af den eksisterende forskning inden for vishing, phishing, smishing og muldyr. Formålet her er at give læseren et indblik i forskningsfeltet samtidigt med, at relevansen for denne undersøgelse understreges. Dertil er det en vigtig del af den videnskabelige proces, hvor vi som forskere kan få baggrundsviden om begreber inden for forskningsfeltet. Geografisk er der foretaget flest studier af vishing i Asien, flest om phishing i Europa, mens undersøgelser om smishing både dækker Asien og USA. Muldyr fremgår i alle inkluderede studier, da disse affødes af forudgående vishing, phishing og smishing. Vi har gjort brug af Google Scholar og Scopus, som vi har fået adgang til via AAU Bibliotek.

3.1 Vishing i Asien

Der er foretaget flest studier inden for *vishing* i Asien, mens der er større fokus på *phishing* i Europa. I dette afsnit fremgår den eksisterende forskning inden for vishing. I samtlige undersøgelser indgår crime script-analyser til at forklare gerningspersonernes modus operandi. Først præsenteres to undersøgelser foretaget i Sydkorea, som ligger på tredjepladsen over de mest offentligt digitaliserede lande i verden (kun overgået af Danmark og Finland) (United Nations Department of Economic and Social Affairs, 2022: 8). Afsnittet afsluttes med en tredje undersøgelse foretaget i Vietnam, der betragtes som et af de stadig mere fremtrædende lande, der bliver et operationelt center for cybercrime (Nguyen, 2022: 226).

I Asien blev vishing første gang opdaget i Taiwan i 2002, mens det nåede Sydkorea i 2006 (Choi, Lee & Chun, 2017: 456). Ifølge Choi, Lee og Chun (2017) er vishing en af tidens mest seriøse problemer i Sydkorea. Fra januar til oktober i 2013 blev der registreret 4.022 tilfælde med vishing med en samlet omkostning estimeret til cirka 42,6 mio. USD (Choi, Lee & Chun, 2017: 454-455).
Resultaterne fra undersøgelsen viser, at der indgår tre stadier i et crime script for vishing: 1) Pre-crime stage, 2) Crime event stage og 3) Post-offense stage. I det første stadie indgår forberedelse, rekruttering af telefonsælgere og sammensætningen af et manuskript, som telefonsælgerne taler ud fra. I andet stadie foretages opkaldene til ofrene. Telefonsælgerne er typisk 'Chinese Koreans', der taler koreansk. Disse trænes yderligere i at tale uden kinesisk dialekt, inden de må foretage opkald. I den sidste fase stjæles pengene og overføres de til en konto i Kina (Choi, Lee & Chun, 2017: 459-464).

Den teknologiske udvikling har gjort udbredelsen af digital identitetstyveri mere almindelig end nogensinde før (Lee, 2020: 202). I sin undersøgelse understreger Lee (2020) en stigende tendens af denne type svindel i Asien – særligt i Sydkorea. Lee definerer vishing ud fra to kriterier; der er tale om en samordnet og tværnational kriminel indsats (1), der er drevet af teknologi (2) (Lee, 2020: 202). Lee undersøger, hvordan vishing er organiseret som en transnational kriminel handling, og hvilken indflydelse teknologi har herpå. Ud fra deltagerobservationern og interviews foretager Lee en crime script analyse af gerningspersonernes tilgang til at begå den kriminelle handling. Lee konkluderer, at de kriminelle handlinger udført i Sydkorea gennemføres af hvervede kinesere eller taiwanesere, samt at de er opdelt i to "call-centre" – det ene er i kontakt med de øverste chefer og udsteder ordrer til det andet call-center, hvor de hvervede befinder sig og skal tage kontakt til ofre og begå den kriminelle handling (Lee, 2020: 212). Lee finder desuden, at de hvervede kinesere og taiwanesere gennemgår træning, inden de tager kontakt til deres ofre. Hun anvender Cohen og Felsons Routine Activity Theory til at forklare, hvordan gerningspersonerne finder frem til deres ofre gennem online tilgængelig data på ofrene, samt at disse ofre ikke er bekendte med de motiverede gerningspersoner og står uden en "guardian". Kontakten til ofrene er udelukkende gennem teknologier såsom smartphones og computere, hvilket igen er med til at understrege relevansen af teknologi ved bedrageri (Lee, 2020: 212).

I første halvdel af 2020 modtog det vietnamesiske politi 776 anmeldelser om computersvindel. Heraf var 65% af anmeldelserne relateret til vishing (Nguyen, 2022: 229). Nguyen hævder, at transnational computersvindel er den mest prævalente form for internetkriminalitet (Nguyen, 2022: 227). I hans undersøgelse sættes der et særligt fokus på teknologiens rolle i computersvindel; navnligt bankkortdata og vishing. Nguyen opdeler modus operandi for den transnationale computersvindel i tre dele: 1) Forberedelse, 2) Aktivitet og 3) Post-aktivitet. Forberedelsen omfatter blandt andet at indhente data på ofrene, hacke ofrene, rekruttere muldyr og andre personer samt forberedelse af det tekniske udstyr til at kunne gennemføre aktiviteten. Aktiviteten (2) består i at købe genstande for de stjålne bankkortdata, mens det i tilfældet med vishing handler om at ringe til ofrene, gennemføre aktiviteten og endelig hæve pengene (Nguyen, 2022: 233). Under den sidste af de tre dele (post-aktivitet) hører 'flugt', som i dette tilfælde omfatter fysisk flugt fra ens position, efter pengene er blevet hævet (Nguyen, 2022: 238).

3.2 Phishing i Europa

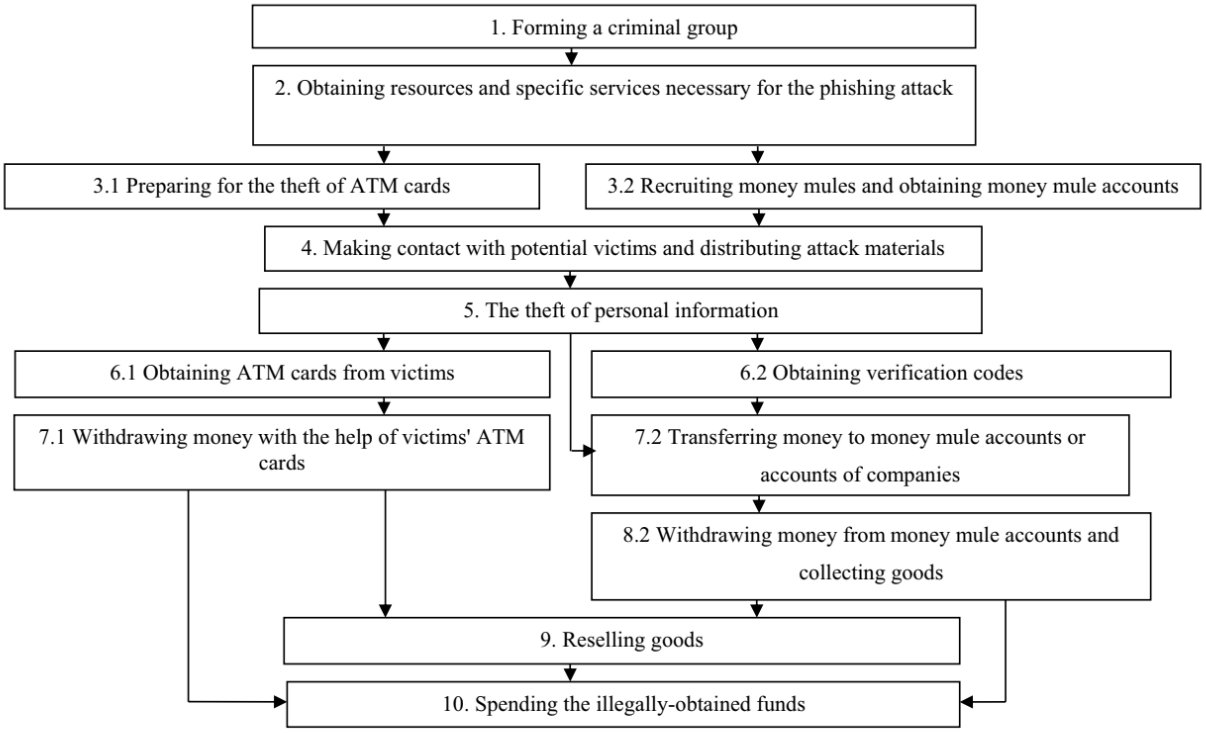
Forskning af phishing er, sammenlignet med Asien, særdeles fremtrædende i Europa. Især i Holland er feltet undersøgt flere omgange af forskere som Leukfeldt, der i dette samt det følgende afsnit optræder i fire af undersøgelserne inden for phishing og muldyr.

I en af udgivelserne af Leukfeldt (2014) fremgår det, at der i hollandske banker i 2011 og 2012 er registreret tab for 35 mio. euro i forbindelse med phishing (Leukfeldt, 2014: 231-232). Ifølge Leukfeldt foregår hvidvask af udbyttet fra phishing ved, at kriminelle grupper opsøger personer gennem direkte kontakt på gaderne og gennem sociale medier i håb om, at de er villige til at udlåne hævekort og PIN-koder i bytte med kontanter, således at gevinster fra phishing kan overføres (Leukfeldt, 2014: 231-232).
I Leukfeldts undersøgelse fokuseres der på kriminelle, som agerer og møder andre "phishere" uden for fora (Leukfeldt, 2014: 232). Leukfeldt inddeler den kriminelle gruppe i tre lag, der agerer på skift i tre faser: 1) Kernen, 2) Facilitatorer og 3) Muldyr (Leukfeldt, 2014: 234-241). Kernen består af tidligere dømte kriminelle fra samme boligområde i Amsterdam. Deres opgave er at rekruttere personer til at udføre handlingerne samt at hæve pengene. Facilitatorerne er ansatte hos banker og postvæsenet og er dem, der ringer til ofrene. Endelig er muldyrene ansvarlige for at dele deres hævekort og PIN-koder. De tre faser består således af: 1) Den forberedende fase hvor personer rekrutteres, 2) Tyverifasen hvor informationer om ofrene indhentes – herunder information som fulde navn, adresse og bankoplysninger (phishing), 3) Kontantudbetalingsfasen hvor muldyrene agerer mellemmænd for ofrenes penge og kernen, der hæver pengene fra kontoen (Leukfeldt, 2014: 241-243).

I en undersøgelse af Loggen og Leukfeldt (2022) undersøges fremgangsmåden bag at stjæle kreditkort, PIN-koder samt tyveri af persondata for at få adgang til ofres bankkonti.
Traditionel kriminalitet såsom hærværk er aftagende i perioden fra 2012 til 2019, mens der ses en stigning i cybercrime i samme periode. Yderligere pointeres det, at hver tredje borger i Holland har stiftet bekendtskab med phishing-beskeder i 2019 (Loggen & Leukfeldt, 2022: 206).
Loggen og Leukfeldts undersøgelse bygger blandt andet på Leukfeldts undersøgelse fra 2014 (omtalt i starten af afsnit 3.2), hvorfor de tre kriminelle lag og faser nævnt i den undersøgelse ligeledes inddrages i denne (Loggen & Leukfeldt, 2022: 206-207). Loggen og Leukfeldt finder to overordnede crime scripts ved phishing: Den ene variant omfatter tyveri af stjålne kreditkort

og PIN-koder. I den anden variant er formålet for den kriminelle at få overført penge fra et offers konto til en tredjepartskonto (Loggen & Leukfeldt, 2022: 210). Crime scripts for de to varianter er opsummeret i den følgende figur:

Figur 1: Skematisk repræsentation af to overordnede crime scripts ved phishing



Kilde: Loggen & Leukfeldt, 2022: 211.

Loggen og Leukfeldt inddeler de forskellige trin i figuren i tre lag. Trin 1-3.2 hører under *forberedelsesfasen*. Trin 4-6.2 hører under *tyverifasen*. De sidste trin (trin 7.1-10) hører under *kontantudbetalingsfasen* (Loggen & Leukfeldt, 2022: 210-214; Leukfeldt, 2014: 242-243).

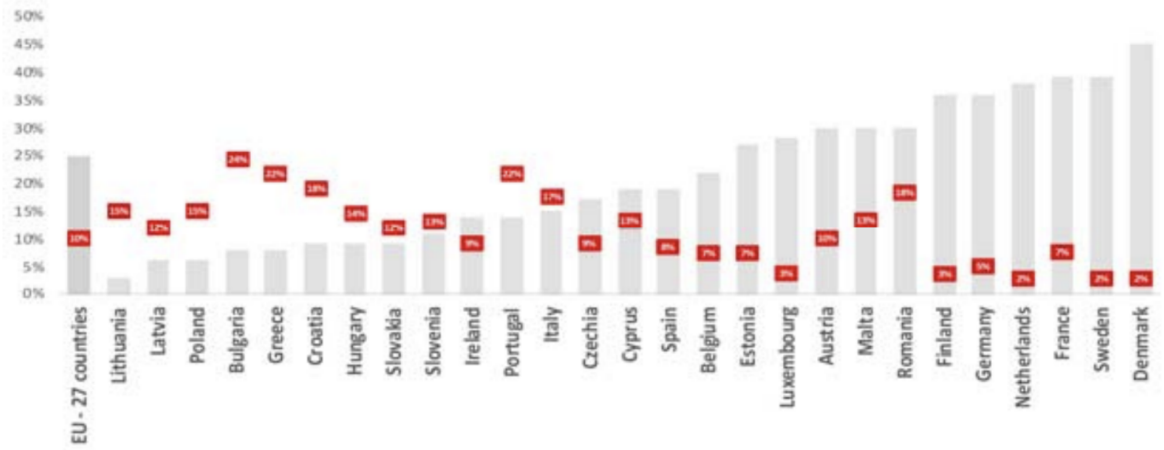
Loggen og Leukfeldt finder, at fremgangsmåden i phishing ikke har ændret sig betydeligt de seneste par år, samt at processen bliver mindre teknologisk, hvilket modsiger ideen om, at digitalisering leder større muligheder for phishing (Loggen & Leukfeldt, 2022: 205).

Når det kommer til forebyggelse, foreslår Loggen og Leukfeldt en oplysningskampagne, pop-ups med advarsler om phishing på søgemaskiner, software til at kontrollere bankansattes aktivitet samt nye måder at fragte kreditkort fra bank til kunde (Loggen & Leukfeldt, 2022: 221-222).

Paraschiv et al. (2021) har lavet en undersøgelse, hvor de præsenterer phishing i en europæisk kontekst. De benytter kvalitative- og kvantitative forskningsmetoder til at undersøge, om der er en sammenhæng mellem en befolknings internetkompetencer samt deres adgang til internet, og hvorvidt disse kompetencer gør, at de er i stand til at identificere phishing-beskeder (Paraschiv et al., 2021: 396).

Resultaterne fra undersøgelsen viser, at phishing er et stigende problem i mange europæiske lande. Dette er på baggrund af digitaliseringen i form af internettet og sociale medier, som har åbnet flere muligheder for svindlerne (Paraschiv et al., 2021: 394). En rapport fra Eurostat viser, at 25% af alle personer i den Europæiske Union har modtaget phishing-beskeder i 2019 (Paraschiv et al., 2021: 396). Danmark er ifølge denne rapport det land, som er hårdest ramt af forsøg på phishing, idet 45% af borgere har meldt, at de har modtaget phishing-beskeder i 2019. Samtidigt har kun 2% af befolkningen aldrig benyttet sig af internettet før (Paraschiv et al., 2021: 396). Nedenstående tabel fra Eurostats føromtalte undersøgelse kommer nærmere ind på korrelationen mellem internetadgang og modtagelsen af phishing-beskeder.

Figur 2: Korrelationen mellem individer som har modtaget phishing-beskeder og individer som aldrig har anvendt internettet.



Kilde: Paraschiv et al., 2021: 398.

Dataen i tabellen baserer sig på befolkningsundersøgelser i de forskellige europæiske lande. Paraschiv et al. påpeger, at det er rimeligt at antage, at disse tal afspejler den generelle befolknings evne til at identificere og opdage et potentiel phishing snarere end det samlede antal af faktiske phishing-angreb registreret i et specifikt land (Paraschiv et al., 2021: 397). De påpeger, at et lands generelle befolknings evne til at identificere potentielle phishing er direkte forbundet med borgernes internetkompetencer og -adgang. Derfor tager Paraschiv et al. i deres

undersøgelse udgangspunkt i ovenstående tabel, som viser den procentvise fordeling af borgere i de forskellige lande, som ikke har benyttet sig af internettet, og kombinerer det med procentfordelingen af individer, som har modtaget phishing-beskeder. Figur 2 viser, at der for Danmark er en negativ korrelation mellem disse to.

Tabellen indikerer en stærk negativ korrelation. Det betyder, at der er en sammenhæng mellem antallet af personer, som identificerer potentielle phishing-angreb, og deres kendskab til internettet. Med andre ord vil lande med en høj opdagelsesrate af phishing have en større tilgængelighed til internettet og dermed en højere internet-kendskab end dem, som ikke har benyttet internettet før eller ikke har adgang hertil (Paraschiv et al., 2021: 398).

3.3 Smishing

Når det kommer til eksisterende forskning om smishing, er omfanget begrænset. De fleste udgivelser om smishing omhandler ”smishing detection” gennem forskellige apps og sikkerhedsmodeller. I det følgende vil vi introducere til to undersøgelser, der omhandler smishing.

Rahman et al. (2022) har lavet en undersøgelse, der vil forklare, hvorfor personer reagerer på smishing-beskeder. Ifølge dem er smishing og phishing stort set det samme, dog foregår smishing over SMS. Ved begge anvendes social engineering. Formålet med SMS’erne er at stjæle personoplysninger og installere malware (Rahman et al., 2022: 49). Forfatterne påpeger, at der anvendes forskellige teknikker til smishing. Her nævner de blandt andet spoofing af telefonnumre og falske navne frem for nummer på afsender (Rahman et al., 2022: 50).

I deres undersøgelse har de designet forskellige smishing-beskeder og sendt dem til 265 personer. De har tildelt beskederne tre forskellige attributter: 1) beskedens afsender, 2) beskedens indhold og 3) ”area code” (numre der starter med 202 = Washington DC) – for at kunne analysere på, hvilke attributter, personer er mest tilbøjelige til at opfatte som valide og dermed reagere på.

Herefter påpeger de, at der findes tre måder at falde for smishing på. Man kan enten 1) klikke på et link i beskeden, 2) svare på beskeden eller 3) ringe tilbage til afsenderen (Rahman et al., 2022: 51). Disse tre måder har forfatterne kunne følge gennem de teknologiske programmer, de har anvendt til undersøgelsen. De udleder, at man enten reagerer på et smishing ud fra frygt (eksempelvis sanktion fra en offentlig myndighed) eller troen om belønning (eksempelvis at man har vundet ting eller penge). De har udsendt smishing-beskeder af to omgange, og de

finder, at der for de to omgange i gennemsnit er 17,6% af de adspurgte, der falder for angrebet. Når det kommer til scenarier, hvor der reageres ud fra frygt, er svarraten 12,96%, mens der for scenarier med troen om belønning er en svarrate på 17,87%. De finder yderligere, at beskedens afsender er af signifikant betydning (Rahman et al., 2022: 54-55).
Personer med størst sandsynlighed for at falde for smishing er: Individer i alderen 45-54 år og personer, der bruger deres mobiltelefon 11-20 timer om ugen. Rahman et al. påpeger, at viden om smishing samt en mekanisme, der automatisk opdager smishing-beskeder, er afgørende for at komme problemet til livs (Rahman et al., 2022: 59).

En undersøgelse af Choi og Lee (2021) kommer ind på, hvordan smishing-teknikker har forandret sig i Sydkorea siden fremkomsten af Covid-19 ved at identificere gerningspersoners modus operandi (Choi & Lee, 2021: 1). Selvom denne undersøgelse er fra Sydkorea, argumenterer vi for, at den kan appliceres i vores undersøgelse, da formålene med begge undersøgelser er at belyse gerningspersonernes modus operandi. Choi og Lee opdeler gerningspersoners generelle modus operandi i følgende 6 faser:

1. *Pre-preparation*
2. *Preparation of smishing attack*
3. *Sending of smishing message*
4. *Downloading of malicious application onto victims' smartphone*
5. *Theft of victims' information and storing it, attempt at financial gain through utilization of attained victims' information*
6. *Charging of transaction/ payments to the victims."* (Choi & Lee, 2021: 1).

I undersøgelsen beskrives smishing som en kriminalitetsform, hvor der benyttes SMS'er til at sprede en 'malicious code' på offerets enhed, således gerningspersoner kan tilgå ofres personlige oplysninger og opnå økonomisk vinding (Choi & Lee, 2021: 1). De tilsendte SMS'er til de potentielle ofre skal fange deres opmærksomhed og lokke dem til at klikke på et link. Når ofrene trykker på linket, vil denne 'malicious application' blive installeret på ofrenes telefon, og herved har gerningspersonen adgang til ofrenes oplysninger. Disse SMS'er fungerer som en form for social engineering, hvor afsenderen udgiver sig for at være en troværdig person eller institution så som en bank (Choi & Lee, 2021: 2). Choi og Lee argumenterer for, at udbredelsen af digitaliseringen er årsagen til, at smishing opstår. De fleste nu til dags bruger telefoner og computere til at tilgå deres banker, hvorfor disse enheder indeholder personlige oplysninger, som kan blive misbrugt (Choi & Lee, 2021: 3).

For at finde ud af, hvilke forandringer der er opstået efter Covid-19, klarlægger Choi og Lee de mest udbredte former for smishing. Disse indebærer falske fragtbeskeder og beskeder, hvor afsenderen udgiver sig for enten at være en institution, virksomhed eller en person (Choi & Lee, 2021: 3). Derudover indeholder disse SMS'er typisk ord eller ting, som er tæt relateret til den generelle befolknings hverdag, hvilket er en af årsagerne til, at det lykkes gerningspersoner at udføre disse angreb (Choi & Lee, 2021: 2). Dette understøtter Choi og Lee ved at påpege, at smishing typisk begås ved, at de kriminelle prøver at: *"lure their victims to click the URL within the SMS by incorporating text that would grab their attention- such as social issues"* (Choi & Lee, 2021: 6).

Choi og Lee tager afsæt i en crime script analysis tilgang til at beskrive, hvordan smishing foregår generelt.

De første to faser består af: *pre-preparation* og *preparation of smishing attack*. I den første fase indsamles ofrenes personlige oplysninger, herunder telefonnumre, som sælges af mæglere på ulovlig vis. I den anden fase køber gerningspersonen 'malicious application' eller får det udviklet af professionelle. I denne fase skal gerningspersoner ligeledes lave en hjemmeside, hvor denne 'malicious application' kan blive uploadet, så gerningspersonen kan få adgang til ofrenes oplysninger (Choi & Lee, 2021: 6).

Efterfølgende omsætter gerningspersonerne deres planlægning til handling. Dette foregår i den tredje fase, hvor smishing-beskeden sendes til potentielle ofre. Beskeden indeholder et link til en hjemmeside, hvori denne 'malicious application' er integreret. SMS'en er essentiel i at fange modtagerens opmærksomhed og indeholder nøgleord som 'delivery', 'finance', 'investegation agency', health check-up' og så videre (Choi & Lee, 2021, 6).

Den fjerde fase opstår, når modtageren trykker på linket. Her vil denne 'malicious application' blive installeret på deres enhed. Gennem en 'malicious code' får afsenderen kontrol over modtagerens enhed. Herefter gemmer den kriminelle de forurettedes personlige oplysninger, som er afslutningen af denne fase (Choi & Lee, 2021: 7).

I den femte fase forsøger gerningspersonen at stjæle finansielle midler fra offeret ved at købe genstande eller kryptovaluta (Choi & Lee, 2021: 7). I denne fase benytter gerningspersonen de oplysninger, som vedkommende har indsamlet i fjerde fase.

En anden måde at udnytte forurettedes oplysninger er gennem den sjette fase. Dette sker gennem overtagelsen af modtagerens verifikationskoder, så gerningspersonen kan udføre transaktioner på spillesider, købe online gavekort eller sælge disse til mæglere. Derudover optages der lån i forurettedes navn for at opnå økonomisk vinding (Choi & Lee, 2021: 7-8).

3.4 Muldyr og hvidvask

I de forrige tre afsnit er der blevet introduceret til eksisterende forskning om vishing, phishing og smishing. Heraf fremgår det, at muldyr hvidvasker de illegitime penge og er en del af den afsluttende handling. I følgende afsnit vil vi uddybe betydningen af muldyr.

Hvidvaskning af penge opfattes som en global trussel, da midlerne, der sløres og hvidvaskes, hovedsageligt kommer fra ulovlige og svigagtige aktiviteter (Vedamanikam & Chethiyar, 2020: 19). Ifølge Vedamanikam og Chethiyar betegnes hvidvask og brugen af muldyr som en økonomisk forbrydelse, hvor de kriminelle forsøger at få udbyttet fra kriminelle handlinger til at se legitime ud (Vedamanikam & Chethiyar, 2020: 20, 24). De belyser, at muldyr deltager i hvidvask-kæden ved at stille deres konto til rådighed, så svindlerne kan bevare deres anonymitet. Muldyrene modtager de illegale penge fra en tredjepart for efterfølgende at hæve pengene eller overføre dem videre til en anden konto. De er dog ikke nødvendigvis en del af det kriminelle netværk (Vedamanikam & Chethiyar, 2020: 24).
Cyberkriminaliteten, herunder vishing og phishing, fylder en del i det malaysiske kriminalitetsbillede. I 2018 udgjorde cyberkriminalitet et tab på 627 mio. danske kroner (Vedamanikam & Chethiyar, 2020: 22). Vedamanikam og Chethiyars pointerer, at størstedelen af muldyrene i Malaysia er unge mennesker, som ikke har forudgående kendskab til kriminalitet. Ifølge Vedamanikam er arbejdsløse, studerende og dem med en desperat økonomisk situation lettere mål for de kriminelle (Vedamanikam & Chethiyar, 2020: 24). Individer mellem alderen 15-44 år ser ud til at være aktive i deltagelsen i muldyrsaktiviteter, hvor personer i alderen 24-34 har den højeste deltagelse (Vedamanikam & Chethiyar, 2020: 24). m

En anden undersøgelse om muldyr af Leukfeldt og Kleemans (2019) kommer ind på, at de illegitime penge, som hvidvaskes gennem muldyr, er penge, som blandt andet stammer fra phishing. Ligesom Vedamanikam og Chethiyar hævder Leukfeldt, at pengesporet til lovovertræderne afbrydes ved, at pengene hæves fra muldyrets konto direkte efter, at pengene er blevet overført til muldyrets konto. Derfor spiller muldyr en vital rolle i de kriminelle netværks crime script, herunder hvidvaskning af penge hvervet fra kriminalitet (Leukfeldt & Kleemans, 2019: 75).
Undersøgelsen er baseret på politiefterforskning, hvor der er blevet taget udgangspunkt i 14 politisager med 211 forhør. Cirka halvdelen af muldyrene er klar over, at de medvirker til

kriminelle aktiviteter. De fleste af muldyrene har begrænsede økonomiske midler eller står uden uddannelse eller arbejde. Ifølge Leukfeldt og Kleemans er denne sårbarhed og negative økonomiske belastning hos muldyrene blevet udnyttet i rekrutteringsprocessen. I 13 ud af de 14 politisager om phishing er muldyrene rekrutteret gennem eksisterende sociale kontakter (Leukfeldt & Kleemans, 2019: 80). Derudover benytter de kriminelle netværk ligeledes jobannoncer til at rekruttere muldyr. Dette gøres gennem websites og e-mails, hvor der ledes efter medarbejdere til en finansiel virksomhed. Disse virksomheder leder efter medarbejdere, som kan stille deres konto til rådighed (Leukfeldt & Kleemans, 2019: 80).
Ydermere kommer Leukfeldt og Kleemans's forskning ind på, hvordan man kan forebygge rekrutteringen af muldyr. De kommer ind på teorien om Situational Crime Prevention og kommer med to strategier. Den første handler om, at man skal reducere provokationerne, der fører til kriminel adfærd. Her handler det primært om at reducere gruppepres og efterligningen af andres adfærd. Analysen viser, at sociale bånd og gruppepres er to faktorer, som er essentielle i rekrutteringsprocessen. Den anden strategi handler om at fjerne undskyldninger for kriminel adfærd, hvor man gør muldyrene klar over den kriminelle handling i at stille deres konto til rådighed. Ud fra disse to forebyggelsesstrategier hævder forfatterne, at oplysningskampagner målrettet potentielle muldyr kan udvikles. Muldyrene skal være klar over, at de samarbejder med de kriminelle, som stjæler penge fra uskyldige mennesker (Leukfeldt & Kleemans, 2019: 86).

Yderligere har Leukfeldt og Jansen (2015) lavet forskning i, hvordan cyberkriminelle bruger muldyr. Ud fra eksisterende forskning om cyberkriminelle grupper skelnes der mellem to grupper af cyberkriminelle, herunder low-tech og high-tech grupper (Leukfeldt & Jansen, 2015: 173). Sigtet med Leukfeldt og Jansens undersøgelse er at belyse, hvordan muldyr benyttes i disse low-tech og high-tech cyberkriminelle grupper (Leukfeldt & Jansen, 2015: 177).
Low-tech netværk er ifølge den eksisterende forskning dem, som benytter mindst muligt af informationsteknologien i deres crime scripts (Leukfeldt & Jansen, 2015: 175). Disse low-tech kriminelle netværk benytter phishing-mails og falske hjemmesider til at få offerets loginoplysninger. Den anden gruppe, high-tech kriminelle netværk, benytter malware, hvor der ikke kræves direkte interaktion med offeret (Leukfeldt & Jansen, 2015: 175). I disse tilfælde får de kriminelle netværk kontrol over offerets computer gennem malware, hvilket betyder, at de har adgang til offerets netbank og andre personlige oplysninger (Leukfeldt & Jansen, 2015: 175).

Ifølge denne undersøgelse kan det hollandske cyberkriminelle netværk, der begår phishing, identificeres i fire hierarkiske positioner: Kernemedlemmer, professionelle katalysatorer, rekrutterede katalysatorer og muldyr. Muldyr findes i bunden af den hierarkiske struktur af de cyberkriminelle netværk. Denne gruppe bruges af kernemedlemmer eller katalysatorer til at sløre det økonomiske spor, som kan lede til det kriminelle netværk (Leukfeldt & Jansen, 2015: 175).

Resultatet fra deres forskning viser, at der er en markant forskel på muldyr, som bliver benyttet i low-tech angreb sammenlignet med dem i high-tech angreb. Den største forskel kan blive observeret ved omfanget af transaktioner, som er blevet foretaget fra et offers bankkonto til et muldyrs. Ud fra undersøgelsens data, som består af bankdata fra en Hollandsk bank, bliver flere penge stjålet ved et low-tech angreb end ved high-tech angreb. Dertil bliver flere muldyr brugt pr. angreb ved low-tech, og summen af penge, som bliver overført til muldyr ved low-tech angreb, er højere (Leukfeldt & Jansen, 2015: 181).

Endvidere viser undersøgelsen, at 44% af muldyrene ved low-tech angreb er mellem alderen 18-24 år og har en privat bankkonto i Holland. Dette er anderledes ved high-tech angreb, hvor 38,1% af muldyrene er i alderen 24-35 år og typisk har en udenlandsk bankkonto.

3.5 Opsummering

Ovenstående kapitel har givet et indblik i den eksisterende forskning, der findes om henholdsvis vishing, phishing, smishing og muldyr.

Den overvejende data i undersøgelserne bygger på interviews og data fra myndigheder, herunder politidata og filer fra retssager. Fælles for flere af studierne er, at de anvender crime scripts til at forklare deres fund. I syv af de tolv inkluderede undersøgelser finder forskeren/ forskerne frem til en decideret crime script eller 'modus operandi' for vishing, phishing og smishing. Fire af undersøgelserne forklarer deres fund ved at anvende Situational Crime Prevention, mens yderligere fire anvender Cohen og Felsons rutineaktivitetsteori.

I arbejdet med at finde eksisterende forskning er det bemærkelsesværdigt, at der i en dansk kontekst findes vejledninger til at undgå vishing, phishing og smishing (primært for virksomheder), mens selve undersøgelsen af, hvordan vishing, phishing og smishing foregår i Danmark er mangelfuld. Denne undersøgelse har til hensigt at belyse dette.

Kapitel 4

Teori

4. Teori

I dette kapitel præsenteres den teoretiske ramme for undersøgelsen. Vi gør brug af Cohen og Felsons Routine Activity Theory (rutineaktivitetsteori),

I 1979 præsenterede Lawrence E. Cohen og Marcus Felson et essentielt social paradoks til at analysere kriminalitetstendenser i USA (Cohen & Felson, 1979: 588). Rutineaktivitetsteorien var atypisk i forhold til tiden, den blev udviklet i, da den ikke fokuserede på karakteristika ved forbrydere. Tværtimod fokuserede denne tilgang på at forklare de omstændigheder, der leder til kriminalitet (Cohen & Felson, 1979: 588).
Rutineaktivitetsteorien blev dermed brugt til at forklare hvorfor og hvordan kriminelle handlinger udføres. Cohen og Felson påpeger i teorien, at sociale strukturelle forandringer i menneskets rutiner påvirker kriminalitetstendenser, som forårsager at nye kriminalitetsmuligheder opstår for potentielle gerningspersoner (Cohen & Felson, 1979: 589). Disse strukturelle forandringer i individets rutineaktivitetsmønstre kan påvirke kriminaliteten gennem konvergens i tid og rum ud fra følgende tre elementer:

1. Motiverede forbrydere
2. Egnede mål
3. Fravær af egnede beskyttere

Rutineaktivitetsteorien forklarer kriminalitet ud fra ovenstående tre elementer. Det vil sige, at enhver kriminel handling som udgangspunkt kræver en motiveret forbryder, som er tilbøjelig og har evner til at udføre den kriminelle handling (Cohen & Felson, 1979: 590). Før den motiverede forbryder kan udføre en kriminel handling, kræver det, at der er nogle egnede mål i form af et passende offer for den kriminelle handling. Derudover vil fraværet af en egnet beskytter, som kan forhindre den kriminelle handling, være udslagsgivende for, at kriminaliteten udspiller sig (Cohen & Felson, 1979: 590). Det er gennem individets strukturelle ændringer i rutineaktiviteten og samspillet af disse tre elementer, at kriminalitet kan opstå (Cohen & Felson, 1979: 589). Derved vil manglen af nogle af disse tre elementer være tilstrækkelige til at forhindre kriminalitet (Cohen & Felson, 1979: 590).

Yderligere kommer Cohen og Felson ind på, at hverdagsrutiner så som arbejde, skole og fritidsaktiviteter er centrale i beskrivelsen af kriminalitet (Cohen & Felson, 1979: 591). Årsagen til dette er, at man gennem disse aktiviteter separerer sig fra dem, man stoler på, og

ens hjem. I forlængelse af det påpeger Cohen og Felson, at man har større sandsynlighed for at blive offer for kriminalitet, når man er udenfor hjemmet. Dette vil sige, at mennesker som primært er hjemme har en lavere risiko for at blive udsat sammenlignet med dem i offentligheden (Cohen & Felson, 1979: 596). Disse rutineaktiviteter defineres som fremherskende aktiviteter, som skal sørge for individets grundlæggende behov. Dette kan være rutineaktiviteter i form af arbejde, mad, husly, social interaktion og læring, som både kan forekomme i hjemmet og udenfor hjemmet (Cohen & Felson 1979: 593). De sociale strukturer i form af rutineaktiviteter har en påvirkning på kriminaliteten (Cohen & Felson, 1979: 593-594). Ændringer i menneskets rutineaktiviteter kan dermed øge sandsynligheden for, at motiverede forbrydere konvergerer i tid og rum med egnede mål og fraværet af egnede beskyttere (Cohen & Felson, 1979: 593).

Ifølge Cohen og Felson vil de motiverede forbrydere altid være til stede. Derfor er det relevant med denne teori at nedbryde faktorer i hverdagen, som kan skabe et opportunt øjeblik for de motiverede forbrydere. Dermed udgør de egnede mål og fraværet af egne beskyttere kernen i forebyggelsen af den kriminelle handling (Cohen & Felson, 2022: 467). Disse to faktorer påvirker forekomsten af kriminalitet, hvorfor vi vil anvende denne teori til at undersøge, hvilke processer gennem interaktion med egnede mål muliggør vishing, phishing og smishing. Fra de motiverede forbryderes perspektiv handler det i høj grad om at kigge på menneskers følelsesmæssige behov, hverdagsrutiner og mønstre, som kan hjælpe motiverede forbrydere med at udføre den kriminelle handling (Cohen & Felson, 1979: 592). Ud fra et vishing-, phishing- og smishing-perspektiv formodes der, at det i høj grad handler om at finde egnede mål, der gennem social engineering videregiver personfølsomme oplysninger, som kan misbruges. Dette vil vi uddybe nærmere i vores crime script analysis af disse it-relaterede angreb (afsnit 5.1).

4.1 Teoretisk refleksion af rutineaktivitetsteorien

Grundlæggende blev denne teori anvendt til at analysere kriminalitetsformer i en fysisk kontekst (Cohen & Felson, 1979: 589). Dette bærer præg af, at rutineaktivitetsteorien er en del af det kriminologiske teoretiske paradigme, der betegnes som environmental criminology. Inden for environmental criminology findes der andre teorier, så som Rational Choice Theory og Situational Crime Prevention, som sigter efter at undersøge og forklare kriminalitet ud fra geografiske faktorer (Chamard, 2011: 2). Ud fra et teoretisk perspektiv og teoriens paradigme kan det være uhensigtsmæssigt at benytte rutineaktivitetsteorien til at analysere kriminalitet

ved ikke-fysiske miljøer, da teorien hovedsageligt fokuserer på kriminalitet i det fysiske miljø. Hermed kan et argument være, at det ville være problematisk at anvende rutineaktivitetsteorien til at analysere it-relaterede kriminalitet, da disse kriminelle handlinger typisk udspiller sig i situationer, hvor hverken gerningspersoner eller ofre befinder sig det samme sted fysisk.
Tværtimod er det også vigtigt at påpege, at rutineaktivitetsteorien er fra 1979, hvilket kan være en forklaring på, hvorfor den udelukkende fokuserer på kriminalitet i det fysiske miljø. Som tidligere nævnt fokuserer teorien på menneskets hverdagsrutiner, og hvis man kigger tilbage på tiden, hvor teorien blev udviklet, kan der argumenteres for, at internettets udbredelse dengang ikke var lige så normaliseret og dominerende som i dag. Den menneskelige rutineaktivitet har bevæget sig i et bredere spektrum, hvor digitaliseringen har muliggjort, at man kan kommunikere på sociale medier på kryds og tværs mellem tid og rum. Det vil sige, at de menneskelige rutiner ligeledes foregår i den digitale verden, som de optræder i den fysiske. Den teknologiske udvikling har muliggjort, at man kan tjekke sin netbank på telefonen eller interagere med andre gennem diverse kommunikationsplatforme. Ud fra ovenstående påpeges det, at en stor del af menneskets rutineaktiviteter og sociale strukturer er flyttet til digitale kanaler. Dette betyder også, at der opstår flere muligheder for potentielle gerningspersoner for at begå it-relaterede kriminalitet, idet brugen af internettet er mere normaliseret i dag sammenlignet med dengang, teorien blev udviklet. Selvom teorien oprindeligt blev udviklet til at undersøge kriminalitet i fysiske miljøer, betyder det ikke, at den skal afgrænses til fysiske lokationer. Yderligere understøtter den eksisterende forskning inden for vishing, phishing og smishing brugen af rutineaktivitetsteorien. Fire ud af de ti undersøgelser i vores gennemgang af litteraturen benytter rutineaktivitetsteorien. Dertil kan der argumenteres for, at teorien kan anvendes til at analysere kriminelle handlinger i ikke-fysiske miljøer, selvom rutineaktivitetsteorien ud fra et teoretisk perspektiv udelukker dette.

Kapitel 5

Metode

5. Metode

I dette kapitel introduceres de metodiske overvejelser og fremgangsmåder, vi har gjort os i løbet af undersøgelsen. Først præsenteres undersøgelsens metodiske ramme, der tager afsæt i crime script analysis. Efterfølgende introduceres dokumentanalysen, hvor vi beskriver anvendelsen heraf på nogle cases. Slutteligt anvender vi Kvale og Brinkmanns (2015) syv faser til at beskrive, hvordan vi har indsamlet empirisk interviewmateriale samt databehandlingen heraf.

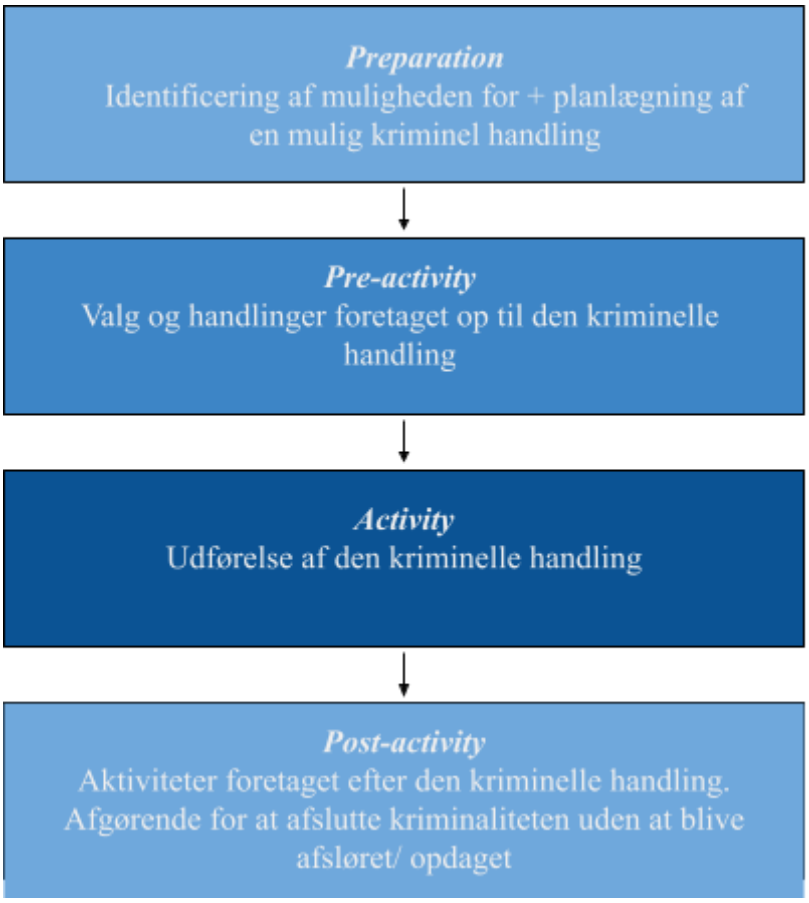
5.1 Metodisk ramme – Crime script analysis

Crime script analysis er en metode, som anvendes inden for kriminologien til at forstå og analysere kriminel adfærd. Script metoden stammer fra kognitiv psykologi, hvor metoden oprindeligt blev anvendt til at forstå menneskelig adfærd og handlinger samt de mentale processer, der organiserer individets viden i specifikke situationer (Keatley, 2018: 127). Mere specifikt bliver scripts beskrevet som hændelsessekvenser, som opsummerer grundlæggende handlinger, som kan være udført på forskellige måder og sammenhænge. I disse scripts indgår forskellige scener, hvor menneskelige handlinger og rutiner udspiller sig i den specifikke situation. Det kan eksempelvis være en restaurant script, hvor der er nogle faste handlingsmønstre og rutiner, som man typisk indordner sig efter i form af: entering, ordering, eating og exiting, som udgør de forskellige scener i den givne handling og script (Cornish, 1994: 158). Disse scripts er indlejret i individets hukommelse, hvorfor nogle daglige handlinger, rutiner eller modus operandi er standardiseret gennem individets viden og erfaring fra andre lignende episoder (Cornish, 1994: 158).

Crime script analysis betragtes inden for kriminologien som videnstrukturer, der klarlægger og organiserer gerningspersonens beslutninger og handlinger i sekventielle stadier (Chainey & Berbotto, 2021: 272-273). Metoden blev introduceret af Cornish i 1993, der med udgangspunkt i den kognitive psykologi videreudviklede script-metoden til at beskrive kriminelle begivenheder. Cornish opstillede nogle scener, som var organiseret i facetter og beslutningsstrukturer, hvor formålet med scenerne var, at de skulle forklare, hvordan kriminelle handlinger kunne udføres og planlægges (Chainey & Berbotto, 2021: 273). For at udforme et crime script tages der oftest udgangspunkt i et universelt script bestående af 9 faser: *Preparation, entry, precondition, instrumental precondition, instrumental initiation, instrumental actualization, doing, postcondition* og *exit* (Cornish, 1993: 40). Indtil 2010 har

brugen af crime script-metoden været begrænset, idet flere forskere argumenterede for, at metoden til at konstruere disse scripts krævede klarhed, processer til kontrol af datavaliditet og en forenkling (Chainey & Berbotto, 2021: 273). Dermed mente Thompson og Chainey, at Cornish's oprindelige metode kunne simplificeres, således man skabte en praksisorienteret crime script analysis uden at tilsidesætte de konceptuelle tanker i Cornish's oprindelige crime script (Chainey & Berbotto, 2021: 273). Thompsens og Chaineys tilgang til crime script analysis indebærer konceptuelle tanker fra Cornish's oprindelige tilgang, hvor der tages afsæt i gerningspersoners handlingssekvenser i form af scener. Disse scener er essentielle stadier i kriminalitetsprocessen (Chainey & Berbotto, 2021: 277). Mere specifikt skal disse scener forstås som omgivelser, hvori den kriminelle handling opstår, og kan inddeles i fire stadier*: preparation, pre-activity, activity* og *post-activity* (Chainey & Berbotto, 2021: 277).

Figur 3: De fire stadier i crime script analysis



Kilde: Eget arbejde

De første to faser *preparation* og *pre-activity* omfatter forberedelsen af den kriminelle handling. Mere specifikt belyser *preparation* identificeringen af en mulighed for at begå en forbrydelse og selveste planlægningen, hvorimod *pre-activity* består af de umiddelbare valg og handlinger, som foretages op til udførelsen af den kriminelle handling (Chainey & Berbotto, 2021: 282). Handlinger i dette stadie er nødvendige for, at selve den kriminelle handling (*activity*) kan udspille sig (Keatley, 2018: 130). Det sidste stadie i form af *post-activity* består af de aktiviteter, som foregår efter den kriminelle handling. Disse aktiviteter indebærer de nødvendige stadier for at afslutte den kriminelle handling uden at blive opdaget (Keatley, 2018: 130).

Inden for kriminologien kan script-metoden benyttes som et analytisk værktøj til at forstå adfærdsmæssige rutiner og rationelle handlinger (Cornish, 1994: 159). Da script-metoden fokuserer på at organisere specifikke handlinger i forskellige situationer, er metoden brugbar til at analysere kriminalitetsforhold, hvor individets beslutningsproces udgør en betydelig faktor i deres adfærdsprocesser (Cornish, 1994: 159). Som tidligere nævnt kan scripts opdeles i scener, hvor hver scene udgør handlingsenheder for at opnå målet. Dette kan perspektiveres til kriminelle handlinger så som vishing, phishing og smishing, hvor individets beslutningsproces spiller en stor rolle i gennemførelsen af disse it-relaterede angreb. I denne undersøgelse anvendes crime script analysis som et analytisk værktøj til at undersøge gerningspersoners processer i vishing, phishing og smishing. Crime script analysis vil blive brugt til at forklare, hvordan gerningspersoner gennem disse fire stadier lykkes at manipulere ofre til at videregive personfølsomme oplysninger, som kan blive misbrugt til at franarre dem økonomisk. Dertil vil disse fire stadier danne fundamentet for vores analyse, hvorfor disse fire stadier ligeledes vil danne fundament for specialets interviewguide og kodning.

Crime script tilgangen lægger op til, at man kan bruge forskellige typer af materiale. Det handler i høj grad i crime script om, at de forskellige typer af data skal give et indblik i de forskellige stadier ved en given kriminalitetsform.

Det datamateriale, som vi har anvendt til at belyse vishing, phishing og smishing, består af i alt fem skriftlige og fysiske interviews af fagprofessionelle fra Sydbank og Fyns Politi. Derudover har vi fået udleveret fire cases fra Sydbank om tidligere vishing- og smishing-sager, som er primærdata, hvor forurettede beskriver hændelsesforløbet op til, midt i og efter den kriminelle handling. Vores empiriske fund og den eksisterende forskning skal være med til at belyse og understøtte vores crime script tilgang.

5.2 Dokumentanalyse af de fire cases fra Sydbank

En udfordring i akademisk arbejde og dataindsamling kan være at skaffe troværdige data. Dokumentanalysen er et vigtigt bidrag hertil, da det fungerer som en mere diskret tilgang. Afstanden til begivenhederne og fraværet af interaktionen mellem forsker og forskningsobjekt gør, at metoden er velegnet til kriminologiske analyser (Møller, 2018: 201). Dokumentanalysen er et bredt fænomen og karakteriseres som en kombination af materialer og metoder. Formålet med denne metode er at finde og analysere fænomener i det allerede eksisterende materiale (Møller, 2018: 201). Dette materiale kan være hvilken som helst arkiveret information, som indeholder viden om et bestemt fænomen. I nærværende undersøgelse tager vi udgangspunkt i fire cases fra Sydbank, som består af ofres egne beskrivelser af, hvordan de har oplevet vishing og smishing.

Dokumentanalysen skal være med til at understøtte vores crime script tilgang, så vi kan få et indblik i svindlernes fremgangsmåder. På denne måde skal inddragelsen af de 4 cases fra Sydbank medvirke til, at vi tilegner os en bedre forståelse af, hvordan vishing og smishing udfolder sig, og hvilke faktorer der er involveret i processen. Ifølge Møller (2018) kan dokumentanalysen indeholde både kvalitative og kvantitative data af mere eller mindre officiel karakter i form af sekundært data, hvilket kan sætte spørgsmålstegn ved kildernes troværdighed (Møller, 2018: 201-202). Denne mulige problematik har vi forsøgt at imødekomme ved at benytte os af primær data, som i forvejen ikke er bearbejdet. På denne måde sikrer vi, at dokumenterne ikke er manipuleret (Møller, 2018: 202), hvilket betyder, at vi kan få et reelt billede af, hvordan disse it-relaterede angreb foregår, samt hvilke fremgangsmåder svindleren benytter sig af i manipulationen af offeret.

I de fire cases kommer ofrene med detaljerede beskrivelser af hændelsesforløbet op til den kriminelle handling. Tre af sagerne handler om smishing, og én omhandler vishing. Disse beskrivelser har ofrene selv udarbejdet, og dermed har Sydbank ikke været involveret i processen. Dokumenterne fra de fire cases består af tekstindhold, hvor ofrene forklarer hændelsesforløbet, samt hvordan de oplever situationen. Derudover består to af sagerne også af skærmbilleder fra samtalen med svindleren. Disse skærmbilleder er inkluderet i vores analyse i en udgave, som vi selv har udarbejdet og tilføjet diverse anonymiseringer af – eksempelvis navne og postnumre, der indgår i materialet. Dette er for at imødekomme GDPR-reglerne om anvendelse af tredjepersonsoplysninger (Kontraktenheden på AAU, u.å.: pkt. 8).

5.3 Dataindsamling

Denne undersøgelse tager udgangspunkt i Kvale og Brinkmanns syv faser af en interviewundersøgelse (Kvale & Brinkmann, 2015: 151). Med udgangspunkt i de indsamlede interviews benyttes disse syv faser til at forklare vores metodiske fremgangsmåde i undersøgelsen. I følgende tabel uddybes fremgangsmåden.

Tabel 2: Undersøgelsens metodiske fremgangsmåde beskrevet i syv faser

Fase 1: *Tematisering* Afklaring af forskningsfeltet gennem eksisterende forskning og talopgørelser.
Fase 2: *Design* Planlægning af dataindsamling; herunder ● Det semistrukturerede interview ● Udarbejdelse af interviewguide ● Valg af interviewpersoner
Fase 3: *Interview* Gennemførelse af interviews med en varighed på cirka 40 minutter. ● Introduktion af interviewpersoner ● Beskrivelse af interviewsituation
Fase 4: *Transskription* Databehandling; herunder ● Transskription af datamateriale
Fase 5: Databehandling; herunder ● Kodning ud fra kodeliste
Fase 6: *Verifikation* Validering af undersøgelse; herunder ● Reliabilitet ● Intern validitet ● Ekstern validitet

Fase 7: *Rapportering*

Præsentation af etiske overvejelser; herunder

- Samtykke
- Fortrolighed
- Konsekvenser

Fase 1: Tematisering

Tematiseringen af en interviewundersøgelse vedrører formuleringen af forskningsspørgsmål og en teoretisk afklaring af det undersøgte tema (Kvale & Brinkmann, 2015: 157). De centrale spørgsmål i forbindelse med tematiseringen handler om interviewets *hvorfor, hvad* og *hvordan.* Det er vigtigt i denne fase at klarlægge undersøgelsens formål og tilegne sig viden omkring det pågældende emne.

I vores undersøgelse ønsker vi at finde frem til de forskellige stadier i vishing, phishing og smishing set ud fra en dansk kontekst. I undersøgelsens opstartsfase havde vi begrænset viden om forskningsområdet. Det har været nødvendigt med en tematisering af undersøgelsen. Her har vi fået en afklaring og viden (et svar på *hvordan*) gennem vores problemfelt og kapitel om eksisterende forskning. Derudover har vi i forbindelse med gennemgangen af den eksisterende forskning fundet det relevant at inddrage rutineaktivitetsteorien i nærværende undersøgelse til at belyse gerningspersoners fremgangsmåder. Gennemgangen har givet os indblik i, hvad vishing, phishing og smishing indebærer, samt hvad omfanget heraf er på et nationalt og globalt plan. Derudover viser det os, hvad der endnu mangler at blive forsket i angående vishing, phishing og smishing og dermed er relevant for os at undersøge. Dette har ledt videre til spørgsmålet om, *hvordan* vi vil undersøge (fase to).

Fase 2: Design

Designet af et interview indebærer planlægningen af procedurer og teknikker. Ifølge Kvale og Brinkmann spørger man i denne fase ind til undersøgelsens 'hvordan' (Kvale & Brinkmann, 2015: 162). Denne fase er inspireret af vores tematisering, hvilket betyder, at planlægningen af designet skal afspejle undersøgelsens formål.

Det semistrukturerede interview

Til indhentning af data benytter vi det semistrukturerede interview, der kendetegnes som et interview, hvis formål er at indhente detaljerede beskrivelser af den interviewedes erfaringer (Kvale & Brinkmann, 2015: 22). I nærværende undersøgelse anvender vi denne metode for at tilegne os viden om vishing, phishing og smishing, så vi kan udarbejde en detaljeret beskrivelse og analyse af gerningspersoners modus operandi gennem vores crime script tilgang. Som et kendetegn af det semistrukturerede interview og en del af vores designproces har vi udarbejdet en interviewguide bestående af tematikker og spørgsmål, som er forberedt på forhånd. Selvom vores interviewguide består af fastsatte spørgsmål, muliggør denne form for interview at stille opfølgende spørgsmål til respondenternes udsagn (Brinkmann & Tanggaard, 2010: 38). Der har således været plads til ændringer undervejs i interviewet. Ændringerne kan være nye indsigter eller relevante temaer, som eksempelvis kommer fra vores respondenter (Kvale & Brinkmann, 2015: 49).

Interviewguide

Som en del af designprocessen har vi udarbejdet en interviewguide, der fungerer som interviewets omdrejningspunkt. En interviewguide er et manuskript, som strukturerer interviewforløbet. Denne interviewguide indeholder nogle emner, som skal afdækkes, men i et semistruktureret interview er rækkefølgen for gennemgang af spørgsmålene ikke fastlåst. Som følge af den semistrukturerede tilgang indeholder vores interviewguide en oversigt af forudbestemte temaer og relevante spørgsmål, som kan belyse disse (Kvale & Brinkmann, 2015: 185).

Spørgsmålene i vores interviewguide er primært faktuelle, da vi ønsker at producere viden om vishing, phishing og smishing frem for relationer til vores interviewperson (Kvale & Brinkmann, 2015: 185 ff). Da vi arbejder tematisk for at indhente viden og data, tager vores videnskabsteoretiske ståsted afsæt i en realistisk tilgang, hvorfor vores interviewpersoner alle er fagprofessionelle inden for databedrageri - herunder vishing, phishing og smishing.

Ud fra tematiseringen har vi i vores interviewguide på forhånd opstillet nogle temaer ud fra rutineaktivitetsteorien og ud fra vores viden fra den eksisterende forskning. Herefter har vi formuleret forskningsspørgsmål med dertilhørende interviewspørgsmål (Hansen, Andersen & Hansen, 2020: 78; Kvale & Brinkmann, 2015: 187). De temaer, vi har spurgt ind til, består af følgende:

- Introduktion og jobbeskrivelse
- Indhold i forbrydelserne
- Gerningspersonerne
- Ofrene
- Muldyr
- Samarbejde med banker
- Crime script

Forskningsspørgsmålene til disse temaer omfatter blandt andet gerningspersoners modus operandi, hvor vi har stillet interviewspørgsmål med fokus på tendenser inden for vishing, phishing og smishing og bedt vores respondenter uddybe forløbene bag disse databedragerityper. Et eksempel på sådan et spørgsmål er: "*Hvilke tendenser ses inden for vishing/ phishing / smishing i forhold til, hvad gerningspersonen siger for at manipulere offeret?"*. Formålet med dette spørgsmål er at få belyst, hvordan gerningspersoner lykkes med at snyde offeret. Ud fra den eksisterende forskning havde vi en idé om, at gerningspersoner udgiver sig for at være en bank eller politiet. Dermed har dette spørgsmål fokus på, hvilke teknikker eller fremgangsmåder der bruges, og hvordan manipulationen lykkes gennem disse fremgangsmåder.

Ydermere har vi spurgt mere konkret ind til den planlægning og forberedelse, gerningspersonerne skal foretage sig. Spørgsmålene hertil tager udgangspunkt i vores overvejelser og viden om crime script tilgangen. I forbindelse med det har vi eksempelvis spurgt ind til: "*Hvilken planlægning og forberedelse kræves for at udføre disse angreb?"* og "*Hvordan vinder gerningspersonen offerets tillid?"*. I og med at crime script tilgangen fungerer som undersøgelsens ramme, er det vigtigt for os at have data på de forskellige stadier. I den eksisterende forskning har der været en begrænset viden omkring, hvordan gerningspersoner planlægger og forbereder deres it-relaterede angreb, hvorfor vi finder det relevant at spørge ind til dette. Dertil er et andet element i form af tillid vigtigt, da dette ligeledes er med til at sige noget om gerningspersonens modus operandi ved disse angreb. Samtlige forsknings- og interviewspørgsmål kan findes i de forskellige interviewguides i bilag 5.

Adgang til interviewpersoner og selektion

I nærværende undersøgelse har vi indgået et specialesamarbejde med Sydbank og Fyns Politi. Det blev muligt at etablere et samarbejde med begge parter, da vi i vores projektorienterede forløb var hos henholdsvis Sydbank og Fyns Politi. Gennem vores specialesamarbejde har vi

fået adgang til dokumenter (cases) fra sager om vishing og smishing, hvor forurettede kommer med sine egne beskrivelser om angrebet. Dertil har vi gennem specialesamarbejdet fået mulighed for at foretage nogle skriftlige og mundtlige interviews med de fagprofessionelle i Sydbank og Fyns Politi, hvilket vil blive uddybet i et senere afsnit.

Gennem dette samarbejde har vi haft en kontaktperson i både Sydbank og Fyns Politi, hvor alt korrespondancen er foregået. Det er også gennem disse kontaktpersoner, at vi har fået adgang til vores interviewpersoner og de fire cases i Sydbank. Der kan argumenteres for, at der er mulighed for bias, idet de udvalgte respondenter kan være valgt på baggrund af en personlig vurdering fra vores gatekeepers (kontaktpersonerne) (Hansen, Andersen & Hansen, 2020: 206). Det vil sige, at vores kontaktpersoner har haft indflydelse på udvælgelsen af respondenterne, hvilket betyder, at de andre medarbejdere fra Sydbank og Fyns Politi muligvis ikke har haft mulighed for at blive inkluderet i udvælgelsen. Dette kan skabe en sampling-bias, som gør, at det er bestemte typer inden for de nævnte organisationer, der bliver valgt som interviewpersoner (Bryman, 2012: 187). Et aspekt af frivillig deltagelse, som er vigtigt at have in mente, er, at personer, som giver samtykke til at blive involveret i interviews, kan være anderledes i forhold til dem, som fravælger deltagelse. På denne måde kan der være selv-selektionsbias, idet interviewpersonerne har givet samtykke til frivillig deltagelse, og kontaktpersonerne har stået for udvælgelsen af respondenter (Robinson, 2013: 35).
For at undgå denne problematik og mulige skævheder i dataen fortalte vi vores kontaktpersoner over mailkorrespondance, at vi søgte efter interviewpersoner, som havde erfaringer inden for vishing, phishing og smishing, således at vi kunne få belyst problemformuleringen. Derudover er det værd at nævne, at både Sydbank og Fyns Politi på tidspunktet for interviewene havde travlt i afdelingerne med sagsbehandling af it-kriminalitet, hvorfor det kan være muligt, at udvælgelsen af respondenterne har været spontant og udvalgt efter dem, som havde tid. Dette vides ikke men er blot nogle overvejelser i forhold til den mulige selv-selektionsbias i vores sampling.

Fase 3: Interview

Kvale og Brinkmanns tredje fase omhandler interview (Kvale & Brinkmann, 2015: 188). I dette afsnit vil vi præsentere vores interviewpersoner samt gennemgå forløbet for de tre interviews.

Interviewpersoner

I vores undersøgelse har vi haft fem respondenter. Tre af dem har deltaget i fysiske interviews, mens to har besvaret vores interviewguide skriftligt.

Vores to respondenter fra Sydbank er begge ansat som 'fraud-specialister' (svindel-specialister) i fraud-afdelingen i Sydbank. Afdelingen er opdelt i 'kortmisbrug' og 'netbankmisbrug', og begge af vores respondenter arbejder med sidstnævnte. Deres arbejdsopgaver omfatter blandt andet at lave betalingsovervågning, analyse og statistik, forebyggelse, politianmeldelser og kundekontakt.

I Sydbank er der udført ét semistruktureret interview med en ansat i fraud-afdelingen (Bilag 7), og én har besvaret vores interviewguide skriftligt (Bilag 10). Sidstnævnte har været nødvendigt, da der grundet travlhed i afdelingen ikke kunne findes tid til flere interviews. Derudover har Sydbank givet os indblik i fire cases med vishing og smishing, og vi har desuden haft mulighed for at stille opfølgende spørgsmål til vores interviewperson.

Givet deres stilling som 'fraud-specialister' er begge vores respondenter fagprofessionelle, der dagligt sidder og behandler sager omhandlende vishing, phishing og smishing. Deres kendskab til området er bredt, og vi finder det derfor relevant at inddrage disse personer i vores undersøgelse, da de har bidraget til ny og uddybende viden til undersøgelsens forskningsområde.

Vores tre respondenter fra Fyns Politi er politibetjente, der er ansat i afdelingen for økonomisk kriminalitet. Deres arbejdsopgaver omfatter blandt andet drift, visitation af sager (prioriteringer af sager), indledende efterforskning og relevansvurdering af sager.

Hos Fyns Politi er der udført to semistrukturerede interviews med ansatte i afdelingen for økonomisk kriminalitet (Bilag 8 og 9). Yderligere har én besvaret interviewguiden skriftligt (Bilag 11).

Som ansat i afdelingen for økonomisk kriminalitet beskæftiger vores respondenter sig både med bedrageri og databedrageri, § 279 og §279a i Straffeloven. Databedrageri dækker over flere former for økonomisk kriminalitet udover vishing, phishing og smishing, men disse tre databedragerityper er dog en stor del af det område, som vores respondenter beskæftiger sig med. Deres viden om vishing, phishing og smishing gør dem til oplagte fagprofessionelle, der kan berige os med viden inden for forskningsområdet.

Tabel 3: Oversigt over empirisk materiale

	SYDBANK	FYNS POLITI
Interviews	1	2
Skriftlige interviews	1	1
Andet data	Dokumenter om fire tidligere cases omhandlende vishing og smishing.	

Interviewsituationen

I det følgende præsenteres vores besøg hos Sydbank og Fyns Politi, og herunder beskrives forløbene af de tre interviews.

Forud for interviewet i Sydbank fik vi udleveret de 4 cases og gennemgik dem. Vi blev introduceret til de øvrige ansatte i afdelingen. Efterfølgende fik vi en rundvisning i banken. Hos Fyns Politi havde vi en forudgående samtale med en politikommissær på cirka 20 minutter, hvor vi blev introduceret til politiets arbejde med bedrageri og databedrageri og hørte politikommissærens egne erfaringer med området. Samtidigt fik vi talt om, hvordan vores undersøgelse kan gavne politiets arbejde fremadrettet.

Til udførelsen af vores interviews har begge forfattere af undersøgelsen ageret interviewer. Det betyder, at vi ved hvert interview har været to om at stille spørgsmål til vores respondent. Dette er gjort, da vi på den måde har haft mulighed for at supplere hinanden. Under interviewene blev dette især relevant, da vi hver har stillet forskellige opfølgende spørgsmål til vores respondenters udtalelser, der ellers ikke var blevet inkluderet, hvis vi kun havde været én interviewer. Det er vores opfattelse, at vores respondenter ligeledes har set dette som en fordel.

De tre interviews er foretaget med én respondent af gangen og har hver haft en varighed på mellem 30 og 45 minutter. Vores interviewguide blev efter ønske sendt til vores kontaktpersoner i Sydbank og Fyns Politi. Hos Sydbank var formålet, at vores kontaktperson i banken ønskede at finde de mest egnede interviewpersoner til os. Hos Fyns Politi var der i første omgang ikke tid til interviews, hvorfor vores interviewguide blev sendt ud til forskellige

medarbejdere til besvarelse. Efterfølgende blev det dog muligt at interviewe to personer, som blev udvalgt af føromtalte politikommissær. Her er der igen mulighed for, at respondenterne er valgt ud fra en præference hos politikommissæren. Det kan dog også være tilfældet, at de to respondenter var dem, der havde tid og lyst til at deltage. Det betyder, at respondenterne havde mulighed for at læse vores interviewguide forud for selve interviewet. Vi anser dette som en fordel, da respondenterne således har haft mulighed for at forberede sig på interviewet – blandt andet med at finde konkrete eksempler fra tidligere sager. Samtidigt vil vi dog påpege, at adgang til spørgsmålene forud for interviewene kan have betydet, at vores respondenter har diskuteret spørgsmålene på forhånd, hvorfor nogle svar lyder ens. I følgende tabel ses en beskrivelse af vores empiriske materiale.

Tabel 4: Beskrivelse af empirisk materiale

INTERVIEWPERSON	BESKRIVELSE		BILAG
SABINE (SA1)	Ansat i Sydbank	Fysisk interview på 42 min. og 33 sek.	7
PHILIP (FP1)	Ansat hos Fyns Politi	Fysisk interview på 31 min. og 27 sek.	8
FINN (FP2)	Ansat hos Fyns Politi	Fysisk interview på 42 min. og 53 sek.	9
SØREN (SA2)	Ansat i Sydbank	Skriftligt interview	10
FREDERIK (FP3)	Ansat hos Fyns Politi	Skriftligt interview	11
CASE 1	*Vishing af politiets og Sydbanks sikkerhedsafdeling:* Forurettede er 80-85 år og oplever vishing, hvor vedkommende er blevet franarret 49.266 kr. Der forsøges at franarre flere penge, hvilket ikke lykkes, fordi offeret har en maksimal beløbsgrænse.		12.a
CASE 2	*Smishing gennem ny post fra "Region Syd":* Forurettede er 56 år og oplever smishing, hvor vedkommende er blevet franarret 11.494,58 kr.		12.b

CASE 3	*Smishing fra en "bekendt":* Forurettede er 66 og oplever smishing, hvor vedkommende bliver franarret for 8.510 kr. Vedkommende blev kontaktet af en veninde.	12.c
CASE 4	*Smishing fra ens "barn":* Forurettede er 82 og oplever smishing, hvor vedkommende bliver franarret 25.540 kr.	12.d

5.4 Databehandling

I dette afsnit vil vi præsentere faserne: *transskription, analyse og verifikation*. Indledningsvis vil vi komme ind på, hvordan vi har behandlet dataen i form af transskribering og kodning (fase 4 og 5). Derefter introducerer vi de overvejelser, vi har gjort for at imødekomme transparens og metodisk gyldighed (fase 6).

Fase 4: Transskription

I fjerde fase behandles den mundtlige interviewsamtale til en skreven tekst i form af en transskription af datamaterialet. Ved at strukturere interviewene fra talesprog til skriftsprog struktureres interviewsamtalerne i en form, der er velegnet til en nærmere analyse. Ifølge Kvale og Brinkmann udgør transskriptionen den første del af den analytiske proces (Kvale & Brinkmann, 2015: 234-235).

Audiooptagelserne af de tre interviews er blevet transskriberet. Dette er gjort af begge forfattere. Her er vi gået ud fra en transskriptionsnøgle, som kan ses i bilag 6, mens de transskriberede interviews kan ses i bilag 7-9. Vi har undervejs i transskriptionsprocessen lavet en ressourcemæssig prioritering. Her vurderede vi, at det var nok kun at transskribere hvert interview én gang, således at vi kunne bruge ressourcer på analysen (Kvale & Brinkmann, 2015: 243).

Fase 5: Analyse af empirisk materiale (kodning)

I interviewundersøgelsens femte fase analyseres det empiriske materiale, hvor kodningen af det indsamlede data er et vigtigt element i den videre analyse (Kvale & Brinkmann, 2015: 249). Selvom disse syv faser udelukkende fokuserer på kvalitative interviews, har vi valgt at inkludere kodningen fra vores dokumentanalyse i dette afsnit.

Indledningsvis har vi fået udleveret de fire cases fra Sydbank i fysisk udgave. Disse er blevet overført til en digital version i forbindelse med kodningen heraf, som er foretaget i tabeller i Google Docs, således at begge forfattere har haft adgang til koderne under hele undersøgelsens forløb (Kvale & Brinkmann, 2015: 235 ff.).

De tre fysiske og to skriftlige interviews er ligeledes kodet i tabeller i Google Docs. Kodningerne af vores empiriske materiale kan ses i bilag 12-17.

Vi har gjort brug af en lukket kodning. Dette afspejler vores deduktive tilgang, idet koderne er lavet i samspil med temaerne fra vores interviewguide, der som nævnt udspringer af teorien og den allerede eksisterende forskning. Ved at have koder, som er udviklet fra den eksisterende litteratur, anvender vi en begrebsstyret tilgang i kodningen (Kvale & Brinkmann, 2015: 262). På denne måde har vi haft en klar og præcis struktur og retning i spørgsmålene, da vi i løbet af indhentningen af empirisk materiale har haft de definerede koder for øje (Hansen, Andersen & Hansen, 2020: 223-224). Der er kodet ud fra 13 koder, hvor kode 4-7 er udledt af crime script analysis, og koderne 8-13 er udledt af eksisterende forskning og teori. Koderne kan ses i følgende kodeliste.

Kodeliste

KODE NR.	*Navn på kode*
1	Vishing
2	Smishing
3	Phishing
4	Preparation
5	Pre-activity
6	Activity
7	Post-activity
8	Muldyr
9	Forebyggelse
10	Målgruppe
11	Gerningspersoner
12	Social engineering
13	Rutineaktivitetsteorien

Efter kodningen er de fem interviews (fysiske og skriftlige) og fire cases blevet sammenlignet. Dette har vi gjort gennem en opdeling af koderne, således at de dele, der omhandler koderne 1-3 er analyseret for sig, og koderne 4-7- er analyseret for sig. Allerede her er det blevet klart for os, at det er nødvendigt at dele vores analyse op i to delanalyser – den ene om vishing og den anden om phishing/ smishing. Vi har anvendt crime script analysis som ramme for vores delanalyser. Det vil sige, at vores delanalyser er opdelt i de fire crime script stadier, som beskrevet i afsnit 5.1. om crime script analysis. I den følgende tabel ses en oversigt over vores interviewpersoner og cases med en kort beskrivelse til hver. Vores interviewpersoner er efter aftale blevet pseudo-nymiseret.

Fase 6: Verifikation

Undersøgelsens verifikation henviser til, hvilke former for kvalitetskriterier der er relevante for valideringen af undersøgelsens resultater (Kvale & Brinkmann, 2015: 320). I nærværende undersøgelse kommer vi ind på begreberne: *reliabilitet, intern validitet* og *ekstern validitet* for at fastslå undersøgelsens pålidelighed, gyldighed og generaliserbarhed.

Reliabilitet

Begrebet reliabilitet refererer til konsistensen og pålideligheden af en undersøgelses forskningsresultater. Forudsætningen for at opnå høj reliabilitet er, at man kan præcisere ens fremgangsmåde, således at den kan reproduceres af andre forskere (Kvale & Brinkmann, 2015: 318; Riis, 2012: 352). Fremgangsmåden skal dermed være begrundet, gennemsigtig, systematisk og grundig, så der skabes en klarhed over undersøgelsens fokus og filtrering (Riis, 2012: 353). I nærværende undersøgelse har vi forsøgt at skabe transparens over undersøgelsens metode- og teorivalg. Dette har vi gjort ved at klargøre, hvordan vi har behandlet vores data i form af indsamlingen, kodningen og hvilke overvejelser, der ligger bag udarbejdelsen af vores interviewguide. Herudover er det værd at nævne, at de vedhæftede bilag af transskriptionen, transskriptionsnøgle, kodningen, interviewguides og samtykkeerklæringer ligeledes er med til at styrke undersøgelsens reliabilitet. Endvidere har vi gennem en grundig gennemgang af vores metode og teori beskrevet, hvad formålet med de inddragne elementer er, og hvordan de vil anvendes i undersøgelsen.

Intern validitet

Validitet henviser til styrken og rigtigheden af et udsagn, og ifølge Riis skal det forstås som troværdigheden af en empirisk baseret konklusion (Kvale & Brinkmann, 2015: 318; Riis, 2012: 357). Mere specifikt handler validitet om, hvorvidt en metode undersøger det, som den har til hensigt at undersøge (Kvale & Brinkmann, 2015: 318). For at opnå høj validitet handler det om, at ens observationer afspejler de fænomener, som man interesserer sig for. I nærværende undersøgelse er det essentielt, at vores empirigrundlag og valg af respondenter afspejler, hvad vi ønsker at få belyst. På denne måde skal der være en sammenhæng mellem problemformuleringen, dataen og analysen, således at vi kan foretage en troværdig empirisk baseret konklusion.

I udvælgelsen af respondenter har vi haft et samarbejde med Sydbank og Fyns Politi, hvilket har muliggjort, at vi kunne få de rette respondenter. Det var vigtigt for os at interviewe fagprofessionelle inden for området, som kunne belyse vishing, phishing og smishing ud fra en

dansk kontekst. På denne måde har vi forsøgt at imødekomme kvalitetskriteriet om validitet. Dertil har vi forinden udarbejdelsen af vores interviews undersøgt fænomenet (tematisering), således at vi havde den nødvendige baggrundsviden til at udarbejde en fyldestgørende interviewguide, som afspejlede problemformulerings sigte. De to ovenstående elementer i samspil med de fire udleverede cases fra Sydbank med forurettedes beskrivelser om hændelsesforløbet har været med til at styrke vores validitet, da det er nogle elementer, som har givet os et indblik i gerningspersoner fremgangsmåder i vishing, phishing og smishing.

Ekstern validitet

Ekstern validitet henviser til, hvorvidt undersøgelsens resultater kan overføres til andre kontekster og situationer. Det handler i høj grad om, at resultaterne kan generaliseres til et større problemfelt end selve undersøgelsens materiale (Kvale & Brinkmann, 2015: 332; Riis, 2012: 358). Det kan diskuteres, hvorvidt vores undersøgelse besidder en analytisk generalisering, når vi blot har fem interviewpersoner. Vi har forsøgt at imødekomme kvalitetskriteriet om ekstern validitet ved at tage udgangspunkt i den eksisterende forskning. Eftersom flere af analysens resultater, mønstre og gerningspersoners fremgangsmåder afspejler den eksisterende forskning inden for vishing, phishing og smishing, påpeges det, at undersøgelsens resultater kan overføres til andre studier, hvorfor undersøgelsen kan anvendes i andre kontekster eller situationer inden for forskningsfeltet.

Fase 7: Rapportering og etiske overvejelser

Den sidste fase, rapportering, henviser til offentliggørelsen af undersøgelsens resultater (Kvale & Brinkmann, 2015: 163 & 348). Afsnittet præsenterer de overvejelser, vi har gjort os i forbindelse med at skulle rapportere vores viden med henblik på senere offentliggørelse af vores fund.
Når man udgiver en forskningsrapport, kan der rejses nogle moralske spørgsmål i forhold til rapporteringen af interviews. Hermed er der nogle etiske retningslinjer for informeret samtykke, fortrolighed og konsekvenser (Kvale & Brinkmann, 2015: 345)

For at overholde de gældende GDPR-regler har alle interviewpersoner underskrevet en samtykke- og fortrolighedserklæring, der giver os tilladelse til at audiooptage interviewet, bruge udtalelser som citater samt et løfte om pseudonymisering (Bengtsson & Mølholt, 2020: 195). Dette er ligeledes grunden til, at de vedhæftede erklæringer i bilag 1-4 ikke indeholder en underskrift, således at respondenternes navne ikke kan identificeres. De underskrevne

erklæringer findes i fysisk form hos undersøgelsens forfattere. Inden afleveringen af undersøgelsen tilbød vores kontaktperson i Sydbank at gennemlæse vores analyse. Dette var for at sikre, at der ikke var nogle fortrolige informationer fra organisationen, som blev offentliggjort uden samtykke. Dette var dog ikke tilfældet.
Vi har ikke indsendt analysen til gennemlæsning hos Fyns Politi. Da vi interviewede vores respondenter og talte med politikommissæren, efterspurgte de at få tilsendt den endelige undersøgelse. Der kan være nogle utilsigtede konsekvenser ved at tilsende undersøgelsen efter færdiggørelsen og ikke inden, fordi der kan være nogle etiske og politiske konsekvenser i citeringen af disse respondenter. Aspekter af deres arbejde kan anses for at være konfidentielle, hvorfor en gennemlæsning af vores analyse af politiet ville være ideelt. Selv om respondenterne har underskrevet en samtykkeerklæring og givet tilladelse til at anvende deres udtalelser, kan der være tilfælde, hvor respondenten kommer til at fortælle noget fortroligt og først bemærker det, når de læser den færdige undersøgelse.

I udarbejdelsen af vores undersøgelse er vi blevet opmærksomme på, hvordan undersøgelsen kan anvendes i det videre arbejde. Dette vil vi komme ind på i kapitel 7 om diskussion. Udover at andre kan forske videre på området, er der en mulighed for, at svindlere ligeledes anvender undersøgelsen. Her tænker vi, at undersøgelsen kan fungere som manuskript til potentielle motiverede forbrydere, der ønsker at begå vishing, phishing og/ eller smishing. Vi vil dog argumentere for, at lignende undersøgelser eller undersøgelser med crime script som ramme i forvejen er offentligt tilgængelige på internettet. Vi kan derfor ikke forudse, hvordan denne undersøgelse vil blive anvendt af svindlere. I vores undersøgelse præsenterer vi, hvordan vishing, phishing og smishing foregår, men vi præsenterer ikke de helt tekniske, bagvedliggende faktorer, som svindlere foretager sig i form af udarbejdelsen af en falsk hjemmeside og oprettelsen af falske links. Dette vil vi argumentere for er med til at vanskeliggøre, at vores undersøgelse i sig selv kan bruges som manuskript af potentielle svindlere.

Kapitel 6

Analyse

6. Analyse

I dette kapitel vil vi analysere vores interview-data, som vil blive understøttet af de fire cases fra Sydbank. Vi vil først analysere vores data om vishing. Efter afsnittet om vishing følger anden delanalyse bestående af phishing og smishing. Vi anvender crime script analysis som ramme for analysen. Rutineaktivitetsteorien vil løbende blive inddraget til at forklare de processuelle stadier i vishing, phishing og smishing.

6.1 Delanalyse I: Vishing – Storytelling

Denne delanalyse fokuserer på de fire crime script stadier i vishing – *preparation, pre-activity, activity* og *post-activity* (Chainey & Berbotto, 2021; Keatley, 2018). Formålet med denne delanalyse er at kortlægge og analysere, hvordan gerningspersoner agerer. Dermed vil vi komme ind på gerningspersonens processuelle stadier i vishing, hvor vi vil supplere analysen af gerningspersonens modus operandi med case 1 fra Sydbank.

6.1.1 Preparation

Første stadie i crime scriptet omhandler den forberedelse og planlægning, der sker forud for, at den kriminelle aktivitet (activity) kan opstå (Chainey & Berbotto, 2021: 282). Ud fra gennemgangen af den eksisterende litteratur inden for vishing omfatter dette stadie rekruttering af telefonsælgere og muldyr samt indhentning af informationer om ofrene (Choi, Lee & Chun, 2017: 459; Lee, 2020: 212; Nguyen, 2022: 233-234). I nogle tilfælde udgør muldyr den sidste del af vishing, hvortil brugen af muldyr er afgørende i post-activity, hvilket vil blive uddybet i afsnit 6.1.4.

Ud fra vores data tyder det på, at fire ud af fem respondenter har en antagelse om, at forberedelsen ved vishing typisk omhandler en indsamling af diverse ældre kvindenavne samt personer med fastnettelefonnummer gennem telefonbøger (også typisk ældre kvinder) (Bilag 7: 10; Bilag 8: 23; Bilag 9: 40; Bilag 11: 53-54). Sabine fra Sydbank og Finn fra Fyns Politi nævner, at telefonbøger suppleres med eksempelvis Krak (Bilag 7: 6; Bilag 9: 40). En af antagelserne kommer fra Frederik, der siger følgende:

> *"En teori er at gerningsmændene benytter sig af en fysisk telefonbog, hvor de slavisk gennemgår telefonbogen og kontakter borgere med samme navn. I særdeleshed navne udbredt blandt ældre - som f.eks. Åse, Yrsa og Else".* (Bilag 11: 53).

Vores data viser, at gerningspersoner indsamler telefonnumre af den ældre generation, hvilket ikke er beskrevet i den eksisterende forskning. Som citatet indikerer er udvælgelsen af potentielle ofre i en dansk kontekst mere målrettet end eksempelvis set hos Choi, Lee og Chun (2017), hvor de anvender call-centre til at foretage opkald til større og tilfældige målgrupper, hvilket er en kontrast i forhold til vores data. En gennemgående forklaring, som vi finder i vores data, er, at den ældre generation er en udsat gruppe, når det omhandler vishing. Ud fra rutineaktivitetsteorien er det denne gruppe, som betegnes *de egnede mål* for vishing. Det er den ældre generation, som de *motiverede forbrydere* målretter deres kommunikation til, da denne gruppe anses for at være mere autoritetstro og tillidsfuld, hvilket kan indikere, at de er mindre skeptiske, når gerningspersoner udgiver sig for at være fra en offentlig myndighed.

Det er værd at påpege, at respondenternes forklaringer blot er antagelser. Dog er disse antagelser om, at den ældre generation er mere udsat for denne kriminalitetsform, baseret på deres erfaringer fra sagsbehandlingen. Vi formoder ud fra eksperternes viden/ antagelser, at svindlerne har samme tankegang – at den ældre befolkning er mindre IT-kyndig. Uden at have talt med gerningspersoner om, hvordan de agerer eller tænker i processen op til vishing, udleder vi ud fra ovenstående, at de udvælger deres potentielle ofre ud fra stereotyper om, at den ældre generation er nemmere at snyde, når det omhandler IT-kriminalitet. I en befolkningsundersøgelse foretaget af Algoritmer, Data & Demokrati (ADD, 2021) fremgår det, at 44% af de adspurgte personer over 60 år har lave digitale kompetencer. Personer i alderen 18-26 år udgør 8%. ADD påpeger samtidigt, at kvinder har lavere digitale kompetencer end mænd, idet de udgør 54% af de 1.409 adspurgte (ADD, 2021). I vores analyse vil vi tage udgangspunkt i denne viden samt påstandene i vores data om, at ældre er mindre IT-kyndige. Vores respondenter omtaler gruppen af borgere med lav IT-kyndighed som "ældre", hvorfor vi vil gøre det samme. Udover en lav IT-kyndighed blandt de ældre påpeger alle fem respondenter, at Danmark er et samfund, der bygger på tillid (Bilag 7: 11; Bilag 8: 27; Bilag 9: 29; Bilag 10: 48; Bilag 11: 55-56). Dette vil vi uddybe i det følgende afsnit.

Danmark som tillidssamfund

Samtlige af vores respondenter nævner, at Danmark er et tillidssamfund, hvilket svindlerne anvender til deres fordel. Finn fra Fyns Politi påpeger, at når en offentlig myndighed kontakter en borger, vil borgerne som udgangspunkt stole på vedkommende. Idet en tillidsbaseret relation på forhånd er etableret gennem den eksisterende tillid til myndighederne, vil paraderne/ barriererne hos et muligt offer som udgangspunkt ikke være til stede (Bilag 9: 29). Ud fra Finns antagelse tolker vi, at tilliden til myndigheder er en af grundene til, at den ældre

generation er udsat i denne form for svindel – et egnet mål ud fra rutineaktivitetsteorien. Vi tolker, at de motiverede forbrydere ved vishing udnytter offerets svagheder i form af deres tiltro til myndighederne. På denne måde kan de tilegne sig personlige oplysninger eller få vedkommende til at overføre penge (Cohen & Felson, 1979: 596). Gerningspersonernes modus operandi er at skabe en falsk fornemmelse af tillid og autoritet hos offeret. Med udgangspunkt i vores respondenters antagelser tolker vi, at denne tiltro til myndighederne kan være en svaghed i den ældre befolkning.

Ud fra rutineaktivitetsteorien kan det påpeges, at den ældre generation er egnede mål ved vishing. Et andet argument for, at den ældre generation er egnede mål, kan være, at denne målgruppe i takt med digitaliseringen oplever nogle strukturelle og teknologiske forandringer i deres rutineaktivitet (Cohen & Felson, 1979: 589; ADD, 2021). I modsætning til før internettets udbredelse har man i dag mulighed for at tilgå sin bank på telefonen, hvor man kan overføre forskellige beløb via sin telefon. I takt med digitaliseringen og det øgede behov for IT bevæger den generelle befolkning, herunder denne målgruppe, sig mere på internettet og det digitale rum. Alt dette kan bidrage til, at den ældre generation er mere sårbare over for de motiverede forbrydere.
Vishing kan ramme enhver gruppe, men det er hovedsageligt den ældre generation, som er den primære målgruppe i en dansk kontekst. Dette skyldes, at de har mindre IT-kyndighed, hvilket gør dem mere sårbare over for vishing (Bilag 8: 29; ADD, 2021). Den manglende viden inden for IT, og hvordan man skal begå sig i det digitale rum, kan betyde, at den ældre generation ikke kender de risici, der er forbundet med at dele deres oplysninger gennem et telefonopkald. Dermed argumenterer vi for, at den ældre generation ikke har den nødvendige viden til at opdage vishing, hvorfor de ifølge rutinektivitetsteorien fremstår som egnede mål.
De præsenterede dele af forberedelsen er essentielle for, at næste stadie i crime scriptet kan finde sted. Dette udgør næste afsnit, som vil blive suppleret af vores data, eksisterende forskning og rutineaktivitetsteorien.

6.1.2 Pre-activity

Andet stadie i vores crime script analysis omfatter de afgørende valg og handlinger, der foretages op til udførelsen af selve den kriminelle handling (activity, stadie tre) (Chainey & Berbotto, 2021: 282). Følgende afsnit vil omhandle, hvordan gerningspersoner lykkes med at manipulere forurettede gennem et manuskript og et struktureret vishing-angreb.

Manipulation gennem et manuskript

Både Søren fra Sydbank og Frederik fra Fyns Politi nævner, at gerningspersonerne taler ud fra et manuskript (Bilag 10: 50; Bilag 11: 59). Vores data indikerer ikke, hvornår manuskriptet bliver udfærdiget, eller hvem der er ansvarlig for det. Vi kan dog se i gennemgangen af den eksisterende forskning, at der anvendes et manuskript, som gerningspersoner taler ud fra (Choi, Lee & Chun, 2017: 460). Vi tolker, at dette gør sig gældende i én af de fire cases (case 1), hvor en ældre kvinde på cirka 85 år kontaktes telefonisk af "Rigspolitiets sikkerhedsafdeling". Vi tolker, at denne handling er essentiel i gerningspersonernes crime script, idet de ved udarbejdelsen af et manuskript skal opdigte en troværdig historie, som medvirker til, at potentielle ofre videregiver deres oplysninger eller sender penge til en "sikker" konto. Uden en troværdig og struktureret historie kan der argumenteres for, at gerningspersoner ikke ville kunne lykkes på samme måde, som vi ser i tilfældet med den føromtalte case.

I den eksisterende forskning fremgår det ligeledes, at gerningspersoner, der foretager vishing, gennemgår træning forud for vishing, således at de fremstår som professionelle fagpersoner med en vis troværdighed (Choi, Lee & Chun, 2017: 459-464). Dette ser vi ligeledes i føromtalte case, hvor en 85-årig kvinde kontaktes af "Henrik". Hun beskriver ham som *"værende højest professionel og troværdig. Han talte højligt og med myndighed. Han talte uden accent og vurderes til at være af jysk oprindelse."* (Bilag 12.b: 62). Denne case vil blive uddybet under *'activity'* i afsnit 6.1.3.

Ovenstående elementer i form af udarbejdelsen af et troværdigt manuskript og en troværdig karakter, herunder medarbejderen fra "Rigtspolitiets sikkerhedsafdeling", er vitale elementer i gerningspersoners manipulation. Det handler i høj grad om at bygge en troværdig historie, som medvirker til, at ofrene sænker paraderne og dermed bliver mere modtagelige for gerningspersonernes historie.

Ud fra eksisterende forskning og vores data argumenterer vi for, at vishing er koordinerede angreb. Dette indebærer både planlægningen og udførelsen af vishing, hvor vi tolker, at gerningspersoner taler ud fra et struktureret og professionelt manuskript. Ud fra rutineaktivitetsteorien kan der påpeges, at de motiverede forbrydere spiller en essentielt rolle ved vishing, hvilket vi vil uddybe i det næste afsnit.

Vishing som koordinerede angreb

I og med at disse angreb virker professionelle, strukturerede og koordinerede, kræver det, at gerningspersoner har motivationen til at lære dette manuskript. Dette kræver en motiveret forbryder, som har evnerne og kan se mulighederne i at begå vishing (Cohen & Felson, 1979:

590). Derudover tolker vi, at de motiverede forbrydere begår vishing, da det er nemt og ikke kræver, at man er fysisk til stede og skal møde offeret ansigt-til-ansigt for at udføre disse angreb. Med udgangspunkt i rutineaktivitetsteorien kan der argumenteres for, at de teknologiske forandringer har forårsaget nye og flere kriminalitetsmuligheder for den motiverede forbryder (Cohen & Felson, 1979: 589 & 591). Dette understøtter den eksisterende forskning på området ligeledes, som kommer ind på, at digitaliseringen har åbnet flere muligheder for svindlerne (Paraschiv et al. 2021: 394). Denne faktor i form af digitaliseringen medvirker til, at der altid vil være motiverede forbrydere til stede. Så længe der kan identificeres en mulighed for at begå kriminalitet og økonomisk vinding, vil det tiltrække potentielle gerningspersoner til at engagere sig i disse kriminelle handlinger, herunder vishing. Ud fra rutineaktivitetsteorien tolker vi, at de egnede mål har en positiv indvirkning på mængden af motiverede forbrydere (Cohen & Felson, 1979: 591). Egnede mål er et element, som skal være til stede, før den kriminelle handling kan udspille sig. Derfor er dette element essentielt for den motiverede forbryder, før den kriminelle handling kan lykkes (Cohen & Felson, 1979: 589). Så længe der findes egnede mål, vil de motiverede forbrydere altid være til stede. Yderligere spiller *fraværet af egnede beskyttere* også en stor rolle i, hvordan motiverede forbrydere lykkes med at franarre egnede mål (Cohen & Felson, 1979: 589).

De egnede beskyttere er vigtige for at forhindre eller stoppe kriminaliteten. Pårørende til de egnede mål vil ligeledes optræde som egnede beskyttere. Dette fremtræder direkte i case 1, hvor den 85-årige dame kontakter sin svigersøn for hjælp og får at vide, at hun skal spærre sine konti og MitID:

> "*Jeg kontaktede kl. 2251 min svigersøn, som oplyste mig om, at det tjenestenummer, og sagsnummer ikke anvendes i politiet, hvorfor jeg skulle lukke mine konto og spærre mit Mit ID. Jeg gik straks herefter i gang med, at spærre min konti"* (Bilag 12.a: 61).

Ud fra dette citat tolker vi, at forurettedes svigersøn agerer som egnede beskytter for den ældre kvinde. I hans fravær havde det for gerningspersonerne været muligt at franarre kvinden et nyt beløb den følgende dag. Vi udleder, at egnede beskyttere i disse kriminelle situationer er essentielle for at forhindre forekomsten af de kriminelle handlinger. Denne pointe understøttes af rutineaktivitetsteorien, som påpeger, at kriminalitet forhindres ved at reducere en af følgende elementer: motiverede forbrydere, egnede mål eller fraværet af egnede beskyttere (Cohen & Felson, 1979: 589 & 591). Dette uddybes yderligere i diskussionsafsnittet, hvor vi kommer ind på mulige forebyggelsesstrategier. I det følgende vil vi præsentere, hvordan handlingerne fra preparation og pre-activity fører til selve activity i vishing.

6.1.3 Activity

Det tredje stadie i vores crime script er *activity*. Dette er hovedaktiviteten (Keatley, 2018: 130) i vishing, hvor gerningspersoner forsøger at overbevise ofrene om at videregive personfølsomme oplysninger eller overføre penge til en "sikker" konto.

"Der er noget galt med dit kort"

Ud fra vores data ser vi, at den kriminelle handling i vishing kan opdeles i to forskellige typer. I den ene type modtager den forurettede et opkald – typisk fra banken – om, at "der er noget galt med dit kort" (Bilag 7: 12; Bilag 9: 29), hvorefter de tilbyder at sende en person ud for at afhente forurettedes kort på forurettedes adresse. Kortet bliver herefter misbrugt i hæveautomater. Udover påstanden om, at der er noget galt med forurettedes kort, oplyser vores data os ikke om, hvad der ligger forud for, at kortene bliver afhentet. Frederik fra Fyns Politi påpeger, at han har en teori om, at gerningspersoner bruger et *"Potentielt manus og oplysninger om den forurettede."* (Bilag 11: 59) som forberedelse på denne form for svindel, som vi ligeledes har beskrevet i afsnit 6.1.2. Vi antager, at gerningspersoner med et manuskript kan fremstå selvsikre, troværdige og som professionelle fagfolk i deres svindel, blandt andet fordi de ikke er nødsaget til at improvisere undervejs. Sabine understøtter dette med at sige: *Jamen de er meget overbevisende. Altså de er jo meget professionelle, lyder meget professionelle i det her."* (Bilag 7: 5).

Denne form for svindel indikerer, at der sker en gennemgående forberedelse forud for den kriminelle handling. Udover at fremstå professionel og troværdig kan vi se fra vores data, at gerningspersonerne ofte taler ind i et offers frygt og uvidenhed for at blive udsat for økonomisk kriminalitet (Bilag 7: 12; Bilag 9: 45). Samtidigt viser vores data, at gerningspersoner er i stand til at 'spoofe' telefonnumre – de manipulerer med et telefonnummer, så det fremstår under et navn eller som et andet telefonnummer. Finn giver følgende eksempel:

> *"så kan de jo se, der står et eller andet telefonnummer [...] så står der jo 66 14 14 48, det så Fyns Politi, "jamen det er rigtigt nok". Og de tænker ikke ind i "jamen det er bare et eller andet spoofing-nummer". De er ikke klar over, det er et nummer, der er lagt ind over, så det fremgår som om, det er fra en institution. "* (Bilag 9: 35).

I denne type af vishing er den ældre befolkning den primære målgruppe (Bilag 7: 12; Bilag 11: 54). Som nævnt i afsnit 6.1.1 er Danmark et tillidssamfund, men især den ældre befolkning nærer stor tillid til offentlige myndigheder. Dette gør dem til egnede mål jf. rutineaktivitetsteorien og ADD (2021). Det er blandt andet denne kombination af egnede mål

med en frygt for at miste økonomiske midler og veludført manipulation gennem spoofing af telefonnumre, der er med til at gøre denne type af vishing mulig. Ifølge rutineaktivitetsteorien kræver udførelsen af en kriminel handling, at alle tre elementer er til stede på samme tid. De egnede mål mangler relevant viden om blandt andet spoofing og databedrageri gennem medier. Den grundige forberedelse forud for vishing indikerer, at der er tale om motiverede forbrydere (Cohen & Felson, 1979: 589).

Den grundige forberedelse kommer ligeledes til udtryk ved den anden type af vishing, hvor gerningspersoner på samme måde ringer forurettede op, men i det her tilfælde forsøger gerningspersonerne at få offeret til at overføre penge til en 'sikker konto'. Dette vil blive uddybet i følgende afsnit.

Safe account fraud – Danske navne og falske myndigheder

I den anden type af vishing bliver forurettede ringet op, og gerningspersonerne udgiver sig for at være fra en myndighed/organisation. Denne organisation eller myndighed har typisk på forhånd en eksisterende legitimitet hos befolkningen (Bilag 9: 33). Det kan eksempelvis være ens bank, politiet, Skat og så videre. Personerne fra myndighederne præsenterer sig med danske navne og taler også dansk – nogle endda med tilpasset dialekt til deres offer (Bilag 12.a: 62). Vi ser samme tendens i den eksisterende forskning. I undersøgelsen fra Choi, Lee og Chun (2017) sidder svindlere med kombineret kinesisk og koreansk oprindelse i Korea. Disse gennemgår forudgående træning i at tale uden kinesisk dialekt, så de virker mere troværdige, når de ringer fra et koreansk nummer til et koreansk offer og udgiver sig for at være fra banken.

Mens opkaldet foregår, er der flere måder, hvorpå gerningspersonerne får adgang til forurettedes oplysninger. Typisk forsøger gerningspersoner at opbygge en historie, hvor de fortæller, at der er nogen, som er i gang med at tømme forurettedes konto, eller at der er nogle igangværende transaktioner, som er mistænkelige. I nogle tilfælde kan disse telefoniske samtaler vare over længere tid. På denne måde opbygger gerningspersonerne tillid hos ofrene. Vores data indikerer, at brugen af et manuskript er en anvendt teknik blandt gerningspersonerne. Manuskriptet gør det muligt for gerningspersonerne at fortælle ofrene en historie, som i princippet kan være målrettet et hvilket som helst offer. Gennem manuskriptet formår gerningspersonerne at manipulere med ofrene, således at de afslører væsentlige informationer. Sabine påpeger, at *"Det handler meget om i vishing, at de får forklaret kunden rigtig mange ting. Rigtig mange ting på samme tid. Så kunden bliver forvirret over, hvad er det der foregår, og så studser kunden ikke over, at det her det kan være fake."* (Bilag 7: 4-5).

Ud fra ovenstående citat vildleder gerningspersonerne de potentielle ofre ved at forvirre dem. Ved at informere de potentielle ofre om en masse ting, lykkes det gerningspersonerne at manipulere ofrene. Denne form for manipulation i samspil med at gerningspersoner udgiver sig for at være fra en offentlig myndighed eller en virksomhed, tolker vi som faktorer, der påvirker de potentielle ofre til at forholde sig mindre kritisk til, hvad der bliver sagt ved vishing. Yderligere tolker vi, at denne fremgangsmåde med at overvælde ofrene med en masse informationer er en måde, hvorpå gerningspersonerne skaber en situation, som skal få ofrene til at føle sig pressede. Vi antager, at gerningspersoner bevidst presser de egnede mål, så de føler sig nødsaget til at handle hurtigt uden at tænke over situationen. Dertil udleder vi, at gerningspersonerne forsøger at få de egnede mål til at udføre forhastede handlinger ved vishing, hvilket er til gerningspersonernes fordel, da de på den måde har en større sandsynlighed for at få de egnede mål til at videregive deres oplysninger eller overføre penge til en "sikker konto".

Finn påpeger, at gerningspersonerne beretter ofrene om, at der foregår noget mistænkeligt på deres konto, eller at deres kort netop har været brugt i udlandet (Bilag 9: 34). Sabine giver eksemplet med, at der er taget et lån i en forurettedes navn og med vedkommendes konto. Til trods for at forurettede benægter lånet, formår gerningspersonen at overbevise om, at lånet er gennemført, og derfor giver forurettede gerningspersonen adgang til sin konto eller godkender anmodninger i MitID, så gerningspersonen kan "hjælpe" med at standse lånet (Bilag 7: 4-5).
Ved vishing kan der både forekomme sager, hvor gerningspersonerne får adgang til forurettedes konti og selv overfører pengene, mens det i andre sager foregår således, at forurettede *selv* overfører pengene til en anden konto. Dette kan være gerningspersonens konto, en tredjeparts eller et på forhånd rekrutteret muldyr (Bilag 7: 13; Bilag 8: 20; Bilag 10: 49; Bilag 11: 55). Dette kaldes for safe account fraud. Ud fra vores data foregår safe account fraud oftest således, at gerningspersoner overbeviser forurettede om, at der foregår noget mistænkeligt på vedkommendes konto, hvorfor forurettede bliver lokket til at overføre sine midler til en "sikker" konto for ikke at lide økonomisk tab (Bilag 11: 55).
Manipulationsteknikkerne, den forudgående træning og anvendelsen af manuskript præsenteret i nærværende afsnit ses anvendt i den følgende case, som vi fik udleveret af Sydbank.

Case 1: Vishing og safe account fraud

Tabel 5: Casebeskrivelse

Case 1 fra Sydbank omhandler vishing, hvor en ældre kvinde bliver kontaktet af "Rigspolitiets sikkerhedsafdeling". Kvinden bliver ringet op af en person, der præsenterer sig som "Julie", der ligeledes oplyser sit tjenestenummer og sagsnummer på forurettedes sag. Julie oplyser forurettede om, at der er blevet oprettet et forbrugslån på 45.000 kr i Nordea i forurettedes navn. Samtidigt nævner Julie navnet på en person og spørger, om forurettede kender personen. Julie informerer forurettede om, at personen er mistænkt for at begå svindel i lignende sager. Julie spørger ind til, om forurettede har mistanke om, at nogen kan have afluret hendes PIN-kode, samt om forurettede fortsat er i besiddelse af alle sine hævekort. Efterfølgende bliver forurettede informeret om, at Julie vil viderestille til "Henrik" fra "Sydbanks sikkerhedsafdeling". Af Henrik får hun at vide, at der er blevet handlet for store summer i henholdsvis Jysk og Elgiganten, og forurettede bliver spurgt ind til, om hun har anvendt sit kort i en specifik del af Danmark. Forurettede benægter det hele. Henrik instruerer kvinden til at samle alle sine penge på én konto, som efterfølgende skal overføres til et sikkert depot (safe account fraud). Forurettede fortæller i vores data, at Henrik var væk fra telefonen flere gange, fordi han både skulle kontakte Nets og politiet. Derefter fortæller han til forurettede, at de har travlt i afdelingen, fordi han har fået oplyst af politiet, at de *"har fat i to mistænkte fra Sydbank"* (Bilag 12.a: 62). Dette er et eksempel på, at Henrik legitimerer sin falske rolle som ansat ved Sydbank ved herunder at påstå, at der er fundet svindlere internt i banken, hvilket er med til at gøre forurettede påpasselig og ivrig efter at få beskyttet sine penge. Henrik hjælper forurettede med at få overført cirka 50.000 kroner til et depot. Idet forurettede har en beløbsgrænse på sin konto beder Henrik hende kontakte Sydbank og hæve beløbsgrænsen. Forurettede bliver bedt om at gøre dette fra en anden telefon, så Henrik kan lytte med. Han forklarer hende samtidigt, at hun ikke må oplyse til banken, samt at banken ikke kan kræve at vide, hvad pengene skal bruges til. Dette lykkes ikke, fordi banken har lukket grundet helligdag. Henrik beder efterfølgende forurettede om at slukke alle sine telefoner og computere indtil 22:30, hvor han vil kontakte forurettede igen. Forurettede bliver "grundet sikkerhed" informeret om ikke at tale med nogen om sagen.

Som det fremgår af casen, bliver der løbende spurgt ind til mange forskellige emner, og gerningspersonerne taler med troværdighed og professionalisme, hvilket skaber tillid til dem. Finn understøtter dette med følgende:

> *"man taler ind i folks frygt for, at nu er man ved at lide et økonomisk tab, og hvis der er noget, man ikke kan lide som privatperson, det er jo lide et økonomisk tab, så derfor så falder barrierer i forhold til at sige hvad, hvad sker der nu, og så er de jo så, de begynder at tale ind i den der manipulerende rolle i forhold til den forurettede, således at de igen bliver afmonteret"* (Bilag 9: 34).

Frygten for at lide økonomisk tab, kan have en manipulerende effekt. Som nævnt i ovenstående citat, bliver ofrene "afmonteret", hvorefter de foretager sig handlinger, som giver gerningspersonerne adgang til deres personlige oplysninger, konti og/ eller MitID.
Gerningspersonerne anvender denne frygt hos ofrene og understøtter deres troværdighed ved at bruge danske navne samt oplyser sagsnummer og tjenestenummer. Denne veludførte storytelling medvirker til, at forurettede bliver overbevist om at overføre sine midler til et sikkert depot for at undgå at ende ud i et økonomisk tab. Når først de motiverede forbrydere begynder at fortælle historien (læse op fra manuskriptet), opbygger tillid og anvender frygt, styrkes det manipulerende element i samtalen, hvilket får det egnede mål til at agere under pres, så de tager forhastede beslutninger.

I vores data finder vi, at vishing foregår over længere tid: *"Tidligere har vi set sager på, at de har siddet og talt med folk gennem flere timer, [...] og så bliver man ringet op igen og så, så det er et langt langt forløb, hvor de så på den måde kan manipulere folk ..."* (Bilag 9: 34). Her bliver de ældre ud fra rutineaktivitetsteorien igen et egnet mål, da vi antager, at voksne personer uden hjemmeboende børn i nogle tilfælde bor og tilbringer mere tid alene end eksempelvis voksne i 40-50 års alderen. Det vil sige, at de ikke på samme måde kan spørge andre til råds i øjeblikket for vishing-angrebet. Med udgangspunkt i rutineaktivtetsteorien påpeger vi ud fra ovenstående, at den ældre befolkning har et fravær af egnede beskyttere i form af andre til at advare dem i øjeblikket, hvilket gør dem sårbare for disse angreb og dermed til egnede mål.

En ting at bemærke ved nærværende case er, at gerningspersonerne er bevidste om, hvilken bank forurettede er kunde i. Sabine påpeger, at "*Nogle* (gerningspersoner) *får adgang til netbank først, så ringer de kunden op bagefter og siger "jamen jeg kan se sådan og sådan", og det er fordi, de har adgang til alle kundens data [...]. Så har de alle kundens data, når de ringer op, og det er dér, hvor de virker rigtig troværdige, for de kan jo se det samme som kunden"* (Bilag 7: 3). Sabine påpeger samtidigt, at de er bevidste om, at der findes svindlere,

som "nøjes" med kun at stjæle personlige oplysninger fra borgere. Disse oplysninger sælger de videre til andre svindlere, eller de anvendes på et senere tidspunkt til større økonomisk vinding (Bilag 7: 13). Gerningspersonerne har altså gjort sig noget forberedelse, inden de kontakter deres ofre. Ud fra rutineaktivitetsteorien kan de betragtes som motiverede forbrydere. Vi ser samme type af forberedelse i den eksisterende forskning fra Choi, Lee og Chun (2017: 459-460) og Nguyen (2022: 233).

Det er samtidigt værd at bemærke, at gerningspersonerne i case 1 kontakter forurettede på en helligdag. Ud fra vores interviewdata kan vi se, at dette ikke er tilfældigt (Bilag 9: 33). Finn påpeger, at gerningspersoner målretter deres angreb ud fra tendenser i samfundet – eksempelvis Covid-19 og årsopgørelser, men også helligdage, hvor bankerne holder lukket. Forurettede fra case 1 understreger også, at hun var bevidst om, at banken var lukket, da hun af Henrik blev bedt om at kontakte Sydbank. Vi antager, at forurettede er blevet grundigt manipuleret og forvirret af de mange spørgsmål fra Julie og Henrik, hvilket har gjort hende godtroende over for deres ord, så hun gør som instrueret. Årsagen til, at forurettede bliver manipuleret, er grundet gerningspersonens professionalisme og troværdighed, hvilket Finn fra Fyns Politi kommer ind på i følgende citat.

> "*Flere ofre forklarer eksempelvis, at gerningsmanden er utrolig tillidsvækkende og overbevisende ved telefonisk kontakt. Nogle gange føler ofre sig næsten hypnotiseret, selvom de endda godt vidste, at der var noget mistænkeligt ved samtalen"* (Bilag 11: 56).

Denne hypnotiserende effekt ses i case 1, hvor den 85-årige kvinde siger, at hun ikke kunne *"opnå telefonisk kontakt til banken, hvilket jeg godt vidste jeg ikke kunne"* (Bilag 12.a: 62). Kvinden er bevidst om, at banken har lukket, men fortsætter alligevel med at tale med og stole på Henrik, som angiveligt ringer fra selv samme bank trods de tydelige faresignaler i interaktionen. Vi tolker, at dette kan skyldes den føromtalte hypnotiserende effekt, som medvirker til, at forurettede ikke afbryder samtalen, selvom hun er klar over, at banken har lukket den pågældende dag. Efter udførelsen af dette eller lignende vishing-angreb, skal udbyttet fra svindlen indhentes. Dette foregår i fjerde stadie af crime scriptet, *post-activity*, som vil blive uddybet i det følgende afsnit.

6.1.4 Post-activity

Fjerde og sidste stadie i vores crime script omhandler den aktivitet, der sker efter hovedaktiviteten i hele den kriminelle handling (Keatley, 2018: 130). Ud fra vores data ser vi fire forskellige tendenser:

1. Hæve pengene i kortautomater efter afhentning af forurettedes kort.
2. Omsætte pengene til værdi – møbler, ure mm.
3. Omsætte pengene til bitcoin og andre krypto-valuta.
4. Anvende muldyr.

Tendenserne 2, 3 og 4 kan forekomme både ved vishing, phishing og smishing, hvorimod tendens 1 udelukkende foregår ved vishing. Den første tendens vil blive uddybet i det følgende, hvorefter vi vil indlede præsentationen af tendens 4 om muldyr. Tendenserne 2 og 3 vil blive præsenteret under afsnit 6.2.4 om phishing og smishing, hvor tendens 4 ligeledes uddybes yderligere. Alle tendenser søger at sløre pengesporet og gerningspersonernes identiteter. Dermed kan den sidste fase i form af post-activity betegnes som en vigtig del i at afslutte den kriminelle handling og dermed hvidvaske de kriminelle penge.

Sabine, Philip og Finn nævner, at der er nogle tilfælde, hvor gerningspersoner afhenter forurettedes kort og hæver pengene i kortautomater (Bilag 7: 12; Bilag 8: 20; Bilag 9: 29). Dette er i forbindelse med vishing, hvor gerningspersonerne kontakter forurettede og fortæller dem, at der er noget galt med deres betalingskort. Herefter fortæller de forurettede, at kortet vil blive afhentet om noget tid, hvorefter en gerningsperson dukker op på forurettedes adresse og afhenter kortet og vedkommendes PIN-kode (Bilag 7: 12). Efterfølgende hæves pengene og dermed slutter pengesporet. Det ser vi ligeledes i den eksisterende forskning på området. Nguyen påpeger, at post-activity-stadiet i hans undersøgelse omfatter flugt fra en fysisk lokalitet, efter der er hævet penge fra et stjålet betalingskort (Nguyen, 2022: 238). Philip og Finn fra politiet påpeger, at det for tiden er vishing, de hyppigst efterforsker, sammenlignet med phishing og smishing, hvorimod det i Sydbank er smishing (Bilag 8: 22; Bilag 7: 3). Politiets arbejde med databedragerisager er især præget af efterforskning, hvor de følger pengesporet for at finde frem til en gerningsperson eller muldyr. Philip, Finn og Frederik fra Fyns Politi påpeger, at der er nogle forhindringer i opklaringsarbejdet, da de kriminelle slører deres færden med taletidskort (Bilag 8: 19; Bilag 9: 36; Bilag 11: 57). Som nævnt i afsnit 6.1.3 'spoofer' de kriminelle også deres telefonnumre, hvilket igen er med til at udfordre opklaringsarbejdet. Generelt siger vores data ikke meget om post-activity-stadiet i et

vishing-crime script, hvorfor videre forskning på området kunne være relevant i forebyggelsesøjemed.

Med henblik på fjerde tendens i form af muldyr kan det være svært at vurdere, hvorvidt der anvendes muldyr til at sløre pengesporet. I case 1 om vishing overføres forurettedes økonomiske midler til en ukendt konto. Vi kan ikke konkludere, om denne konto er en muldyrskonto, men ud fra dataen og den eksisterende forskning antager vi, at der sandsynligvis er anvendt muldyr i case 1. Vedamanikam og Chethiyar påpeger, at muldyr benyttes til at sløre sporet af det kriminelle udbytte (Vedamanikam & Chethiyar, 2020: 20). Anvendelsen af muldyr bliver nævnt flere gange i dataen, hvilket blandt andet kommer til udtryk i nedenstående citat af Philip fra Fyns Politi:

> *"de her sager hvor ældre mennesker bliver ringet op og bliver lokket til at udlevere deres oplysninger [..] i de her typer af sager ser vi ofte at det er muldyr, som får penge overført til sig, og så går de ud og hæver dem, og så kører det på den måde. Så kan du ikke spore pengene længere, så kan du kun spore det til muldyr. Så stopper sporet der."* (Bilag 8: 20).

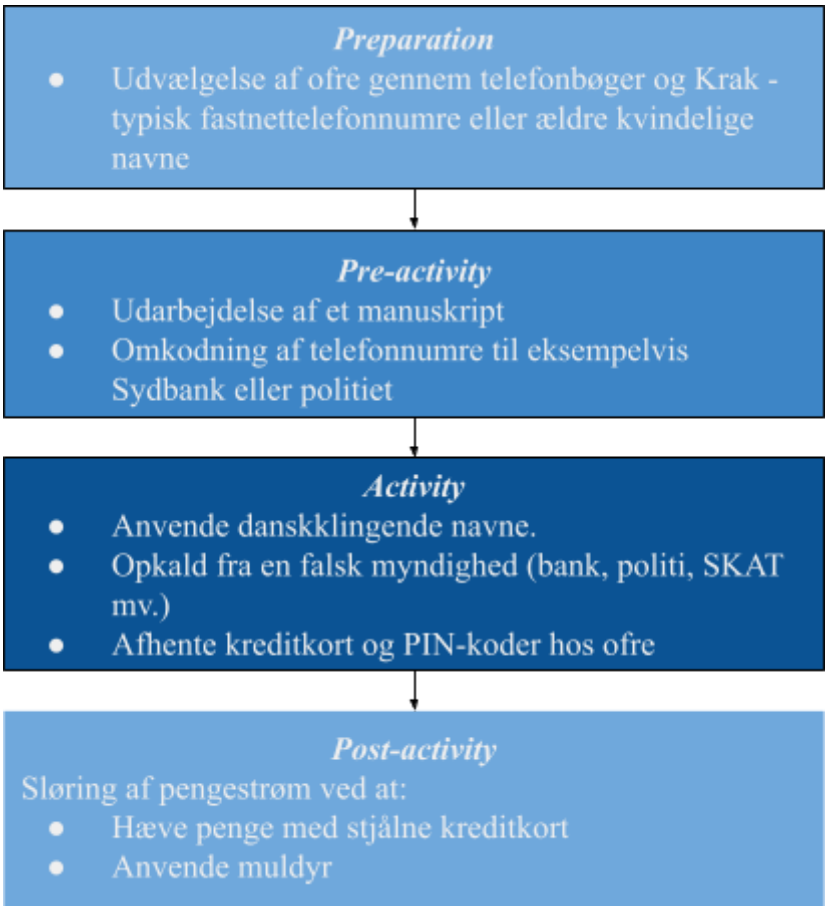
Ud fra citatet udleder vi, at brugen af muldyr er vigtigt i det afsluttende stadie af vishing. I dette stadie anvendes muldyr til at sløre pengene, således at gerningspersonen ikke bliver opdaget. Dette kan gøres ved, at pengene sendes til et muldyr, hvorfra de bliver hævet. En anden måde at sløre pengenes oprindelse er at overføre pengene, så de kommer ud i flere led. *"jo flere led de kommer ud i, jo mere "hvide" bliver pengene, hvis man kan sige det sådan. Fordi vi kan ikke spore dem så langt ud."* (Bilag 7: 12). På denne måde kan pengene ikke spores, hvilket betyder, at den kriminelle handling kan afsluttes uden at gerningspersonen bliver opdaget.

6.1.5 Opsummering på delanalyse 1

Delanalyse 1 har beskrevet de processuelle stadier ved vishing. I forberedelsesfasen (preparation) indhenter gerningspersonerne telefonnumre på deres ofre gennem telefonbøger og Krak. De målretter ældre kvinder og udgiver sig for at kontakte dem på vegne af en dansk myndighed eller en bank. Gerningspersonerne har en stereotyp om, at ældre personer er mere tillidsfulde over for disse instanser, og dette gør dem til egnede mål for visning. Når gerningspersonerne har opnået kontakt til det egnede mål, taler de ud fra et manuskript. Dette udarbejdes i stadiet 'pre-activity'. Vishing er dermed koordinerede angreb. Selve den kriminelle handling (activity) kommer til udtryk på to måder. Ved den første afhenter

gerningspersonen kreditkort i forurettedes eget hjem under påskud af at være fra banken. Herefter hæves der penge med forurettedes kort i en hæveautomat (post-activity). Den anden type af vishing er safe account fraud, hvor gerningspersonen får det egnede mål til selv at overføre penge til en "sikker" konto. Denne konto kan være en muldyrskonto, hvilket er det afsluttende stadie i vishing. De fire stadier af crime scriptet bag vishing er opsummeret i den følgende figur.

Figur 4: Crime script af vishing



Kilde: Eget arbejde

6.2 Delanalyse II:

Phishing & smishing – Troværdighed, legitimitet, manipulation

Dette afsnit omhandler, hvordan phishing og smishing kommer til udtryk i vores data. Vi har valgt at kombinere disse to modus under samme kategori, da phishing og smishing udelukkende adskiller sig ved, at den ene foregår over mail (phishing) mens den anden (smishing) foregår gennem SMS (Bilag 10: 47; Center for Cybersikkerhed, 2022: 3).

6.2.1 Preparation

I vores data finder vi begrænset viden om, hvad der sker i den indledende fase for phishing og smishing. Preparation er den planlægning, der sker forud for den kriminelle handling – de overvejelser som muliggør handlinger i praksis (herunder både handlinger inden for pre-activity og activity) (Chainey & Berbotto, 2021: 282). Den begrænsede viden om den forberedende fase kan opsummeres i en udtalelse fra Finn, hvor han bliver spurgt ind til, hvordan smishing foregår:

> *"Det synes jeg, det er sådan lidt mere random sådan set [...]. Hvordan de så har fundet de der telefonkæder, de der numre der hvor de bare lige sådan lige i flæng sender nogle telefonnumre eller nogle masse-SMS'er ud, det har jeg ikke rigtig belæg for at udtale mig omkring. Det kan godt virke sådan lidt vilkårligt"* (Bilag 9: 33).

Finn er den eneste af vores respondenter, der kommer ind på dette stadie i crime script analysis. Som det fremgår ud fra citatet er udtalelsen ikke stærkt underbygget, idet Finn egentlig ikke har belæg for sin udtalelse men blot hentyder til, at processen er vilkårlig. Ud fra Finns udtalelse udleder vi, at Finn indirekte påpeger, at der er tale om en større, tilfældig indsamling af telefonnumre (og eventuelt anden information om ofre), inden der sendes masse-SMS'er ud. Anvendelsen af massekommunikation vil vi uddybe i afsnit 6.2.3 om activity.

Selvom der er en usikkerhed omkring Finns udsagn, understøtter den eksisterende forskning inden for smishing dette. Choi og Lee (2021) påpeger i deres crime script analysis af smishing, at det i denne fase handler om at indsamle ofrenes personlige oplysninger så som telefonnumre, som de på ulovlig vis køber af mæglere. Ud fra ovenstående pointerer vi, at udvælgelsen af ofre fremstår mere tilfældigt ved phishing og smishing sammenlignet med vishing. Denne del er essentiel for gerningspersoner, fordi de herigennem tilegner sig en database af potentielle ofres informationer, som muliggør, at de kan massekommunikere ud til en bred vifte af mennesker.

Ovenstående forberedelsesmetode anvendes i kombination med, at gerningspersoner målretter deres massekommunikation gennem samfundstendenser og virksomheder, som indgår i den danske befolknings dagligdag – eksempelvis PostNord. Vi vil i det følgende uddybe, hvad vi mener med samfundstendenser samt uddybe betydningen af danskernes "dagligdags-virksomheder".

Samfundstendenser og dagligdags-virksomheder

Af vores data tolker vi, at svindlerne har nogle konkrete overvejelser forud for, at de indleder den kriminelle handling. Vi kategoriserer overvejelserne som *samfundstendenser* og *dagligdags-virksomheder*, hvor sidstnævnte er virksomheder, som er alment benyttet i den generelle befolknings hverdag. Ud fra udtalelser fra Finn kan vi udlede, at svindlere tilrettelægger deres angreb ud fra aktuelle hændelser i samfundet som eksempelvis under Covid-19 – svindlerne tilpasser deres angreb til samfundstendenser. Dette udleder vi fra følgende citat fra Finn:

> "*I forbindelse med Covid-19 der havde vi jo masser af sager fra, fra Seruminstituttet og så alle de der institutioner, der håndterede Covid-19. Så de er faktisk gode til, hvis der er en tendens ude i samfundet, hvis det bliver talt omkring et eller andet, så er de gode til at gribe det. Og bruge det i forhold til at legitimere sig selv som afsender."* (Bilag 9: 33-34).

Ud fra ovenstående citat påpeger Finn, at svindlerne legitimerer sig selv som afsender ved at benytte aktuelle hændelser fra samfundet. Som nævnt i ovenstående citat var der under Covid-19 en masse sager, hvor gerningspersoner udgav sig for at være fra Seruminstituttet over SMS. Vi tolker, at anvendelsen af en samfundstendens er med til at øge sandsynligheden for, at potentielle ofre falder for smishing, idet troværdigheden hos svindlerne styrkes af de samfundsaktuelle hændelser. Ifølge rutineaktivitetsteorien er strukturelle ændringer i kombination med de tre elementer (motiverede forbrydere, egnede mål & fraværet af egnede beskyttere) afgørende for, at kriminalitet kan opstå (Cohen & Felson, 1979: 589). Covid-19 var en stor strukturel ændring i det danske samfund, hvorfor der på daværende tidspunkt er opstået nye metoder til at begå kriminalitet, herunder smishing-beskeder omhandlende Covid-19. Strukturelle ændringer behøver ikke nødvendigvis at være i lige så stor omfang som Covid-19. Et andet eksempel på en strukturel ændring kan være årsopgørelsen, der én gang årligt offentliggøres for hele befolkningen (Bilag 7: 6). Vi tolker, at smishing-beskeder fremstår mere aktuelle og troværdige, når gerningspersoner tilpasser deres kommunikation ud fra samfundets

tendenser. Ved at benytte samfundets tendenser er omfanget af egnede mål større, idet udvælgelsen som nævnt ovenfor er mere tilfældig end målrettet. På denne måde er det nemmere for motiverede forbrydere at finde egnede mål ved at benytte aktuelle samfundstendenser. Dermed kan denne fremgangsmåde være effektiv, da vi tolker, at de potentielle ofre stiller sig mindre skeptiske til de beskeder, de modtager, da det ikke er usandsynligt, at de modtager disse beskeder ud fra aktuelle hændelser i samfundet (Cohen & Felson, 1979: 593).

Vi kategoriserer 'dagligdags-virksomheder' som de tilfælde, hvor svindlerne tilpasser deres SMS'er eller mails, så de fremstår som værende afsender fra eksempelvis en region, en kommune eller PostNord. Der er tale om en myndighed eller en virksomhed, som mange danskere benytter sig af eller har abonnement hos. I disse tilfælde udleder vi, at afsenderen benytter elementer tæt knyttet til potentielle ofres hverdag for at vinde potentielle ofres tillid. Et eksempel på dette ses i følgende citat fra Sabine:

> *Der er rigtig mange af dem, der bliver svindlet på den her måde, de har lige oplevet noget eller venter på en pakke fra PostNord, så derfor klikker de på den her SMS fra PostNord og klikker på linket, fordi "Nå ja det er jo rigtig nok [...] Eller at det er fra Dao. Det er også med, når en pakke kommer "du skal bare lige bekræfte" eller "du skal lige betale 7 kroner for at få den". Men du skal jo aldrig nogensinde betale penge for at modtage en pakke.* (Bilag 7: 5).

Sabine påpeger, at svindleren kan anvende PostNord eller DAO som afsender, når de kommunikerer ud til potentielle ofre. Typisk indgår et link, hvor offeret skal bekræfte eller betale 7 kroner for at få pakken. Vi tolker ud fra Sabines udsagn, at gerningspersonerne benytter sig af elementer, som er tæt knyttet til den generelle befolknings hverdag. Ved at bruge elementer som potentielle ofre er bekendt med ud fra deres daglige rutiner, udleder vi, at det er en måde, hvorpå svindleren opnår potentielle ofres tillid. Ud fra rutineaktivitetsteorien påpeges det, at sociale og teknologiske forandringer forårsager nye kriminalitetstendenser for motiverede forbrydere, hvilket er gældende i disse smishing-beskeder med falske fragtvirksomheder (Cohen & Felson, 1979: 589) Derudover er brugen af disse falske fragtvirksomheder en måde, hvor gerningspersoner fanger ofres opmærksomhed og skaber en følelse af, at beskeden er relevant, hvilket kan være en af grundene til, at ofrene vælger at reagere på beskeden. Ligesom ved vishing benytter gerningspersonen noget familiært fra de potentielle ofres hverdag. Vi antager, at når potentielle ofre ser noget fra en kendt kilde, er de

mere tilbøjelige til at stole på indholdet. Dette understøttes af den eksisterende forskning fra Rahman et al., der blandt andet har undersøgt personers tilbøjelighed til at besvare smishing afhængigt af afsenderen (Rahman et al., 2022: 52). Vi tolker, at gerningspersonen forsøger at skabe en følelse af relevans i beskeden, så de potentielle ofre bliver nødt til at reagere. Relevans og inddragelsen af en potentielt kendt kilde fra offerets hverdag er nogle elementer i smishing, som får ofrene til at trykke på dette link for at løse problemstillingen. I dette tilfælde er problematikken, at ofrene skal betale 7 kr for at modtage deres pakke. Det er værd at nævne, at det naturligvis ikke er alle ofre, som falder for disse falske fragtbeskeder. Vi antager, at de egnede mål består af den målgruppe, som lige har bestilt en pakke eller dem, som venter på en pakke. I forlængelse af dette udleder vi, at de sociale strukturer i form af rutineaktiviteter (Cohen & Felson, 1979: 593) spiller en stor rolle i gerningspersoners modus operandi ved smishing. Der kan argumenteres for, at svindlerne i deres forberedelse tilpasser deres indhold i beskederne ud fra elementer i den almene borgers hverdag, hvilket fremgår af Sabines citat på forrige side (Bilag 7: 5).

Ovenstående analyse omhandler svindlerens identificering af metoder til at franarre offeret. Som tidligere nævnt udnytter svindleren samfundstendenser i deres kommunikation og udgiver sig for at være offentlige myndigheder og 'dagligdags-virksomheder'. Dertil er det ligeledes relevant at kortlægge og analysere hvilke handlinger, der finder sted forud for den kriminelle handling, hvilket vil blive uddybet i følgende afsnit om pre-activity.

6.2.2. Pre-activity

I forrige afsnit introducerede vi det forberedende stadie ved phishing og smishing. I dette afsnit følger stadie to af crime scriptet, som dækker over de første aktiviteter (pre-activities) i smishing- og phishing-angreb. Før-aktiviteterne præsenteret i dette afsnit er afgørende for, at selve den kriminelle handling (activity) kan finde sted (Chainey & Berbotto, 2021: 282). Afsnittet er delt op i de forskellige før-aktiviteter, som vi har identificeret i vores empiri.

Udarbejdelse af falske hjemmesider

Som nævnt i problemfeltet (afsnit 2.2) bliver der på globalt plan dagligt etableret 65.000 nye falske hjemmesider, som anvendes ved phishing og smishing. Oprettelsen af disse hjemmesider er essentielle i gerningspersoners modus operandi, da de gennem disse falske hjemmesider kan tilegne sig ofres personfølsomme oplysninger, som derefter kan misbruges (Leukfeldt & Jansen, 2015: 175).

I afsnittet om preparation nævnte vi, at der bliver svindlet ud fra samfundstendenser, idet der blev udsendt falske SMS'er i forbindelse med Covid-19. Disse SMS'er indeholdt et link, som førte til falske hjemmesider, hvor potentielle ofre skulle logge ind på diverse måder og dermed afgav deres personfølsomme oplysninger. Falske hjemmesider ved phishing og smishing er afgørende for activity, da det er her, databedrageriet og den økonomiske berøvelse finder sted.
Ifølge Frederik fra Fyns Politi foregår smishing på følgende måde. Der er tale om:

> "*en standardiseret sms-besked, der bliver tilsendt til forurettede. Beskeden indeholder et link. Ved at klikke på linket bliver man f.eks. bedt om at logge ind med MitID/NemID. Når man taster oplysningerne ind, kan gerningsmændene se, at oplysningerne bliver tastet, hvorefter oplysningerne kan misbruges.* (Bilag 11: 55).

Frederik påpeger samtidigt, at det er i disse tilfælde, de har håndteret sager, hvor afsenderen udgiver sig for at være fra *"hospitaler, regioner eller andre offentlige instanser"* (Bilag 11: 53). Disse er institutioner, som på forhånd har en eksisterende tillid hos borgerne.
Som det fremgår af Frederiks første citat, indeholder smishing-beskeden et link, der fører til en ekstern hjemmeside. Vi mener, at oprettelsen af en sådan hjemmeside er en pre-activity, der muliggør activity. Vores data indikerer, at linket til hjemmesiden *kan* være fyldt med malware (Bilag 7: 4), mens den eksisterende forskning understreger, at anvendelsen af malware ved smishing er forholdsvist udbredt (Choi & Lee, 2021: 6). Det er denne malware, der giver adgang til de personfølsomme oplysninger (hacking). Essensen i anvendelse af links – med eller uden malware – er at få adgang til personfølsomme oplysninger i håb om økonomisk vinding.

Hjemmesiden er det element, som gerningspersoner anvender til at overbevise potentielle ofre til at logge ind med deres oplysninger, hvorefter gerningspersonerne kan tilegne sig disse oplysninger og misbruge dem. Derfor er det vigtigt for gerningspersonerne at oprette en hjemmeside, som fremstår professionel og troværdig. Søren bekræfter ovenstående, idet han påpeger, at "*Svindler efterligner noget som offeret kender/forventer (mail fra firmaer, det offentlige eller venner) og får offeret til at klikke på links i beskeden. Det som kunder ser ved at klikke på linket er ofte ret professionelt designet."* (Bilag 10: 47).
Disse hjemmesider er et element, som er designet til at narre brugerne til at tro, at de er inde på en legitim hjemmeside. Som nævnt i ovenstående citat af Søren fremstår hjemmesiderne professionelt designet, hvilket kan indikere, at svindlerne forsøger at kopiere udseendet og designet fra andre kendte hjemmesider (eksempelvis Region Syddanmark) for at narre potentielle ofre. Vi tolker, at det er befolkningens tillid til disse organisationer, som lokker de

egnede mål til at indtaste personlige oplysninger, som senere kan blive misbrugt. Ud fra ovenstående udleder vi, at brugen af smishing-hjemmesider er en metode, som giver svindlerne adgang til personlige oplysninger om de egnede mål.

Dermed kræver det ligeledes en motiveret forbryder, som skal planlægge alle disse elementer for at fuldføre den kriminelle handling (Cohen & Felson, 1979: 590). Indledningsvis ved phishing og smishing handler det om at fange de potentielle ofres opmærksomhed. Dette kan lykkes, når der er et fravær af en egnet beskytter. Der kan argumenteres for, at der er en forskel på at blive udsat for kriminalitet i den fysiske kontra den digitale verden. Vi vil argumentere for, at fraværet af egnede beskyttere er større digitalt end fysisk, da offeret og gerningspersonen ikke er lige så afhængig af at være i samme tid og rum digitalt, som man er i den fysiske verden. Når det lykkes at fange et potentielt offers opmærksomhed, er det gennem denne "professionelt designede" hjemmeside, at de motiverede forbrydere tilegner sig nogle personfølsomme oplysninger og opnår økonomisk vinding. Som påpeget i ovenstående citat (Bilag 10: 47) er svindlerne gode til at lave troværdige efterligninger. Dette gælder ikke blot hjemmesider, men ligeledes ved telefonnumre og e-mails. Dette vil vi uddybe i det følgende afsnit, hvor andre metoder inden for phishing og smishing vil blive præsenteret.

Spoofing af mails og telefonnumre

En stor del af gerningspersonens fremgangsmåde er at skabe tillid til modtageren. Som nævnt i ovenstående handler det om at skabe tillid gennem efterligningen af en hjemmeside. Derudover er det væsentligt, at afsenderen fremstår troværdig. Dette kommer til udtryk ved spoofing af telefonnumre og e-mails, der har samme manipulerende element som falske hjemmesider. Finn fra Fyns Politi påpeger følgende til et spørgsmål om phishing:

> *"Og så er ideen jo også [...] du laver bare den der ændring i syntaksen. Så er spørgsmålet, hvordan slører man det så? Jamen man foregiver bare et navn, så det ligner så tæt på som overhovedet muligt. Og ved mailen. Så det ser ud som om, det er den rigtige afsender. [...] der kommer to i'er eller to e'er, hvis det er sådan et snedigt navn, så kan man godt lige overse det, hvis man bare lynhurtigt læser mailen igennem. Så på den måde tror jeg ikke, at det bare er sådan noget, som folk bare lige gør."* (Bilag 9: 32).

På denne måde forsøger svindlerne ved phishing at efterligne troværdige personer/ virksomheder. Som det fremgår i citatet forsøger svindleren at efterligne navnet (mailadressen), så det ligner den reelle afsender mest muligt. En generel tendens i IT-relateret kriminalitet, som

vi ser i vores data, er, at størstedelen af metoderne handler om at manipulere med offeret gennem social engineering (Bilag 9: 30; Case 1; Case 2). Det vil sige, at gerningspersoner forsøger at skabe en følelse af tillid hos det potentielle offer, som typisk udføres ved, at svindleren udgiver sig for at være en betroet person eller organisation.

Dét, at svindleren udgiver sig for at være en legitim afsender, kommer ligeledes til udtryk ved smishing. Her er der tale om spoofing af telefonnumre, således at afsenderen fremstår under et navn eller et andet telefonnummer. Dette har vi uddybet i afsnittet om activity ved vishing (afsnit 6.1.3).

Ud fra vores data kan vi se, at svindlerne ved smishing omkoder deres telefonnumre til et navn – eksempelvis "SydBank", hvorefter fremadrettede beskeder vil blive blandet med beskeder fra den faktiske afsender, Sydbank (Bilag 7: 14; Bilag 10: 47). Søren påpeger, at *[...] en SMS lægger sig normal i samme "tråd" som det offeret tidligere har modtaget (Falsk fragt besked lægger sig i samme tråd som tidligere beskeder fra GLS/PostNord/DAO – eller fra banken) – så kunden er mere tilbøjelig til at tro, at afsender er den rette.* (Bilag 10 : 47).

Ovenstående citat kommer ind på, hvordan svindlerne kan ændre deres afsendernummer og placere deres beskeder i samme tråd, som den reelle afsender – eksempelvis GLS, DAO eller banken. De strukturelle forandringer i form af digitaliseringen har muliggjort, at svindlere i højere grad kan udgive sig for at være betroede institutioner/ virksomheder gennem spoofing. Som nævnt i afsnittet om falske hjemmesider er forskellen i digitale og fysiske rum en faktor, der påvirker, hvorvidt en kriminel handling kan finde sted. Her er der igen tale om et fravær af egnede beskyttere i det digitale rum. Vi argumenterer for, at kriminalitet i det digitale rum er mindre synlig end i det fysiske, og dermed er det ikke givet, at der er nogen personer til at intervenere. Vi tolker, at omkodningen af telefonnummeret i samspil med den troværdige hjemmeside er vigtige elementer, når gerningspersonerne skal vinde ofrenes tillid. Disse to faktorer anses for at være essentielle i gerningspersonens manipulation af offeret.

6.2.3 Activity

Det tredje stadie i vores crime script om phishing og smishing er activity (selve den kriminelle handling). Dette er hovedaktiviteten (Keatley, 2018: 130) i phishing og smishing, hvor gerningspersonen forsøger at få ofrene til at videregive personfølsomme oplysninger. I dette afsnit vil vi anvende vores fund fra preparation og pre-activity til at fortolke på case 2, 3 og 4.

Ud fra vores data kan vi se, at phishing på tidspunktet for vores undersøgelse ikke er lige så dominerende som smishing. Flere af vores respondenter er enige i, at phishing-mails typisk indeholder links, samt at afsender er en kilde, de kender – eksempelvis offentlige myndigheder eller personlige omgangskreds, hvilket ligeledes er nævnt i afsnittet om preparation (Bilag 10: 47; Bilag 8: 22). Ved at udgive sig for at være "bekendte" eller offentlige myndigheder forsøger gerningspersonerne at ramme en så bred målgruppe som muligt gennem massekommunikation.

De metoder, som er mest fremtrædende i vishing, er ligeledes gennemgående ved phishing og smishing. Hyppigt udgiver svindlerne sig for at være fra en offentlig myndighed eller velkendte firmaer (Bilag 10: 47). Typisk indeholder SMS'erne og e-mailene links til hjemmesider oprettet af svindlerne. Disse hjemmesider ligner de originale hjemmesider, hvilket kan få potentielle ofre til at sænke deres parader og videregive personfølsomme oplysninger, som kan misbruges af gerningspersonerne. Ofte vil afsenderen på smishing-SMS'en fremgå som en virksomhed eller en myndighed, som de potentielle ofre kender eller benytter sig af (eksempelvis PostNord eller en region). På denne måde skaber svindlerne en falsk troværdighed hos ofrene, hvilket kan medvirke til, at ofrene stiller sig mindre skeptiske til den pågældende e-mail eller SMS. Alt dette leder til, at det bliver nemmere for gerningspersoner at franarre ofre og dermed tilegne sig personlige oplysninger, som kan misbruges.
I dataen kommer Frederik fra Fyns Politi med et eksempel, hvor svindleren udgiver sig for at være en offentlig myndighed med henblik på at franarre offeret sine personlige oplysninger. Dette ser vi i case 2 fra Sydbank, som vi vil uddybe på næste side. Casen foregår på samme vis, som Frederik giver følgende eksempel på:

> *"Der forekommer sager, hvor gerningsmændene kontakter borgere via sms og udgiver sig for at være fra hospitaler, regioner eller andre offentlige instanser. Sms-beskeden indeholder et link og ved login bliver forurettede f.eks. bedt om NemID/MitID oplysninger. På denne måde kommer gerningsmændene i besiddelse af forurettedes personoplysninger."* (Bilag 11: 53).

De motiverede forbrydere ved phishing og smishing benytter sig typisk af massekommunikation via e-mails og SMS'er (Center for Cybersikkerhed, 2020: 3-4; Bilag 9: 33; Bilag 10: 48). Denne form for fremgangsmåde kan virke vilkårlig, hvilket kan indikere, at udvælgelsen af potentielle ofre er mere tilfældig sammenlignet med vishing. I vores data ser vi dog tilfælde, hvor gerningspersonen er en bekendt til offeret eller udgiver sig for at være en

bekendt, der har brug for hjælp. Anvendelsen af massekommunikation understøttes ligeledes af Sabine, der påpeger følgende:

> *"man har abonnement ved dem i forvejen eller har lige haft. Vi skal også bare huske, at de her svindlere de sender rigtig mange SMS'er ud til folk. Der er nogle af dem, der hopper i, men der er også mange, der ikke hopper i. [...] Så det er jo ikke fordi, de får hit hver gang, de gør det her. Det må I slet ikke tro."* (Bilag 7: 6).

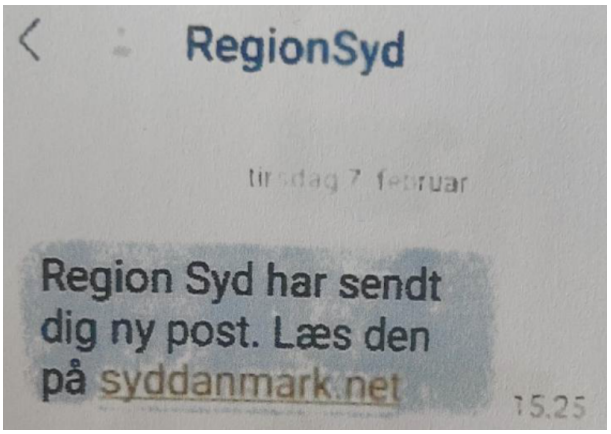
Ud fra ovenstående citat tolker vi, at de motiverede forbrydere bruger massekommunikationen til at nå ud til så mange potentielle ofre som muligt på kort tid, hvilket øger chancerne for at finde egnede mål, som falder for disse beskeder. Selvom gerningspersonerne sender mange SMS'er ud til befolkningen, er det ikke ensbetydende med, at denne kommunikation har den tilsigtede effekt på de potentielle ofre. Dermed kan vi udlede fra det ovenstående citat og ud fra rutineaktivitetsteorien, at de motiverede forbrydere benytter spredehagl til at ramme tilfældigt egnede mål, således at de kan tilegne sig de potentielle ofres oplysninger med sigte om økonomisk vinding (Cohen & Felson, 1979: 590). Et eksempel på anvendelsen af spredehagl, hvor gerningspersonen udgiver sig for at være fra en myndighed, ses i case 2 fra Sydbank omhandlende smishing. I denne case formoder vi, at der er anvendt massekommunikation med en region (en offentlig myndighed) som afsender. Casen vil blive uddybet i det følgende.

Case 2: Smishing fra "RegionSyd"

Tabel 6: Casebeskrivelse

Case 2 fra Sydbank omhandler smishing, hvor en mand i midt 50'erne modtager en SMS fra "RegionSyd". SMS'en indeholder et link til en hjemmeside. Forurettede har samme dag været til fysioterapi og tror, at SMS'en omhandler det tilskud, vedkommende skal have fra regionen. Forurettede påpeger selv en overvejelse om, hvorvidt dette er et tilfældigt sammentræf. Om aftenen tilgår forurettede linket, hvor han kommer ind på en hjemmeside. Forurettede påpeger, at hjemmesiden fra linket ligner Region Syddanmarks hjemmeside. På hjemmesiden logger han ind med MitID for at læse posten fra "RegionSyd". Udover at der er forsinkelser i godkendelsen af MitID, hvilket forurettede studser over, modtager forurettede flere MitID-anmodninger efterfølgende, og han godkender dem alle. Senere modtager forurettede SMS'er om, at der er sket ændringer på MitID, samt at vedkommendes mastercard er blevet tilknyttet Apple Pay. Der er ligeledes forsøgt at straksoverføre beløb til en fremmed konto, og der er overført penge fra forurettedes konti af to omgange til en fremmed konto på i alt 11.494,58 kroner.

Figur 5: Udklip fra Case 2



Kilde: Case 2

Af case 2 udleder vi ud fra rutineaktivitetsteorien, at den motiverede forbryder forsøger at udnytte ofrets tillid ved at udgive sig for at være en offentlig myndighed. Gennem Region Syd giver svindleren offeret nogle forhåbninger om, at offeret kan få et tilskud, hvilket hænger sammen med, at offeret lige har været til fysioterapi. Som det fremgår af udklippet lader afsenderen til at være en region i Danmark. I afsnittet om pre-activity præsenterede vi udarbejdelsen af falske hjemmesider og spoofing af mails og telefonnumre. Spoofing af afsendernummer er med til at øge gerningspersonens troværdighed. I case 2 fremgår afsendernummeret under navnet "RegionSyd", hvilket vi tolker har haft en manipulerende effekt på offeret. Vi udleder, at spoofing af afsendernummer er en vigtig del af svindlerens pre-activity, idet svindleren skaber en falsk troværdighed hos afsenderen. Dette forarbejde af svindleren er et af elementerne, som leder til muliggørelsen af den kriminelle handling (activity). Troværdigheden af en afsender, der fremstår legitim, er med til at understøtte troværdigheden i indholdet af phishing- og smishing-beskeden. Hvis potentielle ofre finder afsenderen legitim, tolker vi, at de er mere tilbøjelige til at følge linket til den falske hjemmeside.

Svindlerne anvender også falske hjemmesider til at få offeret til at videregive personfølsomme oplysninger. Falske hjemmesider ved phishing og smishing er afgørende for activity, da det er her, databedrageriet og den økonomiske berøvelse finder sted. Et eksempel herpå ser vi ligeledes i vores data, hvor Sabine fra Sydbank nævner case 2 under interviewet:

> *"I den sag, jeg viste jer tidligere, hvor han tror, det er en SMS fra Region Syd, hvor han klikker på linket og går ind [...]. Altså det ser ud som om, det er Region Syddanmarks hjemmeside, han kommer ind på. De er jo fantastisk gode til at lave efterligninger af*

tingene i dag. Så de tror, det her det er hjemmesiden. Og så logger han jo på. Fordi han tror stadig, det er det". (Bilag 7: 4).

Citatet indikerer, at disse falske hjemmesider er gode efterligninger af den originale hjemmeside. Dette nævner forurettede i case 2 ligeledes. Som nævnt ovenfor er troværdighed en afgørende faktor for, at den kriminelle handling kan gennemføres. Spoofing af telefonnummer og en vellignende hjemmeside er vitale elementer for, at svindleren opretholder sin falske rolle som myndighed eller virksomhed, således at potentielle ofre ikke fatter mistanke.

Derudover er der nogle sociale faktorer, som medvirker til, at den kriminelle handling opstår. Vi tolker ud fra vores data, at svindleren benytter sig af elementer fra de almene borgeres rutineaktiviteter (Bilag 7: 6; Bilag 11: 65). I føromtalte case lykkes det for gerningspersonen at narre offeret gennem vedkommendes rutineaktiviteter i form af, at offeret har været til fysioterapi. Her er det relevant at overveje, om svindleren i forvejen vidste, at offeret har været til fysioterapi, eller om det er en tilfældighed, at netop denne besked ender hos det pågældende offer. Det kan yderligere pointeres, at forurettede bliver et egnet mål, idet vedkommende lige har været til fysioterapi. Som nævnt tidligere i svindlerens pre-activity benytter de sig af massekommunikation af SMS'er og e-mails, hvor de forsøger at sende indhold, som er tæt forbundet med den almene borgers hverdag. Det vil sige, at intentionen med disse phishing- og smishing-beskeder er gennem spredehagl at ramme en så bred målgruppe som muligt. Det gør målgruppen sværere at definere sammenlignet med vishing-sager og i de smishing-sager, hvor man bliver svindlet af en, der udgiver sig for at være en bekendt. Sidstnævnte uddybes senere i dette afsnit under case 3 og case 4. Hertil vil vi bemærke, at der findes få tilfælde, hvor svindleren rent faktisk er en bekendt og ikke blot én, der udgiver sig for at være det (Bilag 7: 11).

Case 2 har vist os, at processen for phishing og smishing følger nogle stadier, som er afgørende for, at angrebet lykkes. Det forudgående arbejde (pre-activity) i form af spoofing og udarbejdelsen af en professionel hjemmeside er med til at øge troværdigheden hos gerningspersonen, således at potentielle ofre bliver manipuleret under activity. Ud fra tidligere forskning kan vi se, at reaktionen på smishing sker ud fra enten frygt eller troen om belønning (Rahman et al., 2022: 51). I tilfældet med case 2 er der tale om troen om belønning, idet forurettede tror, han skal have et tilskud fra regionen. Dette er med til, at han falder for svindelnummeret.

Smishing fra "bekendte"

I dette afsnit præsenteres de tilfælde, hvor gerningspersonen bag smishing udgiver sig for at være en person, som offeret kender. I vores to cases fra Sydbank er der tale om, at gerningspersonerne er henholdsvis en, der udgiver sig for at være veninde til forurettede (case 3) eller en der udgiver sig for at være forurettedes søn (case 4). Vi har fundet frem til faktorer, som indgår i smishing fra "bekendte", og dette er ikke noget, vi har set uddybet i den eksisterende forskning. I det følgende vil vi præsentere case 3 og 4 med smishing fra "bekendte" og koble vores interviewdata, eksisterende forskning og rutineaktivitetsteorien herpå.

Case 3: Smishing fra en "veninde"

Tabel 7: Casebeskrivelse

I case 3 fra Sydbank er forurettede en person i midt 60'erne. Forurettede bliver kontaktet over Messenger af en veninde, der vil låne forurettedes telefonnummer som del i en konkurrence, hvor begge kan opnå økonomisk udbytte. For at få gevinsten fra konkurrencen overført bliver forurettede bedt om at oplyse kort og kontonummer til veninden, hvorefter forurettede selv skal godkende kommende anmodninger i MitID. Forurettede beskriver, at godkendelserne med MitID tager lang tid, fordi der er systemfejl. Forurettede modtager herefter SMS'er fra Sydbank om, at der er foretaget reservationer på forurettedes kort, og senere at kortet er spærret. Under forløbet modtager forurettede i alt 10 beskeder fra banken om, at kortet er blevet anvendt i udlandet. Forurettede kontakter sin veninde, der beder forurettede om ikke at foretage sig noget eller kontakte Sydbank. Veninden forsikrer forurettede om, at reservationerne blot er af sikkerhedsmæssige årsager, og at disse vil blive slettet, når gevinsten fra konkurrencen er overført. Forurettede ender med at blive franarret i alt 8.510 kroner fordelt på over 30 omgange inden for 2 ½ time.

I ovenstående case antager vi, at venindens Messenger er blevet hacket, således at det ikke er forurettedes egentlige veninde, der skriver, men det er en anden person, der skriver gennem venindens profil. Ud fra rutineaktivitetsteorien fortolker vi, at den motiverede forbryder benytter personlige relationer til at opnå forurettedes tillid i ovenstående case. Idet gerningspersonen udgiver sig for at være en bekendt, er tilliden på forhånd etableret mellem offer og gerningsperson. Dette gør det nemmere for den motiverede forbryder at tilegne sig personlige oplysninger og økonomisk gevinst. Dermed tolker vi, at forurettede er et egnet mål i ovenstående tilfælde, da hun gennem en personlig relation til "afsenderen" forholder sig mindre skeptisk til, hvad "veninden" sender.

I case 3 antager vi, at svindlerens forberedelse består af at få adgang til forurettedes venindes konto, således at vedkommende kan udføre smishing-angrebet. I afsnit 6.2.1 og 6.2.2 har vi præsenteret det arbejde, der laves forud for den kriminelle handling. Elementerne af preparation og pre-activity i case 3 bærer præg af hacking og indgår ikke i vores crime script, da det i vores data ikke nævnes i nogle af interviewene men udelukkende i denne case. Med udgangspunkt i denne antagelse om hacking udleder vi, at svindleren er en motiveret forbryder, fordi vedkommende laver en tidsmæssig investering i at opnå adgang til venindens Facebook-konto. Den tidsmæssige investering kommer også til udtryk i casen, idet svindleren bruger 2 ½ time på at narre offeret til at godkende mere end 30 MitID-anmodninger, der samlet ender med at koste forurettede 8.510 kroner.

I den eksisterende forskning finder vi, at personer reagerer på smishing-beskeder ud fra frygt eller troen om belønning (Rahman et al., 2023: 51). Ud fra case 3 antager vi, at forurettede er interesseret i at hjælpe veninden, fordi der er tale om en konkurrence med økonomisk udbytte som gevinst. Troen om belønning er samtidigt en faktor, som vi antager har indflydelse på, at forurettede godkender mere end 30 MitID-anmodninger. Vi antager, at havde gerningspersonen ikke været en bekendt, havde forurettede været mere skeptisk. Dette udleder vi af interviewet med Søren, der påpeger, at *"Svindler efterligner noget som offeret kender/forventer (mail fra firmaer, det offentlige eller venner)"* (Bilag 10: 47).

Søren understreger samtidigt, at den typiske målgruppe for disse svindelnumre er personer på 60 år og derover – herunder især ældre kvinder (Bilag 10: 49). Forurettede i vores case er i midt 60'erne. Ud fra Sørens udtalelse fortolker vi, at forurettede i casen er målrettet af den motiverede forbryder. Dette faktum i kombination med, at forurettede agerer ud fra troen om belønning, gør forurettede til et egnet mål. Den eksisterende tillid blandt forurettede og veninden er et element, der er med til at opretholde forurettedes rolle som egnet mål.

Ud fra ovenstående case pointerer vi, at der er et fravær af egnede beskyttere. Som udgangspunkt består egnede beskyttere af personer, som kan gribe ind og forhindre den kriminelle handling (Cohen & Felson, 1979: 590). I dette tilfælde kan der argumenteres for, at forurettedes veninde under normale omstændigheder ville være en egnet beskytter, idet hun er en person, som forurettede stoler på og i den forstand kan spørge til råds i tvivlsomme situationer. Dette er ikke tilfældet i ovenstående case, idet den motiverede forbryder benytter sig af viden om en personlig relation til at franarre vedkommende. I undersøgelsen fra Paraschiv et al. (2021) understreger de, at digitaliseringen i form af internettet og sociale medier har åbnet flere muligheder for svindlerne, hvilket har været med til at øge phishing (og

smishing) (Paraschiv et al., 2021: 394). Ud fra rutineaktivitetsteorien er forklaringen herpå en ændring i borgernes rutineaktiviteter. Man kommunikerer med venner over digitale platforme frem for at mødes fysisk. Dette placerer borgerne i en position, hvor det digitale rum bliver deres sted at færdes. Som nævnt i afsnit 6.2.2 er fraværet af egnede beskyttere i det digitale rum større end i det fysiske, da det digitale rum muliggør kriminalitet på afstand. Case 3 er et eksempel på, hvordan svindleren vinder offerets tillid ved at udgive sig for at være en bekendt, hvilket case 4 ligeledes er et eksempel på. Forskellen i de to cases er den faktor, som forurettede handler ud fra – troen om belønning (case 3) eller frygt (case 4) (Rahman et al., 2022: 54-55). Dette vil vi uddybe i følgende.

Case 4: Smishing fra ens "barn"

Tabel 8: Casebeskrivelse

I den fjerde og sidste case fra Sydbank er den forurettede en kvinde i start 80'erne. Hun bliver kontaktet over SMS af en person, der påstår at være hendes søn. "Sønnen" har fået nyt nummer, fordi han har mistet sin telefon. Sønnen beder kvinden (hans "mor") om hjælp til at betale en forfalden gæld på 24.540 kroner med frist på dagen. Sønnen vejleder forurettede til at åbne sin computer og overføre til en konto med straksoverførsel. Hertil oplyser sønnen både et registreringsnummer, kontonummer og referencenummer. Mens forurettede er i gang med at overføre pengene fra sin computer, fortsætter samtalen med sønnen over SMS. Her beder forurettede sønnen om at ringe hende op, men sønnen påstår, at han hverken kan foretage eller modtage opkald før i morgen, fordi telefonnummeret er nyt. Forurettede spørger, om sønnen kan låne "Mettes" (hans partners) telefon til at ringe fra. Denne besked svarer sønnen dog ikke på. Forurettede kan ikke overføre beløbet grundet en daglig beløbsgrænse på 10.000 kroner, som hun selv har sat på sin netbank, hvorfor sønnen beder hende sende de 24.540 kroner over flere omgange. Han lover, at han vil ringe til forurettede i morgen. Undervejs i samtalen bliver forurettede bekymret og spørger, om sønnen kan komme fysisk hjem til hende, så de kan overføre beløbet sammen og tale om det. Hertil svarer sønnen *"Jeg ville ikke have spurgt dig, hvis det ikke var vigtigt."* (Bilag 12.d: 78). Forurettede overfører 10.000 kroner, og fordi hun ikke kan hæve sin beløbsgrænse, spørger sønnen, om han må betale resten med hendes kort. Forurettede sender de 16 cifre på kortet, udløbsdato og kontrolcifre. Herefter ændrer sønnen medie, således at samtalen fortsætter på WhatsApp. Her undskylder sønnen for besværet og lover, at det kun vil tage et par minutter mere. Han vejleder forurettede i at bekræfte transaktionerne i MitID-app'en. Forurettede bekræfter flere anmodninger i MitID. Imens spørger sønnen efter det postnummer, som er knyttet til kontoen.

Han påstår, at overførslen ikke kan godkendes, fordi det angivne postnummer er forkert. Herefter informerer sønnen om, at forurettedes kort vil blive spærret, og beder forurettede om selv at kontakte banken og fortælle dem, at det var forurettede selv, der foretog overførslen. Forurettede bliver bekymret spørger: *Kan du ikke komme hjem i morgen tidlig? Kan jeg sove roligt. Er du rodet ind i noget?"*, hvortil "sønnen svarer*"Nej, jeg har det fint mor, du skal ikke bekymre dig* ❤️. *Få noget søvn, vi tales ved imorgen* ❤️❤️*"* (Bilag 12.d: 75).
Undervejs i hele samtalen spørger sønnen ind til morens velbefindende, og hvordan hendes dag har været. Han sender løbende emojis i form af hjerter (❤️). Selve samtalen varer omkring 9 timer fra kl. 16.00 - 01.00 med yderligere opfølgende beskeder den næste dag. Her beder sønnen om, at samtalen ikke skal nævnes for "Mette". Sønnen lover at betale beløbet tilbage den følgende torsdag.

I ovenstående case fremgår det, at forurettede nærer stor tillid til sin søn. Ved besøget hos Sydbank gennemgik vi casen (se metode, s. 43). Her blev vi informeret om, at sønnen i forvejen har fuldmagt til morens konti og netbank, og han plejer at hjælpe hende med disse anliggender. I ovenstående case har gerningspersonen anvendt viden om denne tillid mellem mor og søn til egen økonomisk vinding. Sagt ud fra rutineaktivitetsteorien har gerningspersonen fjernet den "egnede beskytter" ved selv at overtage denne rolle, som normalvis kan tilskrives forurettedes egentlige søn. Yderligere nævner svindleren i løbet af samtalen, at det skal holdes imellem dem, og at "Mette" ikke skal finde ud af det. Man kan argumentere for, at dette fortrolighedsrum mellem søn og forurettede ligeledes er med til at fjerne den "egnede beskytter".

Flere steder i interaktionen forsøger svindleren at skabe en tryghedsfornemmelse. Vi antager, at svindleren gerne vil have, at forurettede ikke fatter mistanke om, at det ikke er hendes egentlige søn. Tryghedsfornemmelsen kommer til udtryk i brugen af hjerter og i de beskeder, hvor "sønnen" spørger ind til forurettedes velbefindende og viser interesse i det, hun skriver.
I skærmbilledet på næste side ses et udklip fra samtalen. Her fremgår den tryghedsfornemmelse, som "sønnen" forsøger at skabe til forurettede. Han er betænksom og personlig gennem brugen af hjerter. Ud fra skærmbilledet udleder vi, at der for forurettede ikke er grund til at have mistro, da "sønnen" i beskederne forsøger at berolige hende.

Figur 6: Skærmbillede 1[2]

Kilde: Eget arbejde

Derudover tolker vi, at brugen af hjerter også er med til at skabe en beroligende effekt hos forurettede, og at det er et tegn på tillid. Vi antager, at tilliden og det følelsesmæssige bånd, som forurettede har til sin søn, er vitale elementer i svindlerens manipulation af offeret.

Ud fra casen udleder vi, at gerningspersonen er motiveret til at gennemføre forbrydelsen. Dette ses blandt andet i den investering, som gerningspersonen lægger i samtalen og det forudgående arbejde hertil – herunder muligvis køb af et taletidskort (Bilag 9: 36). Gerningspersonen indleder samtalen med at skrive: *"Hej mor, jeg mistede min telefon tidligere. Gem mit nye nummer"* (Bilag 12.d: 73). Sabine påpeger i interviewet, at der findes gerningspersoner, som udelukkende stjæler personlige data for at sælge det videre (Bilag 7: 13).

I den eksisterende forskning kan vi se, at indhentning af personlige oplysninger er del af de crime scripts, der præsenteres (Nguyen, 2022: 233; Leukfeldt, 2014: 241-243). I nærværende case antager vi ud fra Sabines citat, at gerningspersonen har indhentet oplysninger på forurettede forud for smishing-angrebet. Af skærmbilledet fremgår det, at forurettede *"har det ligesom i oktober*" (Bilag 12.d: 75). Her blev hun ligeledes udsat for it-relateret kriminalitet og mistede et større økonomisk beløb. Her er det værd at bemærke, at det er muligt, at gerningspersonen enten har haft kendskab til forurettede fra tidligere, eller at hendes personlige oplysninger sælges blandt svindlere. Samtidigt vil vi bemærke, at vi ikke kan konkludere, om det er tilfældigt, at denne kvinde bliver udsat for it-kriminalitet igen.

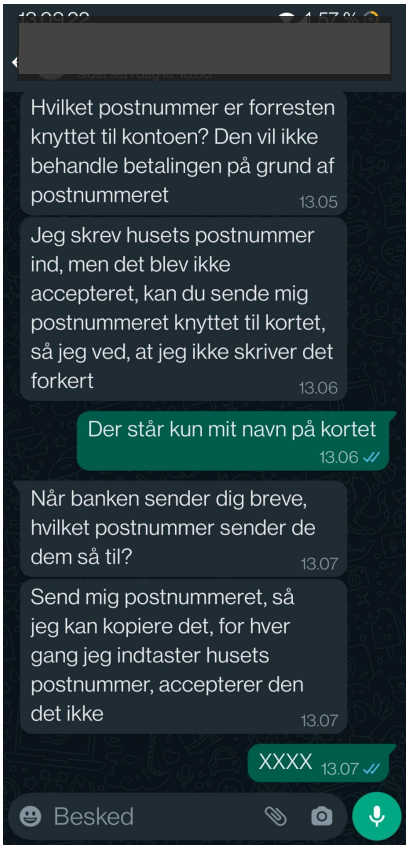
Hvis forurettedes personlige oplysninger bliver solgt blandt svindlere, er dette med til at gøre hende til et egnet mål. Som netop påpeget kan vi dog ikke konkludere dette ud fra vores data, men blot antage, at det er en mulighed ud fra den eksisterende forskning og Sabines ovenstående udtalelse (Bilag 7: 13). Vi tolker, at forurettede er et egnet mål grundet hendes alder. Dette påpegede vi i den første delanalyse under afsnit 6.1.1, hvor vi gennem analysen og respondenternes udsagn kom frem til, at den ældre generation er egnede mål, idet de er mindre

[2] Skærmbilledet er udarbejdet af forfatterne, da dataen fra Sydbank var sløret.

IT-kyndige (ADD, 2021). Manglende IT-kyndighed hos forurettede i case 4 kommer til udtryk ved, at gerningspersonen hjælper forurettede med at foretage overførslerne og vejleder hende i, hvor hun skal skrive registreringsnummer og kortnummer.

Vi bemærker, at forurettede i løbet af samtalen i lav grad forholder sig kritisk til afsenderen og ikke forsøger at ringe til sin søns gamle telefonnummer. Hun foreslår flere gange under samtalen, at "sønnen" skal ringe til hende, eller at han skal komme hjem til hende (Bilag 12.d: 75), men gerningspersonen afværger situationen og skriver eksempelvis: *Jeg har lige registreret denne sim, så jeg kan ikke foretage eller modtage opkald før i morgen, jeg prøvede at ringe til dig tidligere, men det virkede ikke."* **(**Bilag 12.d: 76).
Selvom forurettede til tider forholder sig kritisk i samtalen og gerne vil tale med sin "søn", lykkes det for gerningspersonen at fjerne forurettedes kritiske sans ved at berolige hende og samtidigt modargumentere hende, som det fremgår af citatet. Han påstår, at han har forsøgt at ringe til hende uden held, og dette antager vi er med til, at forurettede stoler på "sønnen".

Figur 7: Skærmbillede 2[3]



Vi vil argumentere for, at denne tillid understøttes af den mængde tid, som gerningspersonen investerer i sit smishing-angreb. Som nævnt varer samtalen omkring 9 timer fra kl. 16.00 - 01.00 med yderligere opfølgende beskeder den næste dag. I vores delanalyse om vishing understregede vi betydningen af den tidsmæssige investering for at opnå tillid hos offeret. I case 4 er den tidsmæssige investering mere omfangsrig end eksemplerne ved vishing (Bilag 9: 34). Noget, som vi ligeledes ser går igen fra vishing, er manipulation gennem en masse informationer eller spørgsmål på samme tid (Bilag 7: 5). Dette kommer eksempelvis til udtryk, når "sønnen" spørger forurettede om hendes postnummer. Dette fremgår skærmbilledet til venstre. Af skærmbilledet kan vi se, at gerningspersonen er meget insisterende på at få forurettede til at oplyse sit postnummer.

Kilde: Eget arbejde

[3] Skærmbilledet er udarbejdet af forfatterne, da dataen fra Sydbank var sløret. Postnummer er anonymiseret.

Vi mener, at dette ikke er afgørende information for at få adgang til forurettedes konto. Vi antager dog, at det er et væsentligt element til manipulation, idet gerningspersonen med 2. besked påpeger, at han ved, hvor forurettede bor (*"Jeg skrev husets postnummer…"*), og dette understreger svindlerens rolle som søn.

Et andet manipulerende element er inddragelsen af sønnens partner, "Mette". Forurettede spørger på et tidspunkt i samtalen, om "sønnen" kan låne "Mettes" telefon til at ringe fra. Dette spørgsmål ignorerer gerningspersonen. Dagen efter smishing-angrebet skriver han igen til forurettede og beder hende om ikke at nævne samtalen for "Mette". Vi antager, at gerningspersonen inkluderer "Mette" i samtalen for igen at understrege sin autenticitet og rolle som forurettedes søn. Dette bliver muligt, idet forurettede ikke tænker over, at hun har nævnt Mettes navn før, og derfor kan gerningspersonen anvende det til sin fordel. På denne måde benytter svindleren den viden, han har opnået gennem samtalen, til at legitimere sig selv som afsender.

Gennem samtalen påvirker svindleren forurettede ved at skabe en følelse af et presserende behov. Finn fra Fyns Politi påpeger, at ingen ønsker at lide et økonomisk tab, og derfor falder barriererne, når man bliver kontaktet af ens "bank" (Bilag 9: 34) I tilfældet med case 4 tolker vi det således, at forurettede har en frygt for, at hendes "søns" gæld bliver større, hvis ikke det betales hurtigst muligt. Den eksisterende forskning påpeger, at man reagerer på smishing ud fra to faktorer, hvoraf den ene er frygt (Rahman et al., 2023: 54-55). Svindleren i case 4 skriver op til flere gange, at forurettede skal skrive, når hun har overført eller spørger direkte ind til, om pengene er sendt. Vi tolker, at svindleren bevidst presser forurettede, således at hun føler sig nødsaget til at handle. Dette kan resultere i, at forurettede foretager impulsive handlinger uden at tænke sig om, hvilket er tilfældet i ovenstående case, idet forurettede overfører 10.000 kroner og efterfølgende oplyser sit kortnummer og kontrolcifre. Denne presserende følelse, som svindleren skaber i samspil med viden om det personlige bånd, som forurettede har til sin søn, er essentielle i gennemførelsen af dette smishing-angreb.

I case 4 kan vi se de fire stadier i crime script. Vi formoder, at gerningspersonen indhenter personlige oplysninger på forurettede (preparation), anskaffer sig et taletidskort (pre-activity), gennemfører sin svindel (activity), og afslutningsvist skifter vedkommende platform, så de skriver sammen på WhatsApp i stedet (activity til post-activity). Dette muliggør en form for flugt (Nguyen, 2022: 238), idet WhatsApp er krypteret, således at samtalen og lokationen for de involverede parter ikke kan tilgås af andre end de involverede parter. WhatsApp gør det dermed muligt for gerningspersonen at afslutte samtalen og gøre brug af/ få udbetalt den økonomiske gevinst.

6.2.4. Post-activity

Fjerde og sidste stadie i vores crime script omhandler den aktivitet, der sker efter activity i den kriminelle handling (Keatley, 2018: 130). Som nævnt i afsnit 6.1.4 ser vi fire forskellige tendenser, hvoraf tendens 1 blev præsenteret og uddybet i delanalyse 1. Tendenserne 2 og 3 vil blive præsenteret i det følgende, mens tendens 4, som blev introduceret i delanalyse 1, vil blive uddybet yderligere i dette afsnit.

Tendens 2: Omsætte pengene til værdigenstande

I tendens 2 omsættes pengene fra svindlen til konkrete værdigenstande. I disse tilfælde får gerningspersoner adgang til forurettedes konto og overfører penge til en person, der har en værdifuld vare til salg. Forurettede har dog intet med købet at gøre. Gerningspersonens identitet sløres ved, at det ikke kan opdages, hvem køberen af varen er, idet forurettede står som betaler af varen.

I case 2 blev forurettede svindlet gennem et link i en SMS. Vi kan ud fra casen se, at udbyttet fra smishing-angrebet er blevet anvendt hos Christian Dior Couture i Paris. Der er desuden overført et beløb til en konto, som den forurettede ikke er bekendt med. Vi kan ud fra casen ikke afgøre, hvem kontoen tilhører, men vi antager, at der enten er tale om en muldyrskonto eller en konto til en person, der har en vare til salg. Sidstnævnte antager vi, fordi forurettedes kort også er anvendt til køb hos Christian Dior Couture. Ved at omsætte beløbet til en materiel genstand ender det sidste led i pengesporet hos butikken med forurettede som betaler. I case 2 har gerningspersonen lavet en overførsel fra forurettedes konto og direkte til Christian Dior Couture. Dette er med til at sløre gerningspersonens identitet, hvilket gør det muligt for svindleren at afslutte den kriminelle handling uden at blive opdaget.

I case 3 har gerningspersonen fået direkte adgang til forurettedes konto. Gerningspersonen slører ligeledes sin identitet ved at anvende udbyttet på Tik Tok, online køb af gavekort samt at have tilknyttet kontoen til et online betalingssystem i Tyrkiet.

På denne måde involverer gerningspersonen ikke en muldyrkonto i de nævnte cases, idet gerningspersonen har adgang til de forurettedes netbank og dermed har mulighed for at foretage en direkte betaling/ overførsel.

I den eksisterende forskning ser vi et eksempel på, at udbyttet fra smishing omsættes til en konkret vare, som det også fremgår i case 2 og 3. I sin undersøgelse finder Nguyen, at der købes genstande for de stjålne bankkortdata (Nguyen, 2022: 233). Dette ser vi ligeledes et eksempel på i vores data, hvor Finn påpeger:

> *"den måde man så kan omsætte pengene, det er så at finde nogen, der er ved at sælge en vare for eksempel.[...] Den forurettedes penge bliver så overført til den person, der har en vare til salg,[...] Så på den måde der, så de penge der nu er fradraget nogen, der er så landet hos en ny forurettet, der så afleverer de varer, og så har du en eller anden let-omsættelig vare i stedet for. Fordi humlen er jo sådan set at få pengene ud i noget håndgribeligt bagefter."* (Bilag 9: 35).

Ud fra ovenstående citat handler det om at omsætte udbyttet fra smishing til noget, som både er håndgribeligt og kan videresælges efterfølgende. Finn nævner blandt andet 'let-omsættelig' i citatet, hvilket vi tolker som, at svindleren køber disse varer med henblik på at omsætte dem til "hvide" penge og bruge dem. En anden måde at omsætte illegalt udbytte fra phishing og smishing ses i forbindelse med bitcoin og andre krypto-valutaer, hvilket vil uddybes i det følgende afsnit.

Tendens 3: Omsætte pengene til bitcoin og andre krypto-valutaer

Vi ser i vores data, at fire ud af fem respondenter nævner, at udbyttet fra databedrageriet i nogle tilfælde omsættes til bitcoin eller andre krypto-valutaer (Bilag 8: 26; Bilag 9: 36; Bilag 10: 61; Bilag 11: 57). Denne form for hvidvask af penge er forholdsvis svær at spore (Bilag 8: 26). Samtidig påpeges det, at penge på bitcoin-børser er juridisk udfordrende at undersøge, fordi de typisk befinder sig i udlandet (Bilag 9: 36). Ud fra den eksisterende forskning kommer Choi og Lee ind på, at svindleren opnår økonomisk vinding ved at benytte offerets kortoplysninger til at købe kryptovaluta (Choi & Lee, 2021: 7). På samme måde som ved tendens 2, kan der påpeges, at svindleren forsøger at forholde sig anonym i forhold til den kriminelle handling. Det handler i høj grad om at være mindre involveret i pengestrømmen, hvorfor direkte tilegnelse af offerets personfølsomme oplysninger og netbank er vigtig for, at svindleren ikke efterlader nogle digitale spor. På trods af at fire ud af fem respondenter nævner omsættelsen til bitcoin og andre krypto-valutaer, er dette ikke et tema, som uddybes yderligere. Dette skyldes, at vi som interviewere ikke har spurgt yderligere ind til temaet, hvilket under analysen har vist sig at være relevant viden. På baggrund af vores problemfelt og eksisterende forskning har vi haft et særligt fokus på muldyr som post-activity, hvilket er en af grundene til, at vi ikke har spurgt nærmere ind til bitcoin og andre krypto-valutaer. Vi kan derfor ikke konkludere mere, end at denne form for post-activity er en mulighed ved phishing og smishing, men det er ikke et område, som vi har undersøgt yderligere. Denne form for hvidvask er som nævnt ovenfor

forholdsvis svær at spore, og ud fra vores data optræder det ikke lige så ofte som i sagerne med anvendelsen af muldyr. Dette vil vi uddybe i det følgende.

Tendens 4: Anvendelse af muldyr

I den fjerde tendens anvendes muldyr til at sløre pengesporet. Ud fra vores data finder vi, at muldyr både kan være rekrutteret af gerningspersonerne og agere bevidst, men de kan også være tilfældige personer, som bliver målrettet i eksempelvis bylivet. Philip, Finn og Frederik påpeger, at de mindre ressourcestærke borgere bliver udpeget som muldyr (Bilag 8: 26; Bilag 9: 43; Bilag 11: 58), hvilket ligeledes fremtræder i den eksisterende forskning (Vedamanikam & Chethiyar, 2020: 24). I den eksisterende forskning nævnes, at muldyr spiller en vital rolle i de kriminelles crime script (j.f. afsnit 3.4), da anvendelsen af muldyr muliggør hvidvaskningen af de kriminelle penge fra phishing og smishing.

I case 4 overfører forurettede 10.000 kroner, og gerningspersonen franarrer selv 14.540, fordi forurettede har oplyst sit kortnummer og kontrolcifre. I og med at der er flere overførsler, antager vi, at der er tale om en muldyrskonto frem for en konto til en person, der har en vare til salg, idet det kan fremstå mistænkeligt med flere overførsler til en sælger. Vi vil ligeledes argumentere for, at gerningspersonens tidsmæssige investering i denne case (9 timer) er et belæg for, at beløbene overføres til en planlagt muldyrskonto frem for en konto, hvor en person har sat en vare til salg. Vi antager, at denne person ikke er involveret i smishing-angrebet. I casen kan vi se, at gerningspersonen franarrer penge både i starten af svindelnummeret og i slutningen. Vi argumenterer for, at dette er endnu en indikator på, at pengene ikke overføres til en sælgers konto, da flere delbetalinger virker omstændigt og potentielt kan vække mistanke hos sælgeren. Vi antager, at gerningspersonen på forhånd har rekrutteret et muldyr, som beløbene overføres til. På denne måde sløres gerningspersonens identitet. Dette er medvirkende til, at muldyret i stedet ender som gerningsperson, hvilket Sabine nævner i nedenstående citat:

> *"Altså det er jo penge, der bliver kanaliseret videre. Og så kommer de jo selvfølgelig hen til de rette personer på et eller andet tidspunkt, men de skal jo ud og have nogle ofre, der kan stille kontoen til rådighed til det"* (Bilag 7: 14).

Af citatet fremgår det, at de personer, der stiller deres konto til rådighed, er dem, hvor pengesporet ender og kan spores til – de bliver "ofre". I den eksisterende forskning påpeger Leukfeldt og Jansen, at muldyr er i bunden af den hierarkiske struktur, når det kommer til databedrageri (Leukfeldt & Jansen, 2015: 175), hvilket indikerer, at det er dem, som

pengesporet ender hos og dem, som er offeret ved en potentielt retsforfølgelse. Vedamanikam & Chethiyar påpeger, at muldyr rekrutteres for at sløre pengesporet og anonymisere gerningspersonerne (Vedamanikam & Chethiyar, 2020: 24) men at disse muldyr ikke indgår i den koordinerede kriminalitet – de bliver igen "ofre", jf. Sabines udtalelse.
Ud fra vores data kan vi se, at muldyr kan opdeles i to typer – dem der agerer bevidst, og dem der agerer ubevidst (Bilag 7: 1; Bilag 10: 49). Muldyr kan både være rekrutteret på forhånd, men de kan også rekrutteres i eksempelvis bylivet. Muldyr, der er rekrutteret på forhånd, agerer bevidst, da der typisk vil være en økonomisk belønning for at agere muldyr (Leukfeldt & Kleemans, 2019: 80).
De personer, som bliver kontaktet i bylivet eller andre steder, udgør den gruppe, som agerer muldyr ubevidst. Her foregår det således, at en gerningsperson, der har et ønske om at hvidvaske penge fra eksempelvis phishing eller smishing, tager kontakt til en person i byen under påskud om, at vedkommendes konto er blevet spærret, eller at vedkommende har mistet sit kort (Bilag 9: 41-42). Finn fra Fyns Politi giver et eksempel på muldyr, der rekrutteres ubevidst i bylivet:

> *"Vi er jo tillidsbaseret, og vi vil gerne hjælpe hinanden. Og så falder folks barrierer, og så. Så får de overført nogle penge. Det sker sådan mange gange, at så siger de "kan du lige hjælpe mig med 1000 kroner?", og det vil folk så gerne være med til, men så får de jo så nogle gange 10.000 eller 20.000 sat ind på deres konto. Så de overtakserer lige pludselig jo. Så kan folk faktisk godt føle sig lidt presset."* (Bilag 9: 42).

De "ubevidste muldyr" er ikke klar over, hvad de medvirker til, og forsøger blot at hjælpe vedkommende med at hæve nogle penge, fordi personen er i nød. Som ovenstående citat indikerer, kan muldyret blive presset ud i en situation, hvor de ikke kan sige nej til at hæve pengene. Ud fra rutineaktivitetsteorien kan gerningspersonen betragtes som en motiveret forbryder, da vedkommende begår en kriminel handling ved at omsætte udbyttet fra phishing og smishing til kontanter, således pengesporet fra den illegitime handling ikke kan spores tilbage til gerninspersonen. Det fremgår ligeledes i citatet, at gerningspersonen er en motiveret forbryder, da vedkommende gennem en koordineret fremgangsmåde presser det "ubevidste" muldyr til at hæve flere penge end aftalt. Det egnede mål kommer også til udtryk i ovenstående citat. Det "ubevidste muldyr", som ifølge Finn's udsagn bliver overtakseret, fremstår som et egnet mål, fordi vedkommende er hjælpsom og har tillid til, at gerningspersonen taler sandt. Rammerne for at rekruttere et "ubevidst muldyr" er i sig selv med til at skabe egnede mål og fjerne de egnede beskyttere. Rammerne for rekruttering foregår i bylivet. Finn påpeger, at de

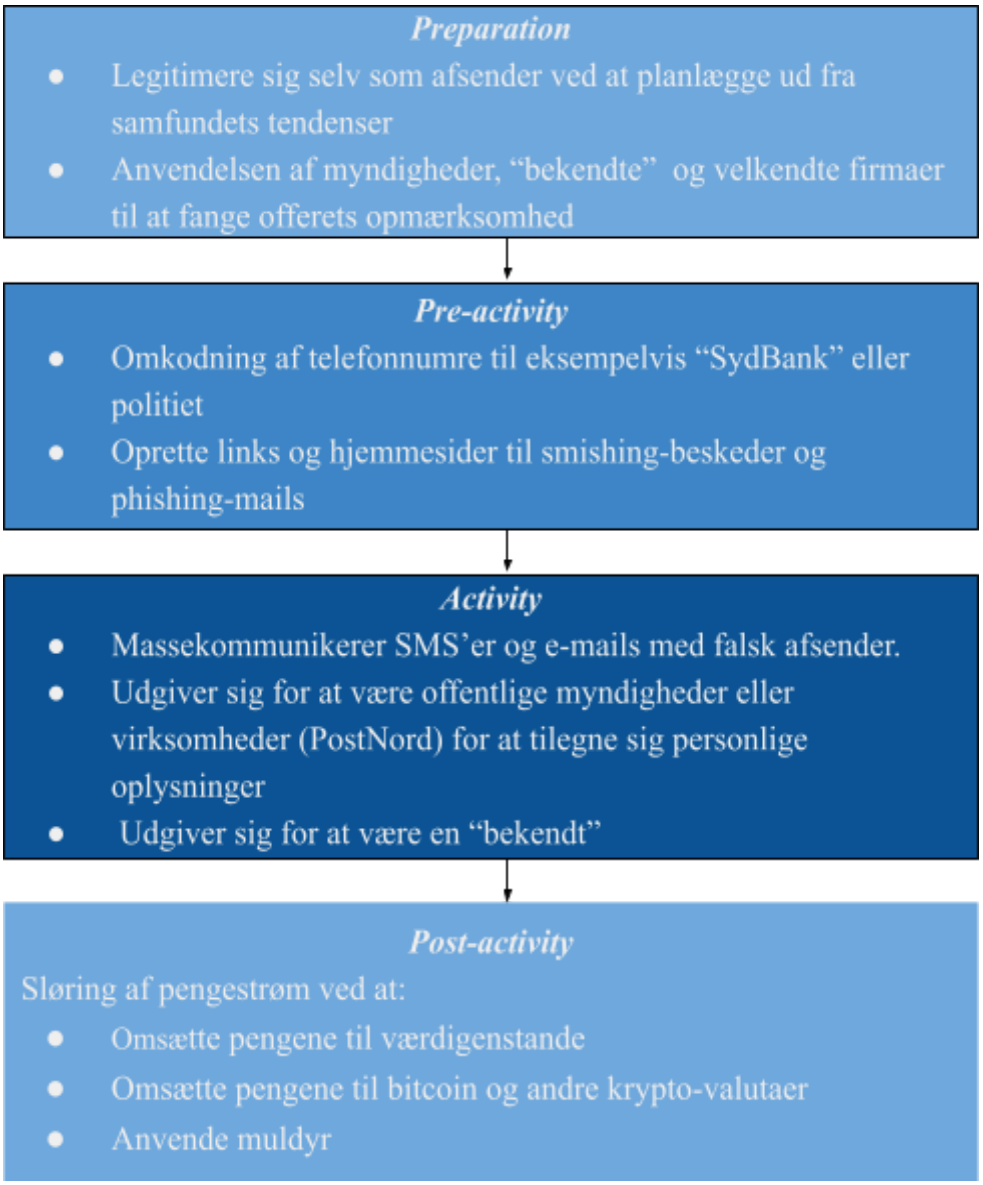
"ubevidste muldyr" typisk er påvirket af alkohol (Bilag 9: 43). Vi antager, at disse egnede mål muligvis også står alene i bylivet i øjeblikket for rekruttering. Uanset om man agerer bevidst eller ubevidst, har muldyr en stor indflydelse på den kriminelle handling, og at udbyttet derfra kan hvidvaskes i det finansielle system. Vi påpeger, at muldyrene fra begge grupper spiller en vital rolle i svindlernes crime script, hvorfor viden om muldyrsaktiviteter er relevant ud fra et forebyggelsesperspektiv. Dette vil vi komme nærmere ind på i vores diskussion.

6.2.5. Opsummering på delanalyse 2

Delanalyse 2 har beskrevet de processuelle stadier, som fremgår i både phishing og smishing. I forberedelsesfasen benyttes der massekommunikation, hvorfor udvælgelsen af ofre ikke er lige så specifik som ved vishing. Gerningspersonerne forbereder deres angreb i dette stadie ud fra samfundstendenser (årsopgørelse) og dagligdags-virksomheder (PostNord), der ligger tæt på den generelle befolknings hverdag. Efter forberedelsesfasen udarbejder gerningspersonen falske hjemmesider samt spoofer e-mails og telefonnumre for at opbygge en troværdighed i de e-mails og SMS'er, som sendes ud til potentielle ofre. Disse elementer gør, at det lykkes gerningspersonen at manipulere med ofrene, hvilket de præsenterede cases (2, 3 & 4) er eksempler på. På denne måde legitimerer gerningspersoner sig selv som afsender ved at massekommunikere beskeder, som ikke er usandsynlige, at potentielle ofre får tilsendt. I andre tilfælde udgiver gerningspersoner sig for at være en bekendt, hvilket kommer til udtryk i case 3 og 4. Her får gerningspersonen den forurettede til at falde for smishing-angrebet ved at lokke med belønning (case 3) eller skabe frygt (eksempelvis for at forurettedes søn er i problemer som set i case 4).

Det sidste stadie (post-activity) er de forskellige tendenser, hvorpå gerningspersonen omsætter de illegitime midler fra phishing og smishing. Det, som er fælles for disse tendenser, er, at gerningspersonerne forsøger at sløre pengesporet, så de undgår at blive afsløret i den kriminelle handling. Den mest omfattende tendens er brugen af muldyr til at hvidvaske disse kriminelle midler, hvor de både kan agere ubevidst og bevidst i den kriminelle handling. De fire stadier af crime scriptet bag phishing og smishing er opsummeret i den følgende figur.

Figur 8: Crime script af phishing og smishing



Kilde: Eget arbejde

Kapitel 7

Diskussion

7. Diskussion

I dette kapitel vil vi diskutere vores empiriske fund samt de metodiske valg, der har muliggjort og/ eller begrænset fundene. Vi vil afslutte kapitlet med at komme med eksempler på forebyggende arbejde og videre undersøgelse af vishing, phishing og smishing.

I denne undersøgelse har vi belyst vishing, phishing og smishing i en dansk kontekst. Som et nyt bidrag til forskningen finder vi uddybende viden om *smishing fra "bekendte"*. Vi har undersøgt fænomenet ud fra en dansk kontekst. Smishing nævnes i den eksisterende forskning og i danske talopgørelser, hvor det er en ven, der kontakter forurettede. I vores analyse finder vi dog mere dybdegående ud af gerningspersonernes fremgangsmåde og de manipulationsteknikker, som anvendes. Så vidt vi kan se, er det ikke beskrevet i den eksisterende forskning, hvorfor vi mener, at fundene fra vores undersøgelser bidrager til nye indsigter. Smishing fra "bekendte" indebærer, at en gerningsperson opererer ud fra en viden om, at deres ofre har en person i deres liv, som de stoler på – eksempelvis et familiemedlem eller en ven. Gerningspersonen udnytter denne viden om relationen ved at udgive sig for at være den "bekendte", så vedkommende kan franarre det potentielle offer deres økonomiske midler.

Generelt er der en begrænset viden om vishing, phishing og smishing i en dansk kontekst, hvorfor vi finder fundene i nærværende undersøgelse relevante. Vores undersøgelse har bidraget med en detaljeret gennemgang og analyse af gerningspersonens fremgangsmåder ud fra crime script tilgangen. Selvom der er nogle elementer, som er bekræftende/ fælles i vores undersøgelse med hensyn til den eksisterende forskning, kommer nærværende undersøgelse ind på nye elementer – her vil vi især fremhæve afsnit 6.1.1 om *Danmark som tillidssamfund*. Selvom noget af den eksisterende forskning anvender crime script og rutinaktivitetsteorien ligesom i nærværende undersøgelse, finder vi nogle forskelle i resultaterne. Vi mener, at der er tale om kulturelle forskelle i, hvordan vishing, phishing og smishing bliver begået i Danmark sammenlignet med andre lande. Kulturelle forskelle optræder i vores analyse under afsnittet om "Danmark som tillidssamfund", hvor den danske befolknings tillid til myndighederne og ikke mindst hinanden er afgørende for gerningspersoner i gennemførelsen af vishing, phishing og smishing. Derimod er dette anderledes i eksempelvis Sydkorea, hvor der ikke nævnes tillid på samme måde i forbindelse med gerningspersonens manipulation, men at de benytter sig af call-centre, hvor de massekommunikerer ud til potentielle ofre (Choi, Lee & Chun, 2017).

Som noget nyt finder vi i en dansk kontekst, at de ældre borgere målrettes som ofre, samt at deres telefonnumre bliver indsamlet gennem telefonbøger. Fundene i vores undersøgelse er muliggjort gennem semistrukturerede interviews og dokumentanalyser af cases om vishing og smishing. Vores empiriske materiale er dog begrænset i den forstand, at vi har arbejdet ud fra et forholdsvis lille sample (5 interviews og 4 cases). Vi kan ikke udelukke, om vi ville have fundet frem til anden ny viden, hvis vi havde interviewet flere respondenter. Samtidigt er det værd at bemærke, at vores data bygger på udtalelser og erfaringer fra fagprofessionelle, der dagligt arbejder med vishing, phishing og smishing på reaktiv vis. Vores data om gerningspersoners fremgangsmåde i disse databedragerityper er derfor ikke fra selve gerningspersonen. Der kan argumenteres for, at den sidstnævnte form for data er mere original end de fagprofessionelles erfaringer, men ressourcemæssigt har det ikke været muligt for os at opnå kontakt til disse gerningspersoner (Åkerström & Wästerfors, 2018: 144-145). En anden grund hertil, som også fremgår af vores analyse, er, at vi ikke har viden om, hvem disse gerningspersoner egentlig er, idet pengesporet ofte ender hos muldyr, og muldyrene er ikke nødvendigvis de egentlige gerningsmænd.

Muldyr

I vores interviewguide har vi spurgt ind til muldyr under sit eget tema, ligesom vores kodning og dele af gennemgangen af den eksisterende forskning fokuserer på muldyr. Det har blandt andet haft den utilsigtede effekt, at muldyr omtales ofte i vores interviews sammenlignet med andre tendenser, der kan sløre gerningspersonernes identitet. Som præsenteret i den eksisterende forskning finder Vedamanikam og Chethiyar i deres undersøgelse, at personer uden uddannelse og med få økonomiske midler hyppigere bliver rekrutteret som muldyr sammenlignet med personer, der står i arbejde og med fast indtjening. Yderligere er personer i aldersgruppen 24-34 år dem, der hyppigst agerer muldyr, selvom Vedamanikam og Chethiyar finder, at personer i 15-44 år ligeledes tager del i denne form for aktivitet (Vedamanikam & Chethiyar, 2020: 24). Ud fra vores data har vi erfaret, at den yngre befolkning samt samfundets mindre ressourcestærke borgere bliver udnyttet af de kriminelle til at agere muldyr. Her kan der diskuteres, om der er tale om at agere bevidst kontra ubevidst, eller om disse målgrupper for muldyr agerer ud fra overvejelser om cost/benefit. Vi vil argumentere for, at de mindre ressourcestærke er villige til at tage flere chancer for at opnå, i dette tilfælde, økonomiske ressourcer ved at agere muldyr. Ud fra vores data tolker vi, at de unge bliver en målgruppe, idet de bevæger sig i bylivet, hvor de kan være påvirkede af alkohol og derfor ikke "har barrierne oppe". Vores fund i undersøgelsen adskiller sig dermed igen fra den tidligere forskning, idet det

ud fra vores data lader til, at muldyr i Danmark er yngre end dem i Malaysia, jf. Vedamanikam og Chethiyar (2020).

Når det kommer til forebyggelse af muldyr, ser vi ud fra vores data, at uvidenhed spiller en afgørende rolle. Der skal på nationalt plan arbejdes med at informere om konsekvenserne ved at agere muldyr, idet vi ud fra vores data kan se, at mange muldyr angiveligt ikke er klar over, at det er en strafferetlig aktivitet. Det Kriminalpræventive Råd har udgivet undervisningsmateriale til forebyggelse af muldyr blandt unge, der blandt andet skal informere de unge om muldyr og det strafferetlige aspekt samt lære dem at spotte rekrutteringssituationer (DKR, 2022b). I den eksisterende forskning påpeger Leukfeldt og Kleemans to forebyggelsesstrategier, som 1) handler om at reducere provokationerne, der fører til kriminel adfærd – herunder eksempelvis gruppepres – og 2) at fjerne undskyldninger for kriminel adfærd (Leukfeldt & Kleemans, 2019: 86). Disse to forebyggelsesstrategier kan indgå i en oplysningskampagne, som kan medvirke til at reducere rekrutteringen af muldyr.

Forebyggelse gennem Situational Crime Prevention

Clarkes teori om 'situationel kriminalietsprævention' fra 1980 handler om forebyggelse af kriminalitet gennem situationelle faktorer. I teorien kommer Clarke ind på to kategorier, som kan nedbryde kriminaliteten: *reduce the physical opportunities for offending* og *increase the chance of an offender being caught* (Clarke, 1980: 139). I 2003 har han i samarbejde med Derek Cornish videreudviklet teorien og udarbejdet 25 teknikker til forebyggelse. De 25 teknikker er placeret under fem overordnede strategier, hvilket vi vil komme ind på i det følgende.

Ud fra vores empiriske materiale kan vi se, at MitID især spiller en afgørende faktor ved phishing og smishing. Det er blandt andet gennem MitID, at de forurettede godkender de anmodninger i MitID, som er tilsendt af gerningspersonen (case 2 og 3). Processen foregår via to forskellige digitale enheder. Gerningspersonen anvender forurettedes oplysninger (deres MitID-brugernavn), hvorefter gerningspersonen med denne oplysning kan sende en anmodning til MitID-app'en, som forurettede godkender fra deres egen mobiltelefon. Ud fra Cornish og Clarke (2003: 90) finder vi forebyggelsesstrategien *"Target harden"* relevant i forebyggelsen af misbrug med MitID. Vi argumenterer for, at en enhedsbegrænsning på MitID ville være et element, som kan reducere disse angreb. Det, vi mener med enhedsbegrænsning, er, at godkendelsen skal ske fra samme enhed, som anmodningen sendes fra. Der kan argumenteres for, at sådan et tiltag vil afskrække svindleren, da implementeringen af enhedsbegrænsning

øger besværligheden for at misbruge potentielle ofres MitID, hvilket gør det sværere at begå phishing og smishing. Hvis det er muligt for gerningspersonen at overtale offeret til selv at foretage en MitID-anmodning og godkende den fra deres egen mobil, kan svindleren dog alligevel forbigå denne enhedsbegrænsning og få adgang til personlige oplysninger og opnå en form for udbytte. I teorien om situationel kriminalietsprævention nævner Clarke *the "displacement" hypothesis: "the idea that reducing opportunities merely results in crime being displaced to some other time or place"* (Clarke, 1980: 138). Dette betyder, at en reducering af mulighederne (enhedsbegrænsning) vil medvirke til, at kriminaliteten udføres gennem andre metoder (eksempelvis vishing). Ifølge teorien om situational kriminalitetsprævention vil der altid være nogle forbrydere til stede, som har tilbøjeligheder og motivation til at begå kriminalitet (Clarke, 1980: 136). Derfor er det vigtigt at påpege, at selvom enhedsbegrænsningen implementeres, vil de kriminelle finde nye fremgangsmåder for at franarre potentielle ofre.

En anden af Cornish og Clarkes 25 forebyggelsesteknikker omhandler *"Alert conscience"*, der omfatter fysiske påmindelser om kriminalitet – herunder oplysning og viden (Cornish & Clarke, 2003: 90). Ud fra vores datamateriale og eksisterende forskning ser vi, at den ældre generation er mindre IT-kyndig, hvorfor oplysning og viden er nødvendig i forebyggelsesarbejdet. Dette har vi uddybet i en diskussion af rutineaktivitetsteorien, der kan ses i følgende afsnit.

Diskussion af rutineaktivitetsteorien og anvendelsen af crime script

Vi har anvendt crime script analysis for at kunne identificere gerningspersoners processuelle stadier og fremgangsmåder i udførelsen af vishing, phishing og smishing. En fordel med denne tilgang er, at vi har fået et detaljeret indblik i, hvordan gerningspersoner forbereder, udfører og afslutter den kriminelle handling. På baggrund af denne viden, rutineaktivitetsteorien og den eksisterende forskning muliggør metoden, at vi kan sætte nogle forebyggelsesforanstaltninger ud fra gerningspersonens fremgangsmåder. Dog kan der være nogle udfordringer ved anvendelsen af crime script, da der er et begrænset fokus på motivationsfaktorer. Denne tilgang fokuserer primært deskriptivt og analytisk på de handlinger og fremgangsmåder, som foretages i forbrydelsen. Derfor argumenterer vi for, at der er mindre opmærksomhed på de underliggende motivations- og sociale-faktorer, som også har en indflydelse på, at disse kriminelle handlinger opstår. Dette er dog ikke afgørende i denne undersøgelse, da vi har haft fokus på selve fremgangsmåden ved de omtalte databedragerityper. Begrænsningerne om motivations- og sociale-faktorer er ligeledes gældende for rutineaktivitetsteorien.

Med udgangspunkt i undersøgelsens problemformulering argumenterer vi for, at crime script tilgangen og rutineaktivitetsteorien er fyldestgørende for at belyse gerningspersoners handlingsmønstre ved vishing, phishing og smishing. Disse handlingsmønstre medvirker til, at der kan sættes nogle forebyggelsesanstaltninger, som kan reducere omfanget af kriminelle handlinger.

En potentiel forebyggelsesforanstaltning kunne være at oplyse den ældre generation om vishing, og hvilke konsekvenser dette kan have (Cornish og Clarkes forebyggelsesteknik nr. 23). Som nævnt i afsnit 6.1.1 er den ældre generation den hovedsagelige målgruppe ved vishing, hvorfor det er relevant at oplyse denne gruppe om disse angreb. Man ville eksempelvis kunne lave nogle oplysningskampagner hos Det Kriminalpræventive Råd, politiet eller Ældre Sagen, som skal skabe en øget bevidsthed om omfanget af vishing, uddanne den ældre generation til at begå sig på internettet og opdage de forskellige typer af vishing. Dette indebærer både afhentning af forurettedes kreditkort men ligeledes de tilfælde, hvor gerningspersoner påstår, at der er et problem med vedkommendes konto, og pengene skal overføres til en "sikker" konto. I disse oplysningskampagner ville det være relevant at komme ind på, hvordan man skal agere, når man modtager sådan et opkald – således at den ældre generation kan være bedre forberedt i forhold til at håndtere disse vishing-opkald.

Ved at skabe en større bevidsthed og en vidensdeling hos den ældre generation argumenterer vi for, at man ville besværliggøre det for gerningspersonen at manipulere med ofre og tilegne sig økonomisk vinding. Hermed skal oplysningskampagner komme med tips og tricks til, hvordan man skal agere samt belyse, hvad gerningspersoner typisk fortæller ved vishing: "der er noget galt med dit kort" eller "du skal overføre pengene til en sikkerhedskonto". Ved indførelsen af sådanne oplysningskampagner vil man ud fra rutineaktivitetsteorien betegne det som at reducere omfanget af det egnede mål. Årsagen til dette er, at man øger den ældre generations bevidsthed og uddanner dem omkring håndteringen af vishing. Hvis det lykkes at informere denne befolkningsgruppe om vishing, således at de bedre kan håndtere disse situationer, vil det betyde, at den ældre generation ikke i lige så høj grad vil være egnede mål. På denne måde vil man kunne forhindre den kriminelle handling ved at fjerne et af de tre elementer i rutineaktivitetsteorien i form af egnede mål. Dette betyder ikke, at man ville kunne forebygge fuldstændigt mod vishing, men at det vil medvirke til at reducere sandsynligheden for, at det lykkes gerningspersoner at franarre ofrene deres økonomiske midler. Sydbank og NCIK har udarbejdet materiale i forhold til at forebygge mod vishing, phishing og smishing (Bilag 7: 7; Bilag 9: 37). Materialerne er vigtige at få massekommunikeret ud, således at den ældre generation oplyses herom. Som nævnt tidligere

vurderer vi, at Ældre Sagen ville være en kapabel afsender, så man på den måde italesætter problematikken i målrettede kredse og fortæller, hvad man skal være opmærksom på.
I analysen finder vi, at gerningspersoner opretter falske hjemmesider ved både phishing og smishing. Dette er en del af gerningspersonernes pre-activity, som har en stor indflydelse på manipulationen af offeret. I disse tilfælde nævner vores respondenter, at de falske hjemmesider er professionelt opbygget, hvorfor det er relevant at få lukket dem samt oplyse befolkningen om at være opmærksomme på falske links, som leder til falske hjemmesider.

Ud fra rutineaktivitetsteorien kan der forebygges mod falske hjemmesider. Hvis vi kigger på fraværet af egnede beskyttere, er definitionen, at det er en person, som kan forhindre kriminaliteten. Rutineaktivitetsteorien (1979) blev primært udviklet til at beskrive kriminelle handlinger i det fysiske rum, hvorfor den tilsidesætter de nye teknologiske forandringer, som gør, at de egnede mål kan beskyttes af andet end personer. Dette ser vi som en begrænsning ved rutineaktivitetsteorien.

Vi argumenterer for, at fraværet af egnede mål ligeledes kan være materielle ting i form af overvågning, it-systemer og antivirus-programmer, som kan beskytte de egnede mål og forhindre kriminaliteten. Med denne tankegang argumenterer vi for, at fraværet af egnede beskyttere kan imødekommes i form af beskyttende software og tekniske hjælpemidler. Gennem denne software vil den enkelte borger blive advaret mod falske hjemmesider, hvilket kan forhindre phishing og smishing. Yderligere kan der forebygges mod modtagelsen af e-mails gennem spamfiltre, så alle de mistænkelige og uønskede mails bliver sorteret fra (Center for Cybersikkerhed, 2022: 8).
Ud fra argumentet om, at materielle ting, herunder overvågning, kan være et egnet mål, er det relevant at nævne Cornish og Clarkes 10. forebyggelsesteknik, *strengthen formal surveillance,* som er et bidrag til at imødekomme fraværet af egnede beskyttere (Cornish & Clarke, 2003: 90). Finn fra Fyns Politi nævner desuden, at de anvender videoovervågning ved hæveautomater i deres efterforskningsarbejde af vishing, men nogle gange slettes optagelserne, før efterforskningsarbejde er påbegyndt (Bilag 9: 28). Gennem en større prioritering af denne formelle overvågning (Cornish og Clarkes 10. forebyggelsesteknik) ville opklaringsarbejdet lettes.

Kapitel 8

Konklusion

8. Konklusion

Denne undersøgelse har belyst de metoder, som gerningspersoner anvender til at gennemføre vishing, phishing og smishing i en dansk kontekst samt de processer, der indgår i gennemførelsen af disse kriminalitetstyper. Vi har inddelt processerne efter de fire stadier i crime script.

Første stadie er *preparation*. Her finder vi, at gerningspersoner indsamler telefonnumre af især ældre kvinder gennem telefonbøger og Krak. Det bliver klart i dette stadie, at gerningspersonerne har en stereotyp om, at ældre personer er mere tillidsfulde over for myndighederne, hvorfor ældre kvinder typisk bliver ofre for vishing. Det første stadie af phishing og smishing er anderledes. Her forbereder gerningspersoner deres angreb ud fra samfundstendenser eller elementer, som ligger tæt på den generelle befolknings hverdag. Dette kan være en årsopgørelse eller en SMS fra PostNord, som ikke er usandsynligt, at det potentielle offer modtager. En generel tendens ved vishing, phishing og smishing er, at gerningspersonerne oftest udgiver sig for at være fra en dansk myndighed eller bank, når de kontakter deres ofre. Vi finder, at befolkningens tillid til disse er en afgørende faktor, som er særlig i Danmark.

Andet stadie er *pre-activity,* hvor gerningspersoner ved vishing udarbejder et manuskript, som de taler ud fra. Ud fra denne viden påpeger vi, at vishing er koordinerede angreb, hvor gerningspersoner fremstår professionelle og overbevisende gennem dette manuskript. Ved phishing og smishing forsøger gerningspersoner at manipulere med offeret ved at oprette falske hjemmesider og spoofe telefonnumre og e-mails, så det ligner, at forurettede får en besked/ e-mail fra en troværdig myndighed. Gerningspersonens formål ved pre-activity er at skabe nogle virkemidler, som skal understøtte gerningspersonens troværdighed og muliggøre manipulation i det tredje stadie.

Tredje stadie er *activity,* hvor gerningspersonernes forarbejde fra preparation og pre-activity omsættes til økonomisk udbytte. Der er to fremgangsmåder ved vishing: safe account fraud og afhentning af kreditkort ved forurettedes hjem. Fremgangsmåden er anderledes ved phishing og smishing. I disse tilfælde massekommunikerer gerningspersonen beskeder og e-mails, som skal fange modtagerens opmærksomhed, fordi de lover belønning (case 3) eller skaber en frygt (case 4 og falske fragtbeskeder). Fælles for disse IT-relaterede angreb er, at gerningspersoner skaber frygt hos ofrene og skaber en presset situation ved at fortælle dem, at der er noget galt med deres konto, kort eller pakkeforsendelse. På denne måde får gerningspersonerne ofrene til

at agere hurtigt, hvilket betyder, at forhastede beslutninger opstår, og gerningspersonerne har nemmere ved at opnå økonomisk vinding.

Fjerde stadie, *post-activity,* henviser til omsættelsen af de illegitime midler til noget, der fremstår som legitime midler. Dette kan gøres på forskellige måder, men den mest fremtrædende tendens i vores data er gennem anvendelsen af muldyr. På denne måde slører gerningspersoner pengenes oprindelse og deres identitet ved brugen af muldyr. Det vil sige, at pengene ikke kan spores tilbage til vedkommende, som har udført den kriminelle handling, men ender hos et muldyr, som ikke har været direkte involveret i den IT-kriminelle handling.

Ud fra crime script analysis tilgangen er vi kommet frem til, hvor i gerningspersonens processuelle stadier, vi kan intervenere. I vores analyse har vi fundet ud af, at den manglende viden er en af årsagerne til, at det lykkes gerningspersoner at franarre ofre ved vishing. I disse sager er målgruppen primært den ældre generation, hvorfor det handler om at oplyse denne gruppe om og forberede dem på, hvordan de skal agere i disse situationer. På den måde er der større sandsynlighed for, at de potentielle ofre udviser skepsis og lægger på, når gerningspersonen kontakter dem.

Den manglende viden forekommer ligeledes ved anvendelsen af muldyr. På samme måde som i ovenstående eksempel er oplysning og viden et afgørende element. Det handler om at informere om konsekvenserne ved deltagelse af muldyrsaktiviteter, og hvordan gerningspersoner narrer muldyr til at hvidvaske flere penge. Med udgangspunkt i Cornish og Clarkes forebyggelsesteknikker betegnes denne form for forebyggelse som *alert conscience*, hvor der skal være fysiske påmindelser om kriminalitet – eksempelvis kampagner og pop-ups på computeren.

Endvidere præsenterer vi med udgangspunkt i gerningspersoners *activity* ved vishing, phishing og smishing en forebyggelsesforanstaltning i form af en enhedsbegrænsning på MitID. Cornish og Clarkes forebyggelsesteknik, *target harden*, er et teoretiske eksempel på, hvordan processen kan besværliggøres. I dette tilfælde handler det om at besværliggøre mulig misbrug af potentielle ofres MitID, da godkendelsen af MitID-anmodningen skal ske fra samme enhed, som anmodningen sendes fra. Dette tiltag skal være med til at reducere tilfælde, hvor potentielle ofre bliver franarret.

Litteraturliste

Algoritmer, Data & Demokrati (2021). *Hovedkonklusioner, Digital ulighed.* Hentet fra: https://algoritmer.org/befolkningsundersoegelse/konklusioner/ (12. maj 2023).

Anti-Phishing Working Group (2022a). *Phishing Activity Trends Report, 3rd Quarter 2022.*

Anti-Phishing Working Group (2022b). *Phishing Activity Trends Report, 2nd Quarter 2022.*

Bengtsson, T.T. & Mølholt, A. (2020). Anonymisering i kvalitative undersøgelser. I: K.E. Petersen (red.), *Forskning med børn og unge: etik og etiske dilemmaer* (s. 193-209). København: Hans Reitzels Forlag.

Brinkmann, S. & Tanggaard, L. (2010). *KVALITATIVE METODER - EN GRUNDBOG.* København: Hans Reitzels Forlag, 1. udgave.

Bryman, A. (2012). *Social Research Methods.* New York: Oxford University Press, 4. udgave.

Center for Cybersikkerhed (2020). *Cybertruslen fra phishing-mails.* Hentet fra: https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/phishing/ (28. februar 2023).

Center for Cybersikkerhed (2022). *Phishing - Beskyt din organisation mod phishing-mails.* Hentet fra: https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/cfcs-phishing vejledning-2022.pdf (6. marts 2023).

Chainey, P. S, & Berbotto, A. A. (2021). A structured methodical process for populating a crime script of organized crime activity using OSINT. *Trends in Organized Crime,* (25), s. 272-300.

Chamard, S. (2011). Routine Activities. I: E. McLauglin, & T. Newburn (red.), *The SAGE Handbook of Criminological Theor*y (s. 2-20). London: SAGE Publications Ltd.

Choi, K., Lee, J. & Chun, Y. (2017). Voice phishing fraud and its modus operandi. *Security Journal,* 30(2), s. 454–466.

Choi, Y. J., & Lee, J. (2021). The change in the methods of smishing in South-Korea after the onset of covid19. *Journal of Legal, Ethical and Regulatory Issues*, 24(S5), s. 1-12

Clarke, R. V. (1980). "Situational" Crime Prevention: Theory and Practice. *British Journal of Criminology,* 20(2), s. 136-147.

Cohen. L. E, & Felson, M. (2022). Routine Activity Theory. I: F. T. Cullen, R. Agnew, & P. Wilcox (red.), *Criminological theory: Past to present* (s. 467-478). Oxford: Oxford Univsersity Press, 7. udgave.

Cohen, L. E, & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Association,* 44(4), s. 588-608.

Cornish, D. B. (1993). Crimes as scripts. I: D. Zahm & P. Cromwell (red), *Proceedings of the International Seminar* on *En.vironmental Criminology and Crime Analysis* (s. 30-46).

Cornish, D. B. (1994). *The Procedural Analysis of Offending and its Relevance for Situational Prevention.* (s. 151-196). London: London School of Economics.

Cornish, D. & Clarke, R. V. (2003). Opportunities, Precipitators and Criminal Decisions. A Reply to Wortley's Critique of Situational Crime Prevention. *Crime Prevention Studies,* (16), s. 41-96.

Danmarks Statistik (2019). *Falske emails fylder i indbakken.* Hentet fra: https://www.dst.dk/da/Statistik/nyheder-analyser-publ/nyt/NytHtml?cid=28912 (5. marts 2023).

Det Kriminalpræventive Råd (2021). *Digital Risikoadfærd.* Hentet fra: https://dkr.dk/media/9542/digital-risikoadfaerd.pdf (5. marts 2023).

Det Kriminalpræventive Råd (2022a). *It-kriminalitet i tal.* Hentet fra: https://dkr.dk/it/it-kriminalitet-i-tal (5. marts 2023).

Det Kriminalpræventive Råd (2022b). *Forebyggelse af hvidvask blandt unge.* Hentet fra: https://dkr.dk/it/undervisningsmateriale-om-unge-muldyr (1. marts 2023)

Digitaliseringsstyrelsen (2022). *FN kårer endnu engang den danske digitale offentlige sektor som verdens bedste.* Hentet fra: https://digst.dk/nyheder/nyhedsarkiv/2022/september/fn-kaarer-endnu-engang-den-danske-digitale-offentlige-sektor-som-verdens-bedste/ (10. februar 2023).

Finans Danmark (u.å.). *Netbankssvindel.* Hentet fra: https://finansdanmark.dk/tal-og-data/institutter-filialer-ansatte/kriminalitet/svindel-med-netbank-og-betalinger/netbanksvindel/ (6. marts 2023)

Forbrugerrådet Tænk (u.å.). *Mit digitale selvforsvar.* Hentet fra: https://taenk.dk/om-os/mit-digitale-selvforsvar (2. marts 2023).

Hansen, K. M., Andersen, L. B. & Hansen, S. W. (2020). Metoder i Statskundskab. København: Hans Reitzels Forlag, 3. udgave

Hvidvasksekretariatet (2023). *Den Nationale Risikovurdering af Hvidvask.* Hentet fra: https://anklagemyndigheden.dk/da/national-risikovurdering-hvidvask (20. februar 2023).

Justitsministeriet (2021). *Bekendtgørelse af straffeloven.* Hentet fra: https://www.retsinformation.dk/eli/lta/2021/1851 (6. marts 2023).

Justitsministeriets Forskningskontor (2022). *Offerundersøgelse 2005-2021, hovedtal.* Hentet fra: https://dkr.dk/materialer/vold-og-voldtaegt/offerundersoegelser-2005-2021-hovedtal (6. marts 2023).

Keatley, D. (2018). Pathways in Crime. An Introduction to Behavior Sequence Analysis. Perth: Springer International Publishing AG part of Springer Nature.

Kontraktenheden på AAU (u.å). *Juristens guide til den studerende.* Hentet fra: https://aaudk.sharepoint.com/sites/persondata-studerende/SitePages/Juristens-guide-til-den-studerende.aspx (31. maj 2023).

Kvale, S. & Brinkmann, S. (2015). *Interview. Introduktion til et håndværk.* København: Hans Reitzels Forlag, 3. udgave

Larsen, H., Sørensen, E., Lindgren, M. & Schytz, J. B. (2020). *Danskernes informationssikkerhed.* Hentet fra: https://www.cert.dk/sites/default/files/uploads/Danskernes%20informationssikkerhed%202020.pdf (20. april 2023).

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.

Leukfeldt, E. R. (2014). Cybercrime and social ties. Phishing in Amsterdam. *Trends in Organized Crime,* 17(4), s. 231–249.

Leukfeldt, E. R., & Jansen, J. (2015). Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands. *International Journal of Cyber Criminology,* 9(2), s. 173-184.

Leukfeldt, E. R. & Kleemans, E. R. (2019). Cybercrime, money mules and situational crime prevention. I: S. Hufnagel & A. Moiseienko (red.), *Criminal Networks and Law Enforcement* (s. 75-89). London: Routledge.

Loggen, J. & Leukfeldt, R. (2022). Unraveling the crime scripts of phishing networks: an analysis of 45 court cases in the Netherlands. *Trends in Organized Crime,* 25(2), s. 205-225.

Møller, K. (2018). Dokumentanalyse. I: M. H. Jacobsen (red.), *Metoder i kriminologi* (s. 201-227). København: Hans Reitzels Forlag.

Nationalt Center for IT-Kriminalitet (2022). *NCIK årsrapport 2021. En rapport om it-relateret økonomisk kriminalitet anmeldt i 2021.* Hentet fra: https://politi.dk/-/media/mediefiler/landsdaekkende-dokumenter/statistikker/oevrige-udgivelser/ncik-aarsrapport-2021.pdf (20. februar 2023).

Nguyen, T. (2022). The modus operandi of transnational computer fraud: a crime script analysis in Vietnam. *Trends in Organized Crime,* 25(2), s. 226-247.

Paraschiv, D., Toader, L., Nitu, M. & Negrea, S. (2021). Internet Fraud and Phishing Attacks - a European Perspective. I R. Pamfilie, V. Dinu, L. Tăchiciu, D. Pleșea, C. Vasiliu (red.). *7th BASIQ International Conference on New Trends in Sustainable Business and Consumption,* Foggia, Italy, 3-5 June 2021. Bucharest: ASE, s. 394-400.

Rahman, M. L., Timko, D., Wali, H. & Ajaya Neupane, A. (2022). Users Really Do Respond To Smishing. *Proceedings of ACM Conference (CODASPY'23).* ACM, New York, NY, USA

Riis, O. (2012). Kvalitet i kvalitative studier. I Jacobsen, M.H. & Jensen, S.Q. (red.), *Kvalitative udfordringer.* København: Hans Reitzels Forlag. (s. 345-374)

Robinson, O. C. (2013). Sampling in Interview-Based Qualitative Research: Theoretical and Practical Guide. *Qualitative Research in Psychology,* (11), s. 25-41.

Sikker Digital (2023). *Mit digitale selvforsvar:* Hentet fra: https://sikkerdigital.dk/borger/digital-svindel/mit-digitale-selvforsvar (1. marts 2023)

Tassy, A., Nielsen, M. B. & Jakobsen, D. T. (2020). *It-anvendelse i befolkningen 2019.* København: Danmarks Statistik

United Nations Department of Economic and Social Affairs (2022). *E-Government Survey 2022. The Future of Digital Government.* New York: United Nations.

Vedamanikam, M. & Chethiyar, S. D. M. (2020). Money Mule Recruitment among University Students in Malaysia: Awareness Perspective. *PUPIL: International Journal of Teaching, Education and Learning,* 4(1), s. 19-37.