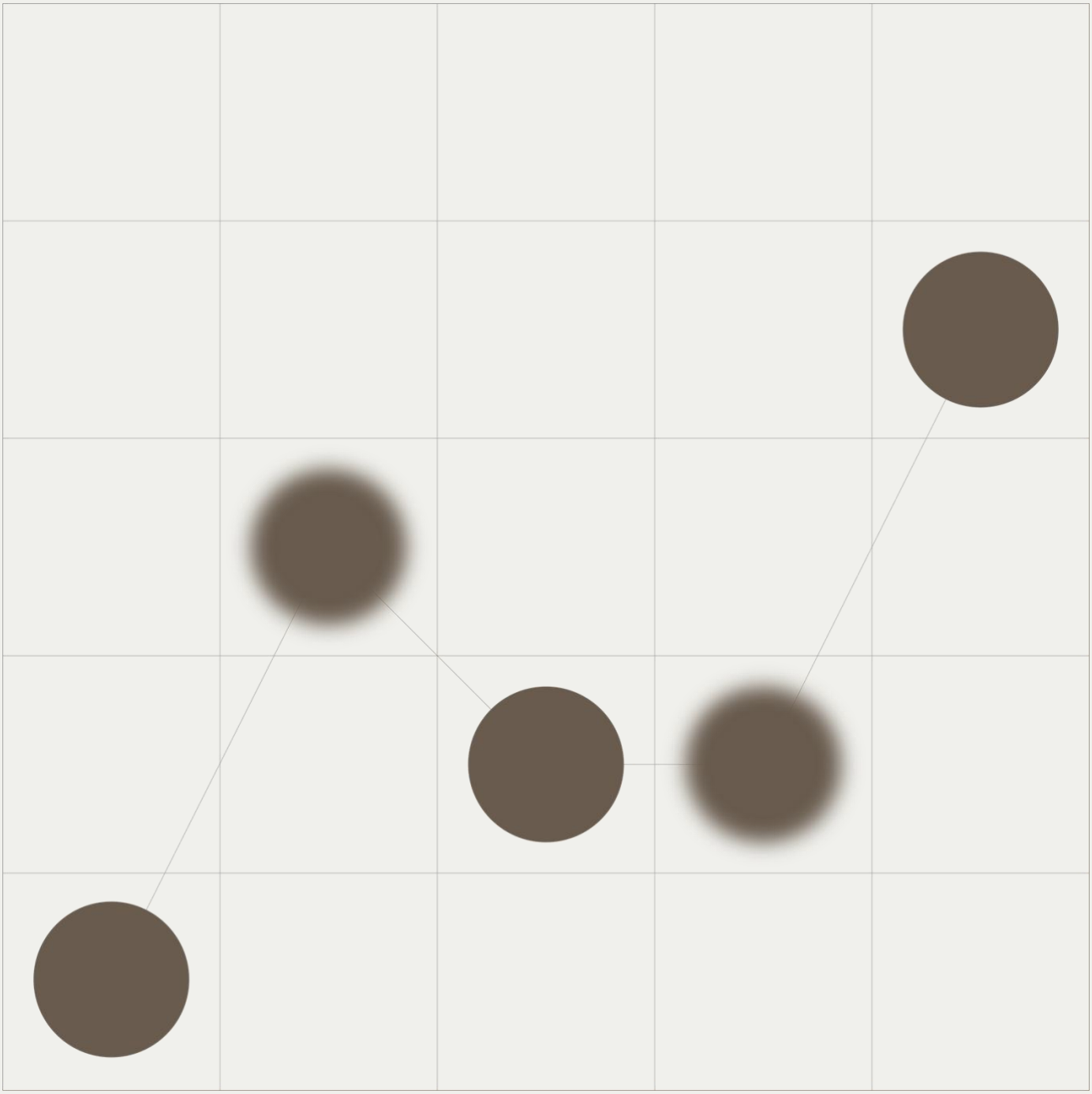


Ansvars- og rollefordelingen i forebyggelsen af IT-relateret økonomisk kriminalitet rettet mod voksne borgere

Udarbejdet af Moos-Bjerre A/S for Det Kriminalpræventive Råd
Den 29. september 2024

Det Kriminalpræventive Råd

Indholdsfortegnelse

EXECUTIVE SUMMARY

Den stigende digitalisering af det danske samfund har medført, at truslen om IT-relateret økonomisk kriminalitet rettet mod voksne borgere er blevet større. Derfor er forebyggelse af IT-relateret økonomisk kriminalitet en vigtig samfundsopgave. Nærværende vidensindsamling skal kvalificere de eksisterende forebyggelsesindsatser ved blandt andet at kortlægge ansvars- og rollefordelingen samt beskrive de involverede aktørers samarbejdsrelationer og rammebetingelser. Vidensindsamlingen bygger på omfattende desk research, en national repræsentativ befolkningsundersøgelse blandt 1.000 danskere over 18 år, fem interviews med videnspersoner på området (forskere og eksperter med særlig viden inden for IT-relateret økonomisk kriminalitet) og 22 interviews med repræsentanter for forskellige offentlige og private organisationer samt interesseorganisationer, som alle arbejder med forebyggelse af IT-relateret økonomisk kriminalitet.

Grundet flere særlige forhold ved IT-relateret økonomisk kriminalitet, er forebyggelsesarbejdet udfordrende. Først og fremmest er borgerne tilbøjelige til at tillægge sig selv et stort ansvar for at beskytte sig mod IT-relateret økonomisk kriminalitet. Konkret svarer 55 pct. af danskerne over 18 år, at de selv bærer det største ansvar for at beskytte sig mod IT-relateret økonomisk kriminalitet. Samtidig med at borgerne tillægger sig selv et stort ansvar, viser forskningen også, at borgerne har en tendens til at overvurdere deres egne evner til at gennemskue forsøg på IT-relateret økonomisk kriminalitet. På trods af at de interviewede aktører har forskellige holdninger til, hvor stort et ansvar man som borger har for at beskytte sig selv mod IT-relateret økonomisk kriminalitet, viser vidensindsamlingen dog enighed blandt aktørerne om, at der er behov for flere forebyggende indsatser. Vidensindsamlingens overordnede konklusioner lyder derfor:

1) Borgerne efterspørger viden om, *hvordan* de undgår IT-relateret økonomisk kriminalitet, samt *hvor* de kan søge hjælp og støtte, hvis de udsættes for det.

Effekten af f.eks. oplysningskampagner er dog usikker, og flere interviewede aktører peger på, at der er behov for en mere strategisk tilgang til oplysningsarbejdet

Vidensindsamlingen viser, at en stor andel af befolkningen (54,2 pct.) ikke ved, hvor de kan søge hjælp og støtte, hvis de udsættes for IT-relateret økonomisk kriminalitet. Samtidig angiver langt størstedelen af de borgere (70,4 pct.), der har være udsat for eller forsøgt udsat for IT-relateret økonomisk kriminalitet, at de ikke kontaktede nogen for at få hjælp i forbindelse med dette. Vidensindsamlingen viser i forlængelse heraf, at en stor del af borgerne oplever, at de ville føle sig bedre klædt på til at beskytte sig selv, hvis de havde øget kendskab til, hvor man kan søge råd og vejledning om IT-relateret økonomisk kriminalitet.

Dog viser vidensindsamlingen, at oplysningskampagner allerede er en af aktørernes foretrukne metoder i forebyggelsesarbejdet. En desk research foretaget i forbindelse med vidensindsamlingen viser også, at der fortsat ikke er nogen påvist effekt af oplysningskampagner. De interviewede aktører peger derfor på, at man i fremtidige oplysningsindsatser bør være mere ”strategisk” for at sikre, at indsatserne har en effekt. Her peger aktørerne særligt på, at man fremover bør være opmærksom på: 1) at målrette oplysningsindsatser mod specifikke borgermålgrupper og ikke befolkningen generelt og 2) at oplysningsindsatser i højere grad koordineres mellem aktørerne på området, så borgerne oplever at modtage de samme budskaber på tværs af oplysningsindsatser.

2) Der eksisterer allerede et velfungerende tværsektorielt samarbejde om forebyggelse, men der er et ønske om, at flere aktører involverer sig – især virksomheder bag sociale medier

På tværs af de interviewede aktører er der bred enighed om værdien af netværk og fora, som bidrager til koordinering og videndeling på området. Dette gælder f.eks. Forum mod IT-relateret økonomisk kriminalitet (FIT), Det Kriminalpræventive Råds Udvalg for Borgernes Digitale og Daglige Tryghed, sikkerdigital.dk samt netværket omkring Mit digitale selvforsvar. Størstedelen af de interviewede aktører peger ligeledes på vigtigheden af tværsektorielle samarbejder, hvor forskellige aktører kan supplere

hinandens kompetencer og perspektiver på arbejdet med forebyggelse af IT-relateret økonomisk kriminalitet. Samtidig peger størstedelen af aktørerne på, at et godt tværsektorielt samarbejde er nødvendigt for at sikre den bedst mulige forebyggelsesindsats, idet hver aktør har forskellige ansvarsområder og handlemuligheder i forhold til forebyggelsesarbejdet.

Vidensindsamlingen viser dog, at flere af aktørerne særligt savner et større engagement fra virksomhederne bag sociale medier i forebyggelsesarbejdet. Ligeledes viser befolkningsundersøgelsen, at borgerne ønsker, at sociale medier bliver bedre til at fjerne, blokere og filtrere kriminelt indhold. I forbindelse med vidensindsamlingen er en repræsentant fra et socialt medie blevet interviewet og udtaler, at de i fremtiden ønsker at spille en større rolle i forhold til forebyggelsesarbejdet – særligt i forhold til oplysningskampagner. Der findes derfor et potentiale i, at sociale medier involverer sig yderligere i forebyggelsesarbejdet af IT-relateret økonomisk kriminalitet.

3) Der er behov for at øge formaliseringen af ansvaret hos de sociale medier – både gennem styrket håndhævelse af eksisterende regulering og gennem yderligere regulering på området

På trods af, at ny regulering trådte i kraft i februar 2024 i form af EU-forordningerne DMA og DSA, som skal sikre et trygt og pålideligt onlinemiljø, mener de interviewede aktører, at der fortsat er behov for yderligere regulering, der kan sikre, at virksomheder bag sociale medier gør mere for at forebygge IT-relateret økonomisk kriminalitet på deres platforme. Aktørerne oplever samtidig, at der er behov for et større fokus på håndhævelse af eksisterende forordninger. Endelig peger aktørerne på, at der med fordel kan foretages en præciserende analyse af de konkrete behov for yderligere regulering på området.

4) Der er behov for en tydeligere ansvarsfordeling i ministerier og styrelser

Vidensindsamlingen viser, at flere aktører oplever, at der er uklarhed om, hvor ansvaret for forebyggelse af IT-relateret økonomisk kriminalitet ligger i staten. Det skyldes, at ansvaret i dag er fordelt på tværs af ministerier og styrelser. Selvom ansvaret for information og

vejledning om digital sikkerhed på det statslige niveau ligger hos sikkerdigital.dk, ligger ansvaret for Betalingsloven f.eks. hos Erhvervsministeriet, mens Justitsministeriet har det formelle samarbejde med Politiet. Både aktører i og udenfor ministerier og styrelser oplever, at der mangler koordinering på tværs af de involverede ministerier og styrelser. Ligeledes mener aktørerne, at når ansvaret går på tværs af ministerier, opstår der manglende ejerskab og i forlængelse heraf kan forebyggelsesindsatsen blive personafhængig. Aktørerne peger derfor på nødvendigheden af en mere systematisk tilgang, hvor ansvarsområderne klart defineres, og der i højere grad koordineres og samarbejdes på tværs.

5) Der er behov for at styrke forebyggelsesindsatsen gennem øget datadeling

Flere aktører påpeger, at manglende datadeling er en barriere i forebyggelsesarbejdet i dag. Datadelingen omfang begrænses især af Databeskyttelsesloven. Aktørerne forklarer, at de tilsammen sidder på vigtige informationer, som med fordel kan anvendes i de tværsektorielle forebyggelsessamarbejder. Aktørerne ser derfor et behov for at undersøge, hvordan der kan ske en øget udveksling og samkøring af data, hvor borgernes følsomme data fortsat beskyttes.

6) Der er behov for mere viden om de kriminelle

Endelig identificerer vidensindsamlingen et behov for mere viden om, hvem de kriminelle er. De interviewede aktører peger på, at man i dag har et godt kendskab til ofrene for IT-relateret økonomisk kriminalitet, men at man omvendt mangler viden om de kriminelle. Aktørerne vurderer, at et øget kendskab til, hvem de kriminelle er, kan bidrage til mere effektive forebyggelsesindsatser.

1. Rapportens formål

Denne rapport gengiver resultaterne af den vidensindsamling af ansvars- og rollefordelingen i forebyggelsen af IT-relateret økonomisk kriminalitet rettet mod voksne borgere, som analysefirmaet Moos-Bjerre har gennemført på vegne af Det Kriminalpræventive Råd forankret i Udvalget for Borgernes Digitale Tryghed[1]. Vidensindsamlingen er affødt af et ønske om at styrke forebyggelsen af IT-relateret økonomisk kriminalitet i Danmark, som udgør en voksende kriminalitetsform i det danske samfund (læs mere om dette i kapitel 2). Der er derfor et stort behov for, at samfundet bliver bedre til at forebygge og gribe ind overfor IT-relateret økonomisk kriminalitet. Vidensindsamlingens resultater er henvendt mod professionelle aktører og beslutningstagere med ansvar for at opbygge digital tryghed og robusthed både nationalt og lokalt.

Der findes allerede en række forebyggende initiativer og samarbejder, men der mangler fortsat et samlet overblik over, hvem der handler hvornår, hvordan og overfor hvilke målgrupper. Derudover kan der være forskellige opfattelser af, hvordan roller og ansvar er fordelt i forebyggelsen af IT-relateret økonomisk kriminalitet. Denne undersøgelse har til formål at belyse dette og derved styrke vidensgrundlaget for det danske samfunds forebyggelse af IT-relateret økonomisk kriminalitet rettet mod voksne borgere.

Vidensindsamlingen kortlægger og analyserer de primære forebyggelsesaktørers ansvarsområder, roller og samarbejder. Konkret afdækker vidensindsamlingen følgende:

- Hvem er de primære aktører, der arbejder med forebyggelse af IT-relateret økonomisk kriminalitet i Danmark?
- Hvad er aktørernes fokus, betingelser og samarbejdsrelationer i forebyggelsesarbejdet?

[1] Det Kriminalpræventive Råd: https://dkr.dk/om-os/organisationen/udvalget-for-borgernes-digitale-og-daglige-tryghed

- Hvilke kompetencer, styrker og muligheder findes der i arbejdet med forebyggelse af IT-relateret økonomisk kriminalitet i Danmark?

Vidensindsamlingen er gennemført ved hjælp af en metode, der kaldes Social Netværksanalyse (SNA), som bygger på:

- Omfattende desk research med fremsøgning og gennemgang af relevante rapporter og undersøgelser.
- 5 kvalitative interviews med videnspersoner med indsigt i det juridiske og forskningsmæssige på området for økonomisk IT-kriminalitet rettet mod voksne borgere.
- 22 kvalitative interviews med repræsentanter for organisationer, der på forskellig vis spiller en rolle i forebyggelsen af IT-relateret økonomisk kriminalitet rettet mod voksne borgere.
- En befolkningsundersøgelse med indsamling af 1.000 spørgeskemabesvarelser fra et nationalt repræsentativt udsnit af danskere over 18 år.

I rapportens metodebilag udfoldes vidensindsamlingens metodiske grundlag, herunder anvendelsen af SNA. Derudover fremgår det af metodebilaget hvilke aktører, der er blevet interviewet i forbindelse med vidensindsamlingen.

1.1. Læsevejledning

I rapporten anvendes følgende begreber og termer:

- *IT-relateret økonomisk kriminalitet:* IT-relateret økonomisk kriminalitet er i rapporten defineret ud fra Politiets Nationale Center for IT-kriminalitets (NCIK) definition af begrebet. Det vil sige, at IT-relateret økonomisk kriminalitet forstås som økonomisk kriminalitet uden et fysisk gerningssted. Gerningsstedet er i stedet på internettet, hvor IT-systemer og telefoner bliver brugt til at opnå økonomisk gevinst. Det kan f.eks. være misbrug af betalingskort, kreditbedrageri eller kontaktbedrageri, hvor offeret overfører penge til en gerningsperson, som eksempelvis udgiver sig for at

være banken.

- *Voksne borgere:* Rapportens genstandsfelt er forebyggelse af IT-relateret økonomisk kriminalitet rettet mod voksne borgere. Det vil sige, at rapporten udelukkende fokuserer på forebyggelse af IT-relateret økonomisk kriminalitet, som er rettet mod borgere over 18 år. I mange tilfælde er der dog klare overlap i både forebyggelsesarbejdet og de former for IT-relateret økonomisk kriminalitet, som børn og voksne rammes af. Flere af pointerne i denne rapport vil derfor også være gældende i arbejdet med at forebygge IT-relateret økonomisk kriminalitet rettet mod børn.

- *Aktør:* Begrebet ’aktør’ anvendes som en bred term om de offentlige institutioner, interesseorganisationer og private virksomheder, som arbejder med forebyggelse af IT-relateret økonomisk kriminalitet.

- *Formel/uformel:* Begreberne ’formelle’ og ’uformelle’ ansvarsområder anvendes til at skelne mellem, hvorvidt aktørerne primært har hhv. lovpligtige eller frivillige ansvarsområder i forebyggelsesarbejdet.

- *Ansvar/rolle*: Begreberne ’ansvar’ og ’rolle’ går også igen i rapporten, idet den netop undersøger ansvars- og rollefordelingen i forebyggelse af IT-relateret økonomisk kriminalitet. Mens begrebet ’ansvar’ bruges om de områder, hvor aktører har en mere formel forpligtelse, anvendes begrebet ’rolle’ mere bredt om områder med deltagelse af alle aktører, der på den ene eller anden måde arbejder med forebyggelse af IT-relateret økonomisk kriminalitet.

Rapporten er bygget op omkring følgende kapitler: Først introduceres baggrunden for rapporten i kapitel 2. Herefter gennemgås i kapitel 3 resultaterne af den befolkningsundersøgelse, der er gennemført i forbindelse med vidensindsamlingen. Det efterfølgende kapitel 4 omhandler de primære aktører på området - dels hvem der

arbejder med forebyggelse af IT-relateret økonomisk kriminalitet rettet mod voksne borgere i dag, dels aktørernes fokus, betingelser samt formelle og uformelle ansvarsområder. Kapitel 5 omhandler udfordringer i forebyggelsesarbejdet, mens kapitel 6 gennemgår de kompetencer, styrker og muligheder, der findes for forebyggelsesarbejdet i fremtiden. Til slut indeholder rapporten et metodebilag, der behandler de metoder, som analysen bygger på, herunder de metodiske overvejelser som ligger bag.

2. Baggrund: Kort redegørelse for cybertruslens omfang og myndighedernes indsats

Danmark er et af verdens mest digitaliserede samfund. Både danskernes privatliv, arbejdsliv og mødet med det offentlige foregår i stadig højere grad digitalt. Digitaliseringen giver mange fordele, men den indebærer også nye risici. En af konsekvenserne af den stigende digitalisering af danskernes liv er en øget sårbarhed overfor cyberkriminalitet. I den nationale strategi for cyber- og informationssikkerhed 2022-2024 beskrives truslen fra cyberkriminalitet som "meget høj", og det vurderes, at "det må den også forventes at være i fremtiden"[2]. Center for Cybersikkerhed uddyber, at: "Alle danske myndigheder, virksomheder og borgere er udsat for en vedvarende og aktiv trussel fra cyberkriminelle. Truslen underbygges af de cyberkriminelles evne til at udvikle

***Faktaboks:* Hvad er IT-relateret økonomisk kriminalitet?**

Dansk Politi definerer IT-relateret økonomisk kriminalitet som økonomisk kriminalitet uden et fysisk gerningssted. Gerningsstedet er i stedet på internettet, hvor IT-systemer og telefoner bliver brugt til at opnå økonomisk gevinst. Det kan f.eks. være misbrug af betalingskort, kreditbedrageri eller kontaktbedrageri, hvor offeret overfører penge til en gerningsperson, som eksempelvis udgiver sig for at være banken.

Kilde: https://politi.dk/-/media/mediefiler/landsdaekkende-dokumenter/statistikker/ncik/aarsrapport-om-it-relateret-oekonomisk-kriminalitet-anmeldt-i-2023.pdf

[2] Digitaliseringsstyrelsen: https://digst.dk/strategier/cyber-og-informationssikkerhed/

og omstille sig til nye virkeligheder samt af det specialiserede samarbejde, der foregår på det lukkede internet" (ibid.). Moos-Bjerres desk research i forbindelse med denne kortlægning tegner et tilsvarende billede, når der zoomes ind på IT-relateret økonomisk kriminalitet. Dette udfoldes i de efterfølgende afsnit.

2.1. IT-relateret økonomisk kriminalitet er i rivende udvikling

Forekomsten af IT-relateret økonomisk kriminalitet er i hastig stigning. I 2023 angav 189.000 danskere i Justitsministeriets, Politiets og Det Kriminalpræventive Råds Offerundersøgelse, at de inden for det seneste år havde været udsat for digital svindel. Til sammenligning angav 147.000 danskere i 2022, at de havde været udsat for digital svindel[3]. Det svarer til en stigning på 28,6 pct. Samtidig viser NCIK's årsrapport 2023, at Politiet i 2023 modtog det højeste antal anmeldelser om IT-relateret økonomisk kriminalitet nogensinde, svarende til 32.163 anmeldelser fra private[4]. Af disse anmeldelser udgjorde "Samhandelsbedrageri" det hyppigst anmeldte sagsområde, efterfulgt af "Phishing, smishing, vishing mfl." og "Misbrug af kortoplysninger" (ibid.). Inden for samhandelsbedrageri er der en overvægt af sager om svindel med fysiske varer såsom elektronik, tøj og tasker, hvorefter svindel med billetter til eksempelvis festivaller eller fodboldkampe udgør den næststørste andel af sagerne (ibid.). Af phishing, smishing og vishing er svindel via SMS (smishing) den mest udbredte af de tre kontaktmodi, om end

***Faktaboks:* Hvad er phishing, smishing og vishing?**

Phishing, smishing og vishing dækker over forskellige metoder, som bruges af kriminelle i forbindelse med IT-relateret kriminalitet. Phishing dækker over svindel, hvor man får tilsendt en e-mail. Det kan eksempelvis være en e-mail fra en troværdig afsender såsom en bank eller en offentlig myndighed. Smishing dækker over lignende svindel via SMS, mens vishing beskriver svindel, hvor henvendelsen fra en gerningsperson foregår via et telefonopkald.

Kilde: https://dkr.dk/it/misbrug-af-betalingskort

[3] Justitsministeriet: https://www.justitsministeriet.dk/wp-content/uploads/2024/05/Offerrapport-2005-2023.-Hovedtal.pdf
[4] NCIK: https://politi.dk/-/media/mediefiler/landsdaekkende-dokumenter/statistikker/ncik/aarsrapport-om-it-relateret-oekonomisk-kriminalitet-anmeldt-i-2023.pdf

der i næsten halvdelen af anmeldelserne ikke er rapporteret et økonomisk tab. Den typiske måde at begå smishing er at sende falske SMS-beskeder, hvor gerningspersonen lokker den forurettede til at afgive oplysninger om deres bankkonti, kortopysninger eller MitID (ibid.). Udover de tre førnævnte sagsområder er anmeldelser om kontaktbedrageri mod private steget fra 2022 til 2023 (ibid.). Kontaktbedrageri mod private kan medføre tab af store pengesummer og kan ske via diverse digitale platforme såsom sociale medier eller e-mails. Det omfatter blandt andet låne- og investeringssvindel, hvor de forudrettede reagerer på falske investeringsmuligheder i eksempelvis kryptovaluta. Kontaktbedrageri også ske i form af datingsvindel, hvor gerningspersonen udnytter forudrettedes følelser til at lokke store pengebeløb ud af dem (ibid.). Derudover foregår kontaktbedrageri også, hvor gerningspersoner udgiver sig for at være en bekendt i nød og på den måde lokker den forudrettede til at låne dem penge eller give dem adgang til deres konto (ibid.). Samtidig indikerer opgørelser også, at der eksisterer et stort mørketal, når det handler om anmeldelser om digital svindel. Tal fra Danmarks Statistik viser, at kun hver femte borger, der har været udsat for IT-relateret økonomisk kriminalitet, kontakter Politiet efterfølgende[5]. Omfanget af IT-relateret økonomisk kriminalitet er derfor formodentligt langt højere, end de rapporterede anmeldelsestal.

Udover at forekomme i stigende omfang finder IT-relateret økonomisk kriminalitet også hele tiden nye former. Flere af de videnspersoner[6] på området, som Moos-Bjerre har interviewet i forbindelse med vidensindsamlingen, beskriver, hvordan kriminelle hele tiden tager nye teknologier i brug i den digitale svindel for at omgå Politiets metoder til opklaring af IT-relateret økonomisk kriminalitet. Brugen af kunstig intelligens i den IT-relaterede økonomiske kriminalitet nævnes som det seneste eksempel på dette. En konsekvens af dette ”teknologiske våbenkapløb” er, at den IT-relaterede økonomiske kriminalitet hele tiden sker på vidt forskellige måder og i varierende formater, hvilket betyder, at alle borgere kan rammes. Disse videnspersoner er således enige om, at det ikke giver mening

[5] Danmarks Statistik 2023 – It-anvendelse i befolkningen 2023. https://www.dst.dk/Site/Dst/Udgivelser/GetPubFile.aspx?id=49775&sid=itbef2023

[6] Moos-Bjerre har i forlængelse af desk researchen gennemført 5 interviews med videnspersoner med indsigt i det juridiske og forskningsmæssige inden for økonomisk IT-kriminalitet rettet mod borgerne. I rapportens metodebilag gengives det konkret, hvilke videnspersoner, der er blevet interviewet i forbindelse med vidensindsamlingen.

at tale om bestemte risikogrupper eller typiske ofre i relation til IT-relateret økonomisk kriminalitet. Alle aldersgrupper og sociodemografiske grupper udsættes for IT-relateret økonomisk kriminalitet, blot i forskellige former. Det samme viser NCIK's seneste årsrapport over anmeldelsestal[7]. Her fremgår det, at alle borgergrupper på tværs af alder og køn rammes af IT-relateret økonomisk kriminalitet. Forskellen ligger dog i de former for kriminalitet, som bestemte borgergrupper udsættes for. F.eks. er yngre borgere i højere grad udsat for samhandelsbedrageri ved køb og salg af billetter til festivaler og koncerter eller ved køb af værdier i online spilverdener eller -platforme, f.eks. virtuel valuta eller "skins" (virtuelle genstande som optjenes eller købes i computerspil). Omvendt udsættes ældre borgere i højere grad for kontaktbedrageri (ibid.).

2.2. Myndighedernes indsats mod IT-relateret økonomisk kriminalitet

Risikoen for at blive udsat for IT-relateret økonomisk kriminalitet er stor og må forventes at vokse, efterhånden som digitaliseringen udvikler sig og integreres yderligere i danskernes hverdag. Derfor findes der også allerede i dag en række myndighedsinitiativer, der skal forebygge og forhindre IT-relateret økonomisk kriminalitet rettet mod voksne borgere.

I det følgende udfoldes først kort den eksisterende lovgivning, der regulerer området. Derefter præsenteres den nationale strategi for cyber- og informationssikkerhed, der beskriver, hvordan regeringen ønsker at styrke cybersikkerheden i Danmark.

2.2.1. Eksisterende lovgivning på området

Cybersikkerhed og IT-relateret økonomisk kriminalitet reguleres af flere love og retsakter, der løbende opdateres og udvikles. Herunder er oplistet nogle af de centrale:

[7] NCIK årsrapport 2023 – En rapport om IT-relateret økonomisk kriminalitet anmeldt i 2023. https://politi.dk/-/media/mediefiler/landsdaekkende-dokumenter/statistikker/ncik/aarsrapport-om-IT-relateret-oekonomisk-kriminalitet-anmeldt-i-2023.pdf

1. **Straffeloven**: Straffeloven er central i bekæmpelsen af IT-relateret økonomisk kriminalitet begået mod den enkelte borger, da den specificerer den juridiske ramme for økonomisk kriminalitet, samt hvordan de forskellige forbrydelser skal straffes. Flere bestemmelser i straffeloven omhandler forbrydelser som hacking (§ 263), uberettiget brug af IT-systemer (§ 263a), bedrageri (§ 279) og databedrageri (§ 279 a)[8]. Bestemmelserne om hacking og uberettiget brug af IT-systemer blev tilføjet i hhv. 1985 og 1987 i takt med den stigende brug og implementering af IT-systemer. Bestemmelsen om databedrageri blev tilføjet til bestemmelsen om bedrageri i 2001 for at fokusere specifikt på håndtering af bedrageri og svindel, der involverer IT-systemer og data. Det er Politiet, der har ansvaret for at håndhæve straffeloven i Danmark.

2. **Databeskyttelsesloven**: Databeskyttelsesloven er en implementering af EU's General Data Protection Regulation (GDPR) i dansk lovgivning, som trådte i kraft i maj 2018, to år efter at GDPR blev vedtaget i Europa-Parlamentet. Databeskyttelsesloven regulerer beskyttelsen af persondata og pålægger organisationer at sikre personoplysninger mod uautoriseret adgang og misbrug, således at den enkelte borger i højere grad er beskyttet mod trusler som hacking og datatyveri[9]. Det er Datatilsynet, der har ansvaret for at føre tilsyn med, at Databeskyttelsesloven bliver håndhævet.

3. **Lov om betalinger**: Denne lov fra 2017 regulerer betalingstjenester og elektroniske penge og indeholder bestemmelser om sikkerhed og ansvar ved uautoriserede transaktioner[10]. Hermed beskytter loven borgerne, blandt andet ved at begrænse den enkeltes ansvar, hvis denne bliver offer for IT-relateret økonomisk kriminalitet og ved at sikre retten til tilbageførsel ved svindel. Det er Finanstilsynet, der har ansvaret for at føre tilsyn med, at lov om betalinger bliver håndhævet.

[8] Retsinformation, straffeloven: https://www.retsinformation.dk/eli/lta/2021/1851#P279
[9] Retsinformation, databeskyttelsesloven: https://www.retsinformation.dk/eli/lta/2018/502
[10] Retsinformation, lov om betalinger: https://www.retsinformation.dk/eli/lta/2017/652

4. **Hvidvaskloven**: Denne lov stiller krav til finansielle institutioner og andre relevante aktører om at implementere foranstaltninger mod hvidvaskning af penge og finansiering af terror, herunder specifikt i relation til IT-relateret økonomisk kriminalitet[11]. Hvidvaskloven bidrager således til at beskytte borgerne mod økonomisk tab og forhindre, at kriminelle kan udnytte dem som led i større operationer. Loven er fra 1993, men blev gennemgribende revideret i 2017 med en implementering af det fjerde EU-hvidvaskdirektiv. Loven opdateres løbende for at imødegå nye trusler og metoder inden for hvidvaskning og finansiering af terror. Finanstilsynet har ansvaret for at føre tilsyn med, at hvidvaskloven bliver håndhævet.

5. **Net- og informationssikkerhedsloven (NIS-loven)**: Denne lov fokuserer primært på sikkerheden indenfor digital infrastruktur samt digitale tjenester, der er kritiske for samfundets funktionalitet og økonomi. Dette indbefatter blandt andet netværksudbydere og datacentre, samt virksomheder der leverer digitale tjenester til væsentlige sektorer såsom sundhedsvæsenet. Loven trådte i kraft i 2018 med fokus på at højne cybersikkerheden og sikkerheden for essentielle netværks- og informationssystemer[12]. Den stiller krav om sikkerhedsforanstaltninger samt krav om underretning om IT-sikkerhedshændelser til myndighederne[13]. Dermed bidrager loven til at mindske risikoen for, at borgernes personlige og finansielle data bliver brugt i kriminelle aktiviteter. Digitaliseringsstyrelsen har ansvaret for at føre tilsyn med, at hvidvaskloven bliver håndhævet.

6. **Finanstilsynets IT-sikkerhedsstyring**: Finanstilsynet har udstedt en række retningslinjer og bekendtgørelser, der fokuserer på finansielle institutioners IT-sikkerhed og krav til forebyggelse af økonomisk kriminalitet. De er blevet udviklet løbende, og de seneste blev udstedt i 2020. Disse retningslinjer indbefatter blandt andet, at de finansielle virksomheder skal implementere strenge

[11] Retsinformation, hvidvaskloven: https://www.retsinformation.dk/eli/lta/2022/316
[12] NIS-loven: https://www.retsinformation.dk/eli/lta/2018/436
[13] Digitaliseringsstyrelsen, Tilsyn med NIS-loven: https://digst.dk/sikkerhed/digitale-tilsyn/tilsyn-med-nis-loven/

adgangskontrolsystemer og omfattende IT-sikkerhedsprocedurer. Finanstilsynet udfører også løbende IT-inspektioner, der har til formål at sikre, at kravene bliver overholdt. Retningslinjerne samt de løbende IT-inspektioner er essentielle for at sikre, at finansielle institutioner er rustede til at modstå cybertrusler og andre former for IT-relateret økonomisk kriminalitet samt for at beskytte deres kunders økonomiske interesser[14].

7. **E-handelsloven**: E-handelsloven blev indført i 2002 med det formål at beskytte borgere mod risici ved handel på nettet. Loven indeholder en lang række regler og krav for, hvordan virksomheder eller hjemmesider med kommercielt sigte skal agere i forhold til elektronisk handel. Blandt andet skal de opgive visse officielle oplysninger, og særlige værktøjer skal stilles til rådighed for at sikre gennemsigtighed og mindske risikoen for økonomisk svindel[15]. Forbrugerombudsmanden har ansvaret for at føre tilsyn med, at E-handelsloven bliver håndhævet.

8. **DSA og DMA**: DSA (forordningen om digitale tjenester) og DMA (forordningen om digitale markeder) trådte formelt i kraft i november 2022, om end reglerne (med få undtagelser) først har fået virkning fra februar 2024. Forordningerne er dermed et af de nyeste tiltag i bekæmpelsen af IT-relateret økonomisk kriminalitet. DSA har til formål at sikre et trygt og pålideligt onlinemiljø med særligt fokus på at bekæmpe ulovlige varer, ulovlige tjenester og ulovligt indhold på digitale tjenester. Dette omfatter blandt andet fjernelse af salg af ulovlige og forfalskede produkter på sociale medier samt ulovlig og vildledende reklame[16]. DMA har til formål at sikre mere retfærdig og transparent konkurrence i den digitale verden. Dette indebærer en række krav og regler for de største tech-virksomheder, eksempelvis Apple og Meta, som bidrager til at øge borgernes valgfrihed og sikkerhed samt øge

[14] Finanstilsynet: https://www.finanstilsynet.dk/finansielle-temaer/it-tilsyn-og-datasikkerhed/it-sikkerhedsstyring-i-finansielle-virksomheder
[15] Forbrugerombudsmanden: https://forbrugerombudsmanden.dk/alle-emner/anden-lovgivning/e-handelsloven/
[16] Konkurrence- og forbrugerstyrelsen: https://kfst.dk/forbrugerforhold/digitale-formidlingstjenester-dsa/

konkurrencen[17]. Det er Konkurrence- og Forbrugerstyrelsen, der er udpeget til at føre tilsyn med DSA og DMA i Danmark.

2.2.2. Den nationale strategi for cyber- og informationssikkerhed

Myndighedernes indsats for at forebygge IT-relateret økonomisk kriminalitet målrettet voksne borgere hviler ikke kun på lovgivning. Et bærende element er også den nationale strategi for cyber- og informationssikkerhed, der er udformet af regeringen[18]. Den aktuelle strategi blev lanceret i december 2021 og beskriver regeringens vision for, hvordan den digitale sikkerhed i Danmark skal styrkes. Strategien har fokus på både myndigheder, virksomheder og borgere, og den beskriver fire strategiske målsætninger for at øge den digitale sikkerhed i Danmark:

- Robust beskyttelse af vigtige samfundsfunktioner
- Øget kompetenceniveau og ledelsesforankring
- Styrkelse af det offentlig-private samarbejde
- Aktiv deltagelse i den internationale kamp mod cybertrusler

I forhold til at forebygge IT-relateret økonomisk kriminalitet rettet mod voksne borgere indeholder strategien flere relevante elementer. Den peger blandt andet på behovet for at øge kompetence- og vidensniveauet blandt borgerne og behovet for at styrke samarbejdet og videndelingen mellem virksomheder og myndigheder. De foreslåede strategiske indsatser indebærer blandt andet udbredelse af inspirationsmateriale, forøget awareness i alle uddannelsesled samt styrkelse af virksomheders, statslige myndigheders og borgeres kompetencer indenfor cyber- og informationssikkerhed gennem kurser og informationsindsatser på digitale platforme (ibid.).

[17] Konkurrence- og forbrugerstyrelsen: https://kfst.dk/konkurrenceforhold/digitale-markeder-dma/
[18] Digitaliseringsstyrelsen: https://digst.dk/strategier/cyber-og-informationssikkerhed/

3. Befolkningens viden om og erfaringer med IT-relateret økonomisk kriminalitet

Et fokuspunkt i den nationale strategi for cyber- og informationssikkerhed er som nævnt at højne befolkningens viden om, hvordan de færdes og beskytter sig digitalt. Netop oplysning af borgerne om, hvordan de undgår og håndterer IT-relateret økonomisk kriminalitet, er et fokuspunkt i flere af de samarbejder om forebyggelse af IT-relateret økonomisk kriminalitet, som denne kortlægning har afdækket. For at kvalificere denne del af forebyggelsesarbejdet og indsamle viden om borgernes syn på de forskellige aktører, der er engageret i forebyggelsen af IT-relateret økonomisk kriminalitet rettet mod voksne borgere, har Moos-Bjerre i forbindelse med kortlægningen gennemført en national repræsentativ befolkningsundersøgelse. Undersøgelsen er gennemført som en befolkningssurvey med 1.000 besvarelser fra et nationalt repræsentativt udsnit af danskere over 18 år. Befolkningsundersøgelsen har bl.a. spurgt til borgernes erfaringer med IT-relateret økonomisk kriminalitet, herunder viden om hvor man kan søge hjælp og støtte i tilfælde af, at man udsættes for IT-relateret økonomisk kriminalitet. Derudover afdækker befolkningsundersøgelsen ligeledes befolkningens oplevelse af aktørerne på området, samt hvilket ansvar man som borger har for at beskytte sig selv mod IT-relateret økonomisk kriminalitet. Befolkningsundersøgelsens resultater udfoldes i de følgende afsnit.

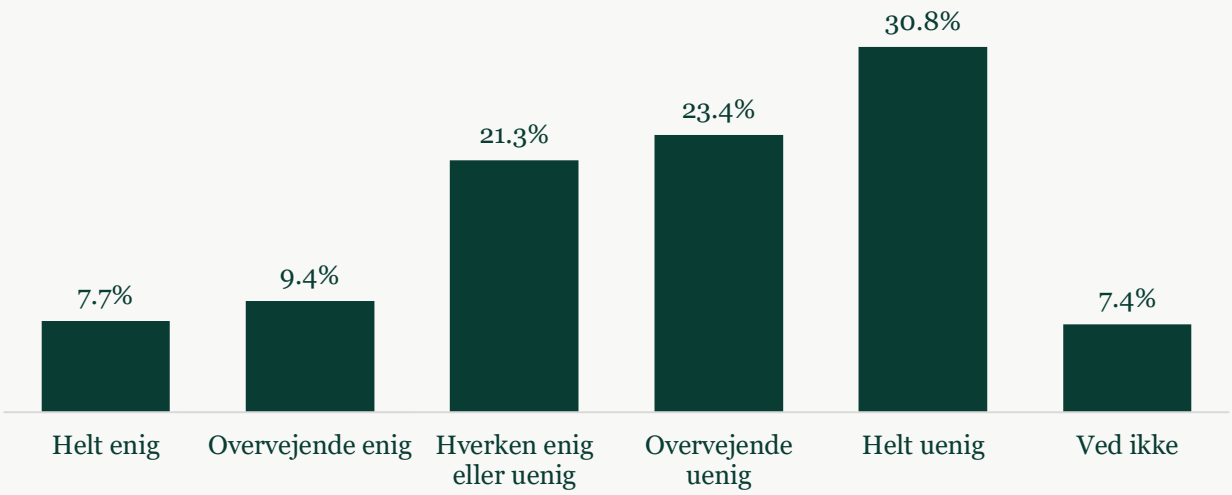
3.1. Kendskab til muligheder for hjælp og støtte

Det repræsentative udsnit af befolkningen er allerførst blevet adspurgt, hvilke myndigheder, organisationer, foreninger og lignende, som de kender til, hvor man kan modtage hjælp og støtte fra, i tilfælde af at man udsættes for økonomisk svindel på nettet. Til dette spørgsmål angiver langt størstedelen af respondenterne 'Politiet'. Herefter angiver næstflest deres bank. Efter Politiet og banksektoren angiver størstedelen, at de ikke har kendskab til nogen aktører, som man kan modtage hjælp og støtte fra i tilfælde af, at man udsættes for økonomisk svindel på nettet. Endelig angiver en mindre andel deres

forsikringsselskab. Andre aktører nævnes kun et fåtal af gange. Det gælder eksempelvis interesseorganisationer, hvor særligt Ældre Sagen nævnes. Ligeledes nævnes aktører som Forbrugerrådet Tænk og Det Kriminalpræventive Råd af enkelte.

Der er således en tendens til, at det særligt er Politiet og banksektoren, som borgere kender til, at man kan søge hjælp og støtte hos, om end en stor andel af borgerne ikke oplever at have kendskab til nogen aktører på området.

Figur 1: Hvor enig eller uenig er du i følgende udsagn:
"Det er tydeligt for mig, hvor jeg kan søge hjælp og støtte, hvis jeg som privatperson udsættes for økonomisk svindel på nettet?"



Note: n = 1025

Ovenstående figur viser, at over halvdelen (54,2 pct.) af respondenterne er uenige i, at det er tydeligt, hvor de kan søge hjælp og støtte i tilfælde af, at de udsættes for økonomisk svindel på nettet. Kun 17,1 pct. angiver, at de ved, hvor de skal søge hjælp, mens 21 pct. hverken er enige eller uenige i udsagnet. Dette indikerer et behov for bedre information og vejledning til borgerne, da en betydelig andel ikke føler sig sikre på, hvor de kan få hjælp. Samtidig er det dog væsentligt at påpege, at det manglende kendskab hos mange borgere kan skyldes, at de ikke tidligere er blevet udsat for økonomisk svindel på nettet, hvorfor de ikke har undersøgt mulighederne for hjælp og støtte.

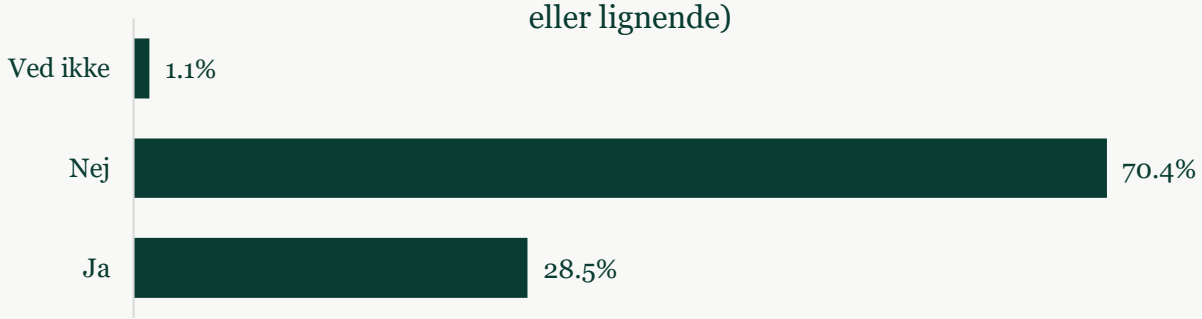
3.2. Hvor borgere har søgt hjælp og støtte i forbindelse med IT-relateret økonomisk kriminalitet

Figur 2: Har du som privatperson inden for de seneste 12 måneder været udsat for økonomisk svindel på nettet eller et forsøg herpå?

Note: n = 1025

6,2 pct. af respondenterne har de seneste 12 måneder været udsat for økonomisk kriminalitet på nettet, imens 28 pct. har været forsøgt udsat for økonomisk svindel på nettet. En betydelig del af befolkningen er dermed enten direkte berørt af eller i risiko for at blive offer for økonomisk kriminalitet på nettet. Dog ses det samtidig også, at størstedelen (60,9 pct.) hverken har været udsat for eller forsøgt udsat for økonomisk svindel på nettet.

Figur 3: Kontaktede du nogen, da du blev udsat for økonomisk svindel på nettet eller forsøg herpå? (Fx Politiet, banken, forsikringsselskab eller lignende)



Note: n = 351. Det er kun borgere, der har svaret, at de har været forsøgt udsat eller har været udsat for økonomisk kriminalitet, der er blevet adspurgt om dette.

Hele 70,4 pct. af de borgere, der har været udsat for eller forsøgt udsat for økonomisk svindel på nettet svarer, at de ikke kontaktede nogen i forbindelse med dette. Omvendt angiver 28,5 pct., at de kontaktede nogen i forbindelse med svindlen eller forsøget herpå.

Figur 4: Hvem kontaktede du? (Det er muligt at vælge flere svarmuligheder)

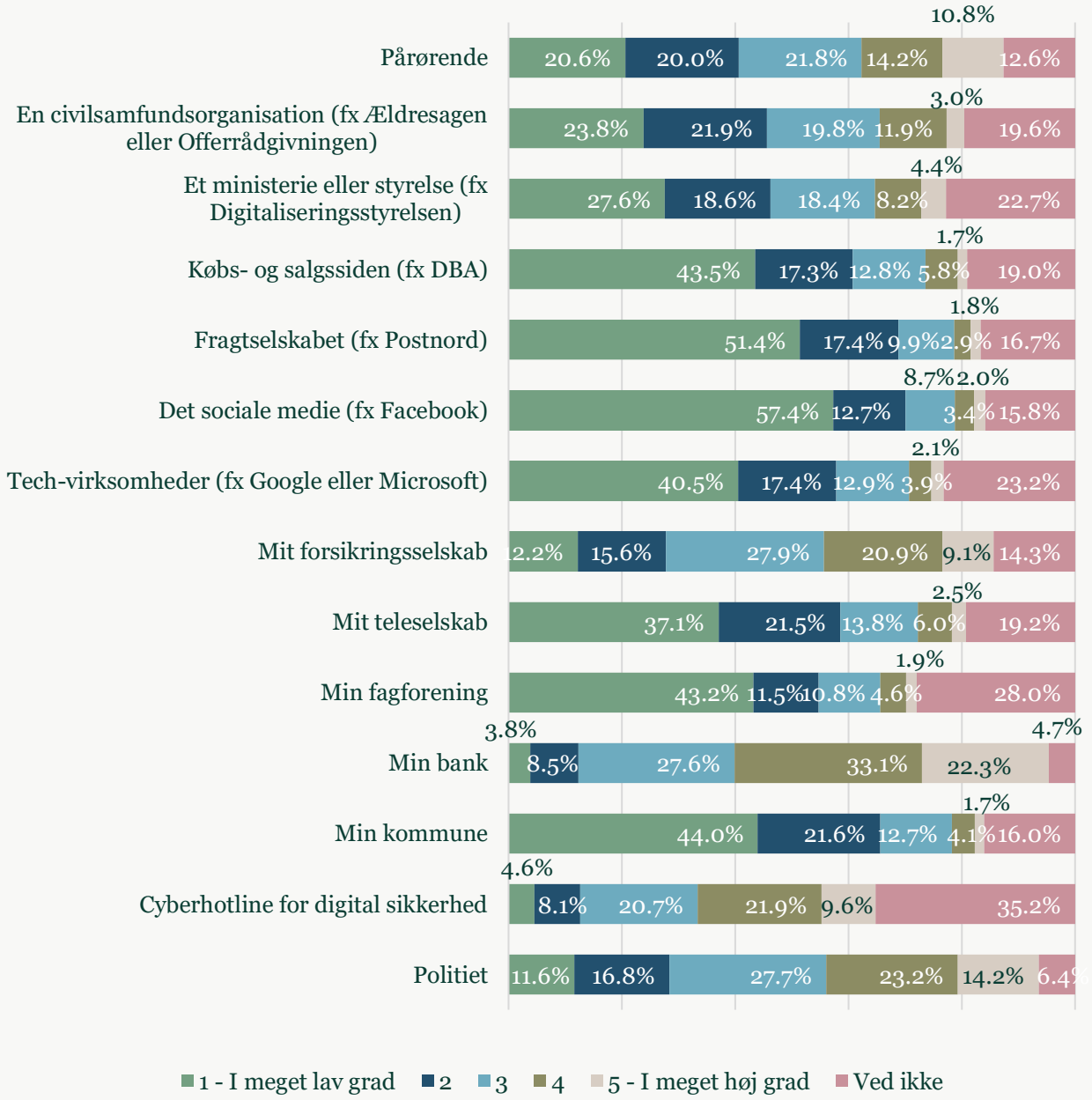
Note: n = 100. Det er kun personer, der har svaret, at de kontaktede nogen i forbindelse med, at de enten blev udsat for eller forsøgt udsat for økonomisk svindel på nettet, der har besvaret dette spørgsmål.

Ovenstående figur viser, at når borgere oplever økonomisk svindel eller forsøg herpå, er banken den primære kontaktinstans. Når borgere har været udsat for økonomisk svindel

eller forsøg herpå, har størstedelen, 75 pct, kontaktet deres bank, hvilket understreger bankernes centrale rolle i håndteringen af disse situationer. 34 pct. har angivet, at de kontakede Politiet, mens kun 7 pct. har henvendt sig til den pågældende købs- og salgsside (f.eks. Den Blå Avis (DBA)), hvor svindlen havde fundet sted. Omvendt er det kun meget få borgere, der har kontaktet det sociale medie f.eks. Facebook (5 pct.), Cyberhotline for digital sikkerhed (3 pct), fragtselskabet f.eks. Postnord (3 pct.), deres teleselskab (2 pct.), tech-virksomheden f.eks. Google eller Microsoft (2 pct.), deres kommune (1 pct.), deres fagforening (1 pct.), et ministerie eller styrelse (0 pct.) eller en civilsamfundsorganisation (0 pct.). Det kan tyde på, at disse kanaler enten ikke er lige så velkendte, eller at borgerne ikke opfatter dem som lige så effektive i forhold til håndteringen af økonomisk svindel. De respondenter, der har angivet ”Andre”, uddyber med følgende: ”Forbrugerombudsmanden”, ”Den side hvorpå det økonomiske svindel foregik”, ”Forbrugerrådet Tænk”, ”MobilePay” og ”MitID”.

3.3. Borgernes oplevelse af aktørerne på området

Figur 5: Du kan blive svindlet på mange forskellige måder og platforme. Uanset svindelformen i hvilken grad ville du så forvente, at følgende aktører ville være i stand til at hjælpe dig, hvis du henvendte dig til dem, fordi du var blevet udsat for økonomisk svindel på nettet?

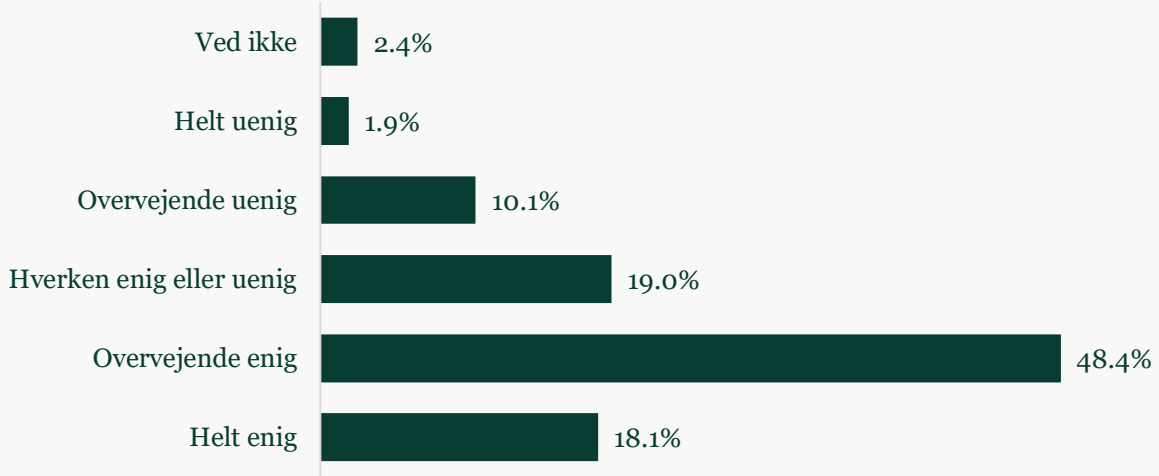


Note: n = 1025

Når borgerne adspørges om deres tiltro til, at ovenstående aktører ville være i stand til at hjælpe, hvis de blev udsat for økonomisk svindel på nettet, vurderes særligt tech-virksomheder og sociale medier til kun i lav grad at forventes at være en hjælp. Politiet, bankerne, Cyberhotline for digital sikkerhed og forsikringsselskaberne er de aktører, som respondenterne i højeste grad forventer kan være en hjælp i tilfælde af økonomisk svindel på nettet. Dette er i tråd med Figur 4, som illustrerede, at langt de fleste borgere kontakter deres bank eller Politiet, hvis de udsættes for økonomisk svindel på nettet.

3.4. Borgernes oplevelse af ansvar og roller i forbindelse med forebyggelsesarbejdet

Figur 6: Hvor enig eller uenig er du i følgende udsagn:
"Man har som borger i et digitalt samfund selv ansvar for at finde ud af, hvordan man bedst beskytter sig selv mod økonomisk svindel på nettet."



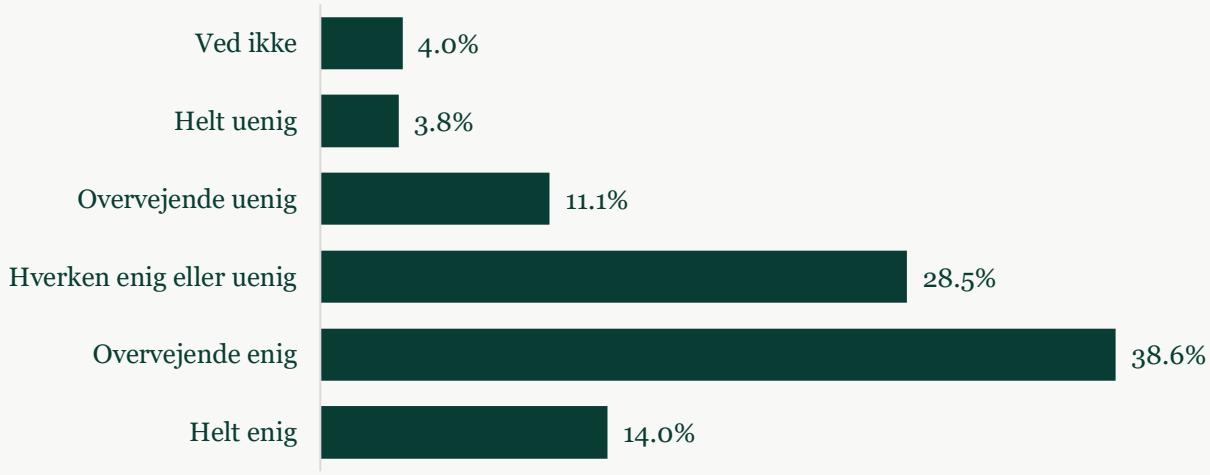
Note: n = 1025

Blandt respondenterne svarer 18,1 pct., at de er helt enige i, at man som borger i et digitalt samfund selv har ansvar for at finde ud af, hvordan man bedst beskytter sig selv mod økonomisk svindel på nettet. Omtrent halvdelen (48,4 pct.) af respondenterne er overvejende enige i ovenstående udsagn. Når så stor en andel af respondenterne er enten helt enige eller overvejende enige i, at man som borger selv bærer et ansvar, kan

dette hænge sammen med en generel overvurdering af egne evner i forhold til at beskytte sig selv. Forskning viser, at borgere har en tendens til at overvurdere egne evner til at gennemskue svindel på nettet, hvilket potentielt kan lede til en overvurdering af eget ansvar i forhold til at beskytte sig selv[19].

19 pct. er hverken enige eller uenige, mens kun 12 pct. er helt eller overvejende uenige i førnævnte udsagn.

Figur 7: Hvor enig eller uenig er du i følgende udsagn: "Jeg har en forventning om, at de offentlige myndigheder klæder borgerne på til at beskytte sig selv mod økonomisk svindel på nettet."

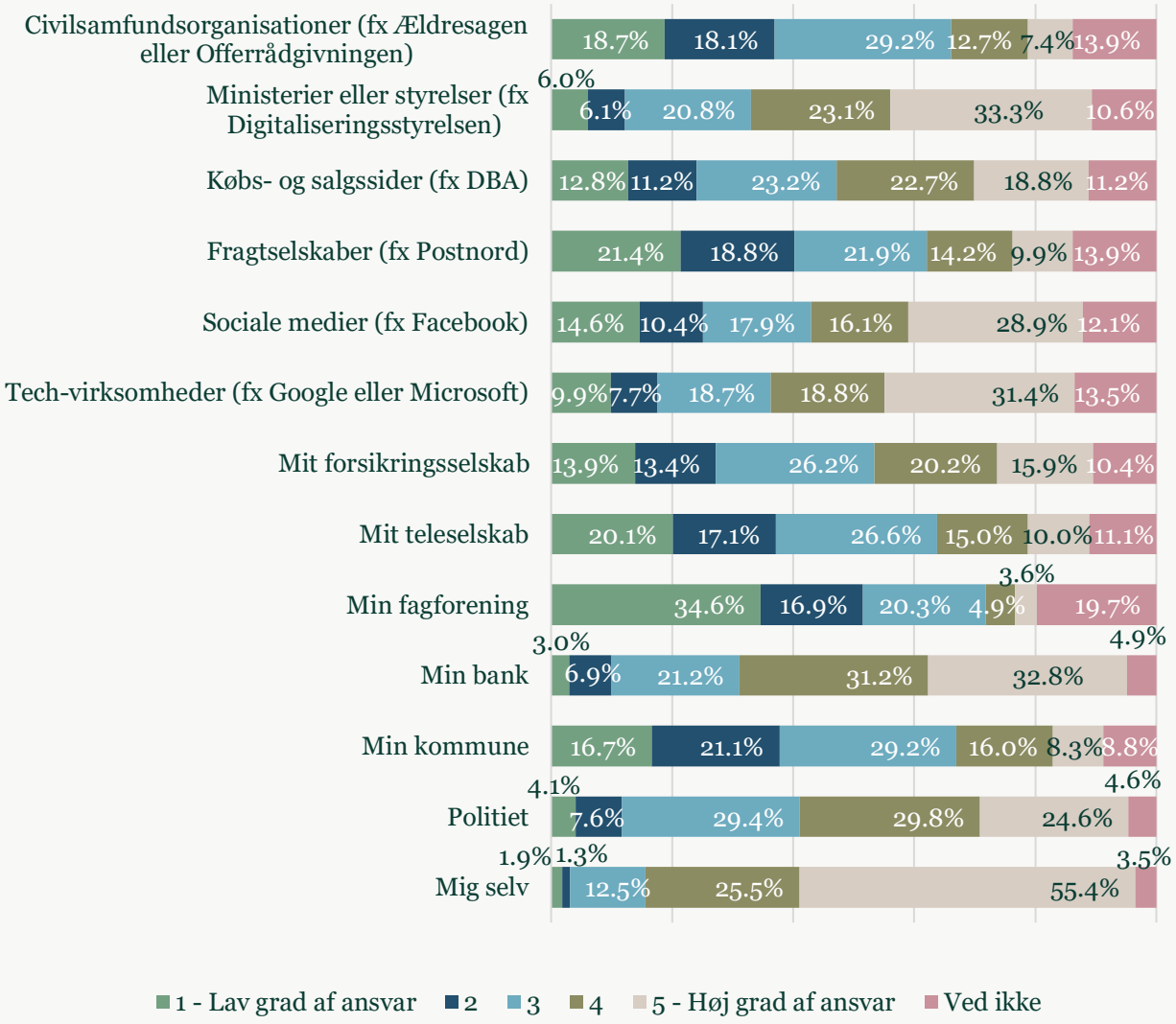


Note: n = 1025

På trods af at en stor del af borgerne oplever, at der påhviler den enkelte borger et ansvar for at beskytte sig selv, viser ovenstående figur, at en stor andel af borgerne også har en forventning om, at de offentlige myndigheder klæder borgerne på til at beskytte sig selv mod økonomisk svindel på nettet. 38,6 pct. er overvejende enige og 14 pct. er helt enige i dette. 28,5 pct. er hverken enige eller uenige, mens kun 11,1 pct. er overvejende uenige og 3,8 pct. er helt uenige.

[19] Det Kriminalpræventive Råd: https://dkr.dk/media/9542/digital-risikoadfaerd.pdf

Figur 8: Vurdér følgende aktører på en skala fra 1-5 i forhold til i hvor høj grad du mener, at de bærer et ansvar for at beskytte borgere mod økonomisk svindel på nettet.



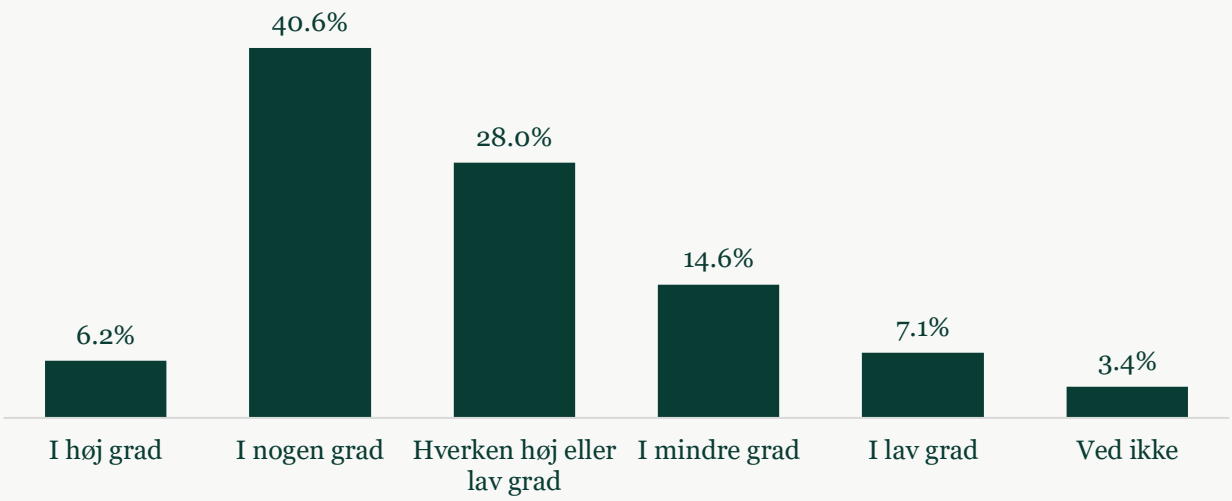
Note: n = 1025

Når respondenterne bedes vurdere, i hvor høj grad de forskellige aktører bærer et ansvar for at beskytte borgere mod økonomisk svindel på nettet, angiver de i højeste grad 'Mig selv'. Det faktum, at størstedelen peger på 'Mig selv' som den aktør, der bærer det største ansvar for at beskytte dem selv mod økonomisk svindel på nettet, indikerer et behov for flere indsatser på et opbyggende niveau, der har til formål at ruste borgerne til at beskytte

sig selv. Bankerne, tech-virksomhederne, sociale medier samt ministerier, styrelser og Politiet vurderes ligeledes til at bære en høj grad af ansvar. Aktører som kommunerne, civilssamfundsorganisationer eller fagforeninger vurderes i lavere grad til at bære et ansvar i forhold til at beskytte borgerne mod økonomisk svindel på nettet.

Befolkningsundersøgelsen viser dermed, at borgerne primært ser sig selv som ansvarlige for at beskytte sig mod økonomisk svindel på nettet, men at banker, tech-virksomheder og myndigheder også bærer en del af ansvaret. Det samme billede tegner sig i den kvalitative analyse, hvor aktørerne er enige om, at ansvaret er både individuelt og kollektivt (se afsnit 4.5.1.).

Figur 9: I hvilken grad føler du dig i dag beskyttet mod at blive udsat for økonomisk svindel på nettet?



Note: n = 1025

Kun 46,8 pct. af respondenterne føler sig i høj eller nogen grad beskyttet mod at blive udsat for økonomisk svindel. 28 pct. angiver, at de hverken i høj eller lav grad føler sig beskyttet, mens 21,7 pct. i mindre eller lav grad føler sig beskyttet.

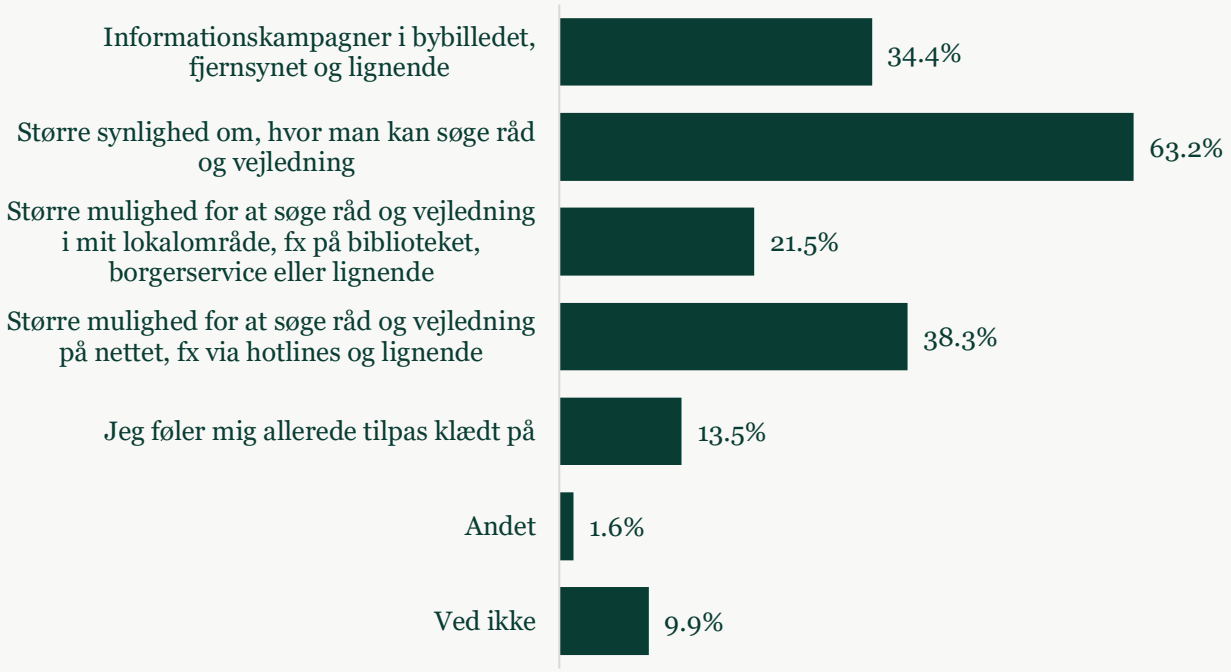
Supplerende analyser (se bilag) viser, at størstedelen af de respondenter, der har angivet at føle sig beskyttet mod økonomisk svindel på nettet, begrunder dette med en oplevelse af selv at have den nødvendige viden om og forståelse for, hvordan man beskytter sig selv på nettet. Dette er i overensstemmelse med den eksisterende forskning, som viser, at

borgere har en tendens til at overvurdere egne evner til at beskytte sig selv[20]. Den næststørste andel af respondenterne begrunder deres angivne svar med en følelse af at være beskyttet af det omkringliggende samfund og de indsatser, der eksempelvis er igangsat af Politiet, banker, teleselskaber osv.

Af de respondenter, der har angivet, at de kun i mindre grad føler sig beskyttet mod økonomisk svindel på nettet, begrunder størstedelen det med en følelse af ikke i tilstrækkelig grad at være beskyttet af det omkringliggende samfund og de indsatser, der eksempelvis er igangsat af Politiet, banker, teleselskaber osv. Den næststørste andel af respondenter, som kun i mindre grad føler sig beskyttet mod økonomisk svindel på nettet, peger på, at deres angivne svar skyldes, at de selv mangler den fornødne viden og forståelse for, hvordan man beskytter sig selv på nettet.

[20] Det Kriminalpræventive Råd: https://dkr.dk/media/9542/digital-risikoadfaerd.pdf

Figur 10: Hvilke konkrete informationstiltag ville bidrage til, at du følte dig endnu bedre klædt på til at beskytte dig selv mod økonomisk svindel på nettet? (Det er muligt at vælge flere svarmuligheder)



Note: n = 1025

Ovenstående figur viser, hvilke informationstiltag respondenterne peger på i forhold til at klæde dem bedre på til at beskytte sig selv mod økonomisk svindel på nettet. Her peger 63,2 pct. på, at større synlighed om, hvor man kan søge råd og vejledning, kan bidrage. 38,3 pct. peger på større mulighed for at søge råd og vejledning på nettet, og 34,4 pct. peger på informationskampagner i bybilledet, fjernsynet og lignende. Kun 13,5 pct. angiver, at de allerede føler sig tilpas klædt på.

Endelig er respondenterne i et åbent svartekstfelt blevet adspurgt, hvilke andre konkrete tiltag, udover informationstiltag, der ville kunne bidrage til, at de følte sig endnu bedre beskyttede mod økonomisk svindel på nettet. Her nævner størstedelen igen, at der er

behov for mere information og oplysning om økonomisk svindel. Derudover nævner en stor andel af respondenterne, at der bør være en større indsats fra Politi, myndigheder og retsvæsenet i forhold til at opspore, efterforske og straffe kriminelle, der udøver økonomisk kriminalitet på nettet. Eksempelvis skriver en respondent: ”At de relevante myndigheder, primært Politi også rent faktisk gør noget ved anmeldelser. De svigter – sandsynligvis på grund af ressourcemangel”.

Herefter efterspørger den tredjestørste andel af respondenterne, at tech-virksomheder og sociale medier tager et større ansvar og gør mere for at kontrollere deres platforme i forhold til økonomisk kriminalitet. Konkret ønsker borgerne, at tech-virksomheder og sociale medier bliver bedre til at fjerne, blokere og filtrere kriminelt indhold. Derudover nævner enkelte i forlængelse heraf, at der bør være hårdere krav, regler og sanktioner overfor tech-virksomheder og sociale medier i forhold til at forebygge økonomisk kriminalitet.

Endelig nævner en stor andel af respondenterne, at man bør fokusere yderligere på større sikkerhed og verificering ved online transaktioner og login. Konkret ønsker respondenterne, at flere, særligt online handelssider, indfører to-faktor login eller MitID-godkendelse.

4. De primære aktører i forebyggelsen af IT-relateret økonomisk kriminalitet

Øget samarbejde og videndeling på tværs af myndigheder og virksomheder er som beskrevet et fokuspunkt i den nationale strategi for cyber- og informationssikkerhed. Vidensindsamlingen finder i forlængelse heraf, at der i dag samarbejdes om forebyggelse af IT-relateret økonomisk kriminalitet rettet mod voksne borgere på tværs af offentlige institutioner, virksomheder og forskellige aktører fra interesseorganisationer.

I dette kapitel vil de eksisterende større, tværsektorielle samarbejdsfora først blive beskrevet. Herefter vil kapitlet gennemgå de aktører, der er i dag er involveret i forebyggelse af IT-relateret økonomisk kriminalitet, samt hvordan de hver især arbejder med forebyggelse. Beskrivelsen af aktørernes rolle i forebyggelsesarbejdet vil tage afsæt i Det Kriminalpræventive Råds forebyggelsesmodel.

4.1. De eksisterende tværsektorielle samarbejdsfora

Der eksisterer i dag en række samarbejder mellem offentlige myndigheder, interesseorganisationer og private aktører omkring forebyggelsen af IT-relateret økonomisk kriminalitet. Nedenfor er oplistet nogle af de mest væsentlige tværsektorielle samarbejdsfora på området:

1. **Mit digitale selvforsvar:** Mit digitale selvforsvar er en app udviklet af Forbrugerrådet Tænk med økonomisk støtte fra TrygFonden og i samarbejde med Det Kriminalpræventive Råd[21]. Appen er designet til at beskytte brugere mod digitale trusler og vejlede dem i sikker online adfærd. Den fungerer som en personlig sikkerhedsassistent, der advarer om potentielle risici som phishing, svindel og andre former for cyberkriminalitet. Appen bygger på et samarbejde mellem en bred vifte af myndigheder, interesseorganisationer og private aktører, herunder PostNord, Matas, Politiet, Skat, Coop, Jysk, DBA, Center for Cybersikkerhed, Nets, MobilePay, Nordea, Bilka og Telenor. Alle samarbejdspartnere bidrager med deres ekspertise og information og hjælper dermed brugerne med at navigere sikkert i den digitale verden. Brugere af Mit digitale selvforsvar får ikke kun besked om aktuelle digitale trusler, men også praktiske råd om hvordan de kan beskytte sig mod dem, f.eks. ved at genkende mistænkelige e-mails, sikre deres personlige oplysninger og beskytte deres økonomi online. Appen er dermed et vigtigt værktøj til at øge bevidstheden om digitale farer og styrke brugernes evne til at forsvare sig mod dem.

[21] Forbrugerrådet Tænk: https://taenk.dk/om-os/mit-digitale-selvforsvar

2. **Sikkerdigital.dk:** Sikkerdigital.dk er Danmarks fælles og autoritative informationsportal for hjælp og vejledning om digital sikkerhed i regeringens nationale strategi for cyber- og informationssikkerhed[22]. Med borgerne som målgruppe har sikkerdigital.dk særligt fokus på adfærdsændrende indsatser i forhold til digital svindel samt hjælp og vejledning. Sikkerdigital.dk har i flere år stået i spidsen for en stor borgerrettet kampagne – "Kampagne om identitetstyveri" - i samarbejde med blandt andre Det Kriminalpræventive Råd, Politiet, Forbrugerrådet Tænk, Skattestyrelsen, KL, Danske Regioner og Finans Danmark. Formålet med "Kampagne om identitetstyveri" er at hjælpe borgere med at passe bedre på deres personlige oplysninger og undgå identitetstyveri[23]. Som en del af sikkerdigital.dk eksisterer desuden Cyberhotline for digital sikkerhed, hvor man som borger kan få vejledning om, hvordan man bliver mere digitalt sikker samt forebygger svindel og cyberangreb. Desuden kan man kontakte Cyberhotlinen, hvis man har fået misbrugt eller stjålet sin identitet[24]. Sikkerdigital.dk drives og udvikles under Ministerium for Samfundssikkerhed og Beredskab og Center for Cybersikkerhed og har følgende aktører bag sig i en koordineringsgruppe: Politiet, Det Kriminalpræventive Råd, Finanstilsynet, Ældre Sagen, Forbrugerrådet Tænk, KL, Danske Regioner, Finans Danmark, Datatilsynet, Konkurrence- og Forbrugerstyrelsen, Rådet for Digital Sikkerhed og Politiets Efterretningstjeneste (PET).

3. **Forum for it-relateret økonomisk kriminalitet (FIT):** FIT er et samarbejdsforum ledet af Politiets NCIK[25]. Dette forum er skabt for at bekæmpe og forebygge IT-relateret økonomisk kriminalitet gennem et tæt samarbejde mellem myndigheder, organisationer og private aktører. FIT samler ca. 90 aktører på området på tværs af organisationer og brancher. Eksempler på medlemmer i FIT er Finans Danmark, Det Kriminalpræventive Råd, DBA, DSB, PostNord, Gul&Gratis, Dansk Erhverv,

[22] Sikkerdigital.dk: https://www.sikkerdigital.dk
[23] Sikkerdigital.dk: https://www.sikkerdigital.dk/borger/kampagne-om-identitetstyveri
[24] Sikkerdigital.dk: https://www.sikkerdigital.dk/cyberhotline
[25] Politi: https://politi.dk/om-politiet/samarbejde/fit-forum-mod-it-relateret-oekonomisk-kriminalitet

Forsikring og Pension, Nets, Nordea, Forbrugerrådet Tænk, e-mærket og Digitaliseringsstyrelsen. Disse aktører arbejder sammen for at udveksle viden. skabe netværk, koordinere indsatsen og udvikle forebyggende initiativer mod IT-kriminalitet. Derudover skaber FIT, gennem forskellige interesse- og arbejdsgrupper, mulighed for at yde indflydelse og påvirke beslutningstagere og lovgivning i en forebyggende retning.

4. **Udvalget for Borgernes Digitale og Daglige Tryghed:** Det Kriminalpræventive Råd oprettede i 2024 Udvalget for Borgernes Digitale og Daglige Tryghed[26]. Formålet med udvalget er at forebygge kriminalitet ved at øge den digitale dannelse og tryghed blandt voksne borgere. Konkret arbjeder udvalget med: 1) At fremme tekniske tiltag til, og rammer for, borgernes digitale tryghed, 2) Sikre fokus på de kriminalitetstyper, der har betydning for befolkningens tryghed i dagligdagen, 3) Sikre rådets muligheder for at nå relevante målgrupper og 4) Bidrage til rådets kommunikation til og dialog med myndigheder, beslutningstagere og relevante kriminalitetsforebyggende aktører om digital tryghed. Medlemmerne i udvalget er Offerrådgivningen, IDA, National enhed for Særlig Kriminalitet (NSK), NCIK, Teleindustrien, Finans Danmark, Ministerium for Samfundssikkerhed og Beredskab, Ældre Sagen, Forbrugerrådet Tænk, Københavns Politi, Finn Nørgaard Foreningen, Forsikring og Pension, Fritid & Samfund, SSP-Samrådet, Ungdomsuddannelsernes Vejlederforening, Skattestyrelsen og Trine Baumbach, professor i jura ved Københavns Universitet.

5. **Rådet for Digital Sikkerhed:** Rådet for Digital Sikkerhed er en medlemsorganisation, der arbejder for at styrke digital sikkerhed i Danmark[27]. Rådet samler en bred vifte af aktører fra både den private og offentlige sektor, som deler en fælles interesse i at fremme sikkerhed og beskyttelse i den digitale verden. Rådet fungerer som et forum for videndeling, samarbejde og udvikling af løsninger. Medlemmerne inkluderer alt fra forskningsinstitutioner til private virksomheder f.eks.

[26] Det Kriminalpræventive Råd: https://dkr.dk/om-os/organisationen/udvalget-for-borgernes-digitale-og-daglige-tryghed
[27] Rådet for Digital Sikkerhed: https://www.digitalsikkerhed.dk

Alexandra Instituttet, Microsoft, Atea, Danske Bank, Dansk IT, DI Digital, Dubex, Forbrugerrådet Tænk, DK-CERT, IDA IT, Københavns Universitet (KU), Medierådet for Børn og Unge, Roskilde Universitet (RUC), TDC og DIFO.
Rådet udsender løbende nyhedsbreve til sine medlemmer, som holder dem opdateret om de nyeste trends, trusler og løsninger inden for digital sikkerhed. Derudover indkalder rådet til en årlig generalforsamling, hvor medlemmerne har mulighed for at drøfte vigtige emner, udveksle erfaringer og fastlægge rådets fremtidige strategi.

6. **Svindel Task Force:** Finans Danmark nedsatte i december 2023 en Svindel Task Force som en målrettet indsats mod den voksende trussel i forhold til IT-relateret økonomisk kriminalitet[28]. Task Forcens hovedopgave er at gennemføre en omfattende 360 graders analyse af de processer, metoder og IT-systemer, som kriminelle anvender til at begå svindel. Målet er at udvikle nye løsninger, der kan sætte banker og andre finansielle institutioner et skridt foran i kampen mod svindel. Svindel Task Forcen består af en bred sammensætning af eksperter, herunder repræsentanter fra Politiet, teleindustrien, bankerne samt specialister inden for cybersikkerhed og teknologi.

4.2. De primære aktører på området

Udover de eksisterende tværsektorielle samarbejdsfora, der i dag findes på området for IT-relateret økonomisk kriminalitet, er det ligeledes væsentligt at kigge på, hvilke primære ”aktørgrupper” der arbejder med forebyggelse af IT-relateret økonomisk kriminalitet. I denne rapport arbejdes der ud fra termen ”aktørgrupper” for at overskueliggøre, hvilke typer af aktører, der eksisterer på området. En aktørgruppe kan eksempelvis være ”Bankerne”, da denne gruppe dækker over alle landets banker.

[28] Finans Danmark: https://finansdanmark.dk/aktuelle-emner/bekaempelse-af-svindel/svindel-task-force/

De **private aktører** dækker over: 1) Bankerne, f.eks. Danske Bank eller Nordea, 2) Fragtselskaber, f.eks. PostNord eller DAO, 3) Købs- og salgssider, f.eks. DBA, 4) Sociale medier, f.eks. Meta eller Tinder, 5) Tech-branchen, f.eks. tech-virksomheder som Google eller Microsoft og 6) Telebranchen, herunder teleselskaber såsom Telia, Telenor eller Call me.

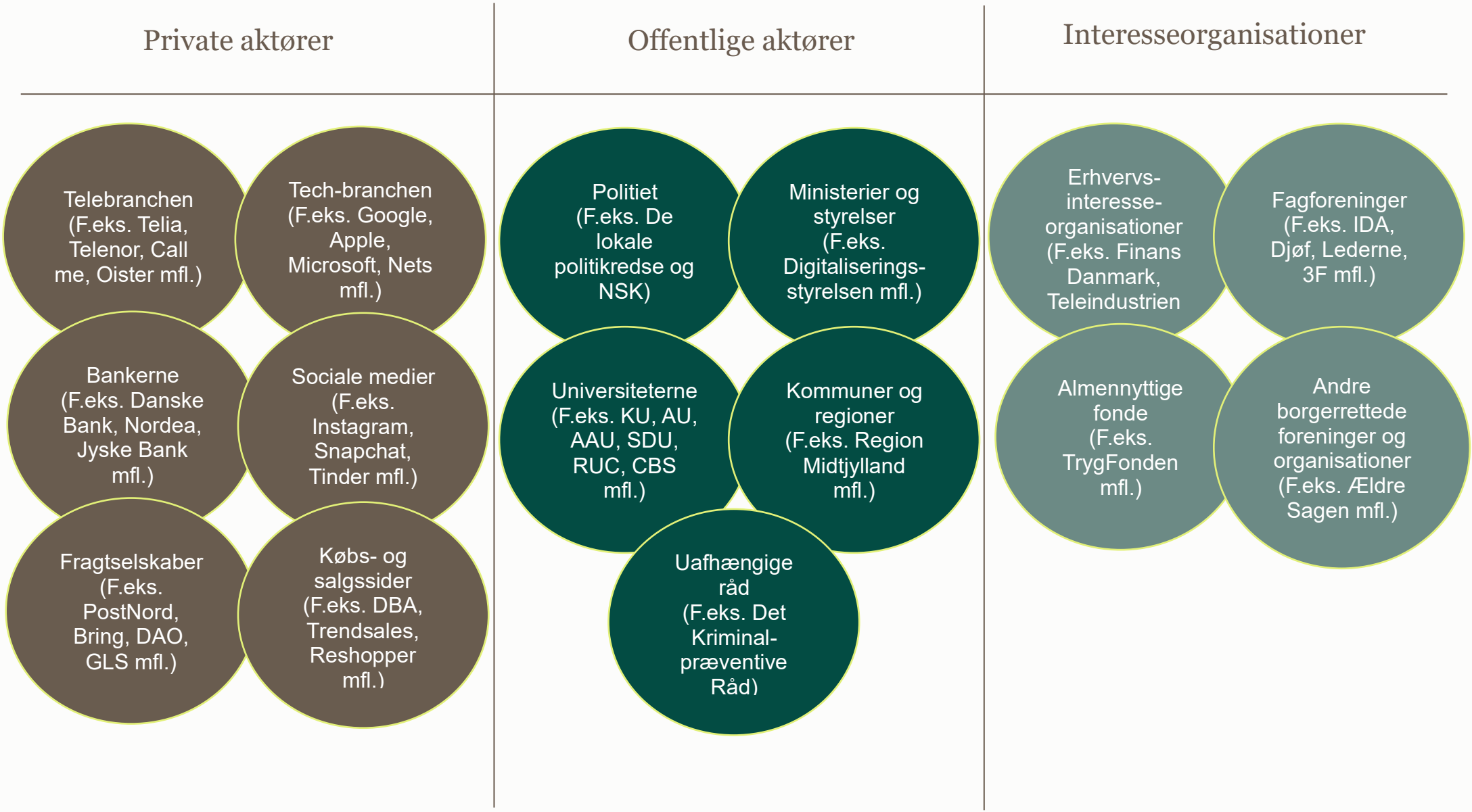
Herefter kommer **de offentlige aktører** på området, som dækker over: 1) Politiet, herunder de lokale politikredse samt NSK og NCIK, 2) Ministerier og styrelser, herunder Ministerium for Samfundssikkerhed og Beredskab, Erhvervsministeriet, Justitsministeriet, Konkurrence- og Forbrugerstyrelsen, Ældreministeriet, Forskningsministeriet, Skattestyrelsen og Finanstilsynet, som alle arbejder med forebyggelse, 3) Universiteterne, f.eks. KU, 4) Kommuner og regioner, der omfatter landets 98 kommuner og fem regioner og 5) Uafhængige råd, f.eks. Det Kriminalpræventive Råd.

Til sidst kommer **interesseorganisationerne** på området, som består af: 1) Erhvervsinteresseorganisationer, f.eks. Dansk Industri, Dansk Erhverv, Teleindustrien eller Finans Danmark 2) Fagforeninger, f.eks. IDA eller Lederne, 3) Almennyttige fonde, f.eks. TrygFonden og 4) Andre borgerrettede foreninger og medlemsorganisationer, som dækker over organisationer som Ældre Sagen, Forbrugerrådet Tænk, Offerrådgivningen eller Rådet for Digital Sikkerhed.

De følgende kapitler vil gennemgå, hvordan de konkrete aktørgrupper arbejder med forebyggelse af IT-relateret økonomisk kriminalitet samt deres formelle og uformelle ansvarsområder.

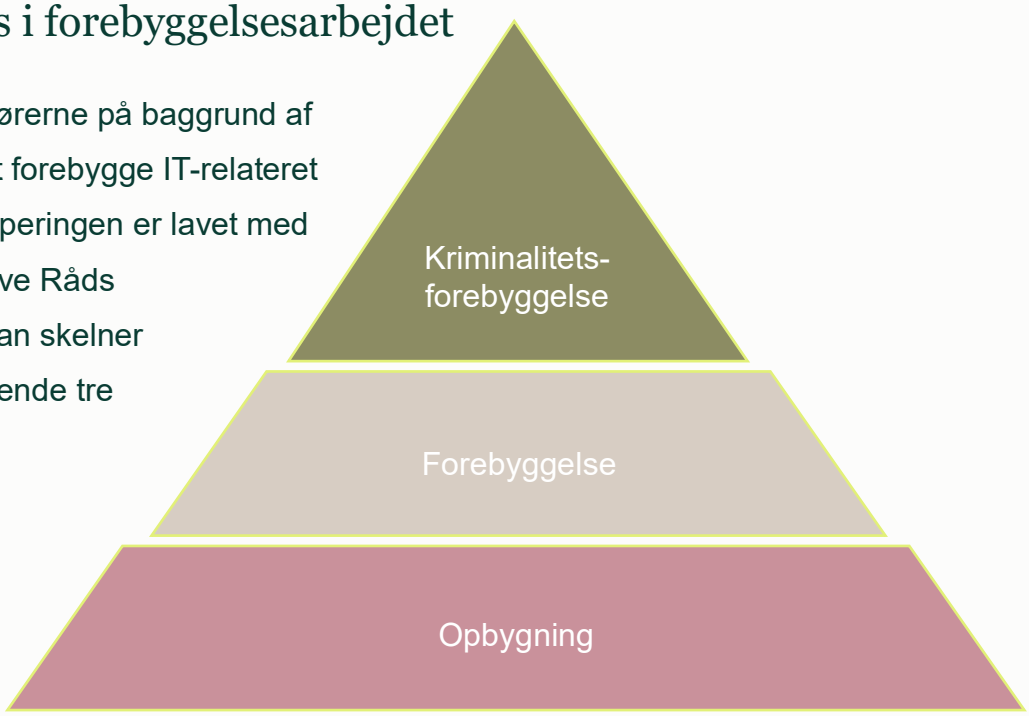
Tabel 1: Landskabet af relevante aktører på området.

OBS: Navne på aktører i de enkelte bobler er udelukkende eksempler på aktører i den enkelte aktørgruppe.



4.3. Aktørernes fokus i forebyggelsesarbejdet

I det følgende grupperes aktørerne på baggrund af deres fokus i indsatsen for at forebygge IT-relateret økonomisk kriminalitet. Grupperingen er lavet med afsæt i Det Kriminalpræventive Råds forebyggelsesmodel, hvor man skelner mellem forebyggelse på følgende tre niveauer: 1) Opbygning, 2) Forebyggelse og 3) Kriminalitetsforebyggelse.[29]



Figur 1: Det Kriminalpræventive Råds forebyggelsesmodel.

Forebyggelsesmodellen er illustreret med trekanten til højre, der også viser, hvordan de tre niveauer bygger ovenpå hinanden med det opbyggende niveau som grundlaget for det forebyggende niveau, som igen er grundlaget for selve kriminalitetsforebyggelsen. Det **opbyggende niveau** dækker over brede indsatser, der generelt handler om at forbedre vilkårene både på et samfundsmæssigt og et individuelt plan. I forhold til IT-relateret økonomisk kriminalitet dækker det opbyggende niveau over aktører, der arbejder med at fremme den generelle uddannelse af borgerne til at kunne begå sig i et digitalt samfund. Dette niveau indbefatter ikke direkte indsatser, som har til formål at forebygge kriminalitet, men omfatter i stedet bredere indsatser, der f.eks. har til formål at undervise borgere i, hvordan man anvender ny teknologi. Herefter kommer det **forebyggende niveau**, som er det mellemste niveau i modellen, der omhandler undgåelse af, at et problem opstår eller forværres. Arbejdet på det forebyggende niveau kan have en kriminalpræventiv effekt, men defineres ikke ud fra at skulle forebygge en bestemt form for kriminalitet. Eksempler på forebyggende arbejde inden for IT-relateret økonomisk kriminalitet er Det Kriminalpræventive Råds løbende rådgivning af myndigheder og private aktører inden for forebyggelse af svindel mod

[29] Det Kriminalpræventive Råd. Forebyggelse af kriminalitet – fire grundbegreber. https://dkr.dk/media/7051/forebyggelsesbegreber2009.pdf

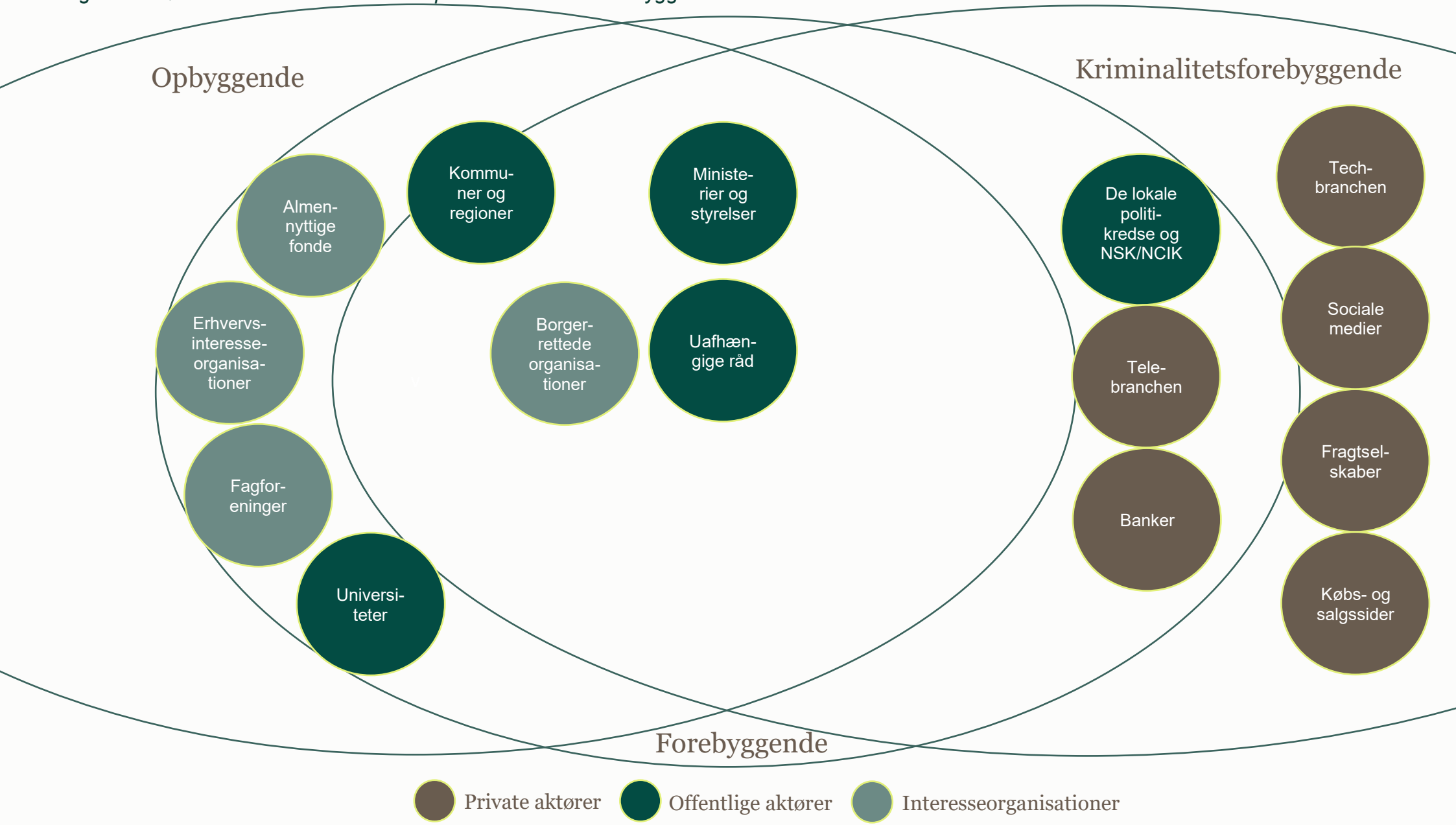
borgere samt Københavns Kommunes nye kampagne: ”*Hvem taler du med?”*, der har til formål at øge bevidstheden og dialogen om digital svindel blandt ens nærmeste relationer for at bidrage til, at borgere oplyser hinanden om forskellige svindelmetoder[30].

Endelig er i spidsen af modellen det **kriminalitetsforebyggende niveau**, der har til formål at forebygge, at specifikke kriminelle hændelser opstår eller gentager sig. Det dækker f.eks. over Politiets arbejde med at identificere de kriminelle, som står bag IT-relateret økonomisk kriminalitet, eller indsatser som har til formål at styrke den tekniske sikkerhed. Dette gælder eksempelvis Teleindustriens arbejde med at styrke sikkerheden i de tekniske løsninger og dermed hindre kriminalitet, eller bankernes arbejde med at styrke sikkerheden i eksempelvis MitID.

På den følgende side er der opstillet en model, som viser, hvordan aktørgruppernes arbejde med forebyggelse af IT-relateret økonomisk kriminalitet rettet mod voksne borgere placerer sig i forhold til forebyggelsesmodellens tre niveauer.

[30] Københavns Kommune, nyhed d. 27. maj 2024. ”Ny kampagne sætter fokus på digital svindel”. https://www.kk.dk/nyheder/ny-kampagne-saetter-fokus-paa-digital-svindel.

Figur 2: Aktørernes niveau i Det Kriminalpræventive Råds forebyggelsesmodel.



Som det fremgår af figur 2, placerer størstedelen af aktørgrupperne sig på flere niveauer i forebyggelsesmodellen samtidig. Anskues figuren fra venstre mod højre repræsenterer den første gruppe dem, som indplacerer sig på både det opbyggende og forebyggende niveau. Dette gælder: 1) Almennyttige fonde, 2) Erhvervsinteresseorganisationer, 3) Fagforeninger og 4) Universiteter. Almennyttige fonde er den aktørgruppe, der placerer sig tættest på det opbyggende niveau, om end flere fonde også arbejder på et forebyggende niveau. Fondene arbejder typisk med forebyggelse af IT-relateret økonomisk kriminalitet ved at støtte projekter og initiativer, der har til formål at ressourceopbygge borgere, så de på sigt står stærkere i forhold til at beskytte sig selv mod IT-relateret økonomisk kriminalitet. Herefter kommer erhvervsinteresseorganisationerne og fagforeningerne. Disse arbejder ligeledes typisk på det ressourceopbyggende niveau ved at lave oplysende kampagner og kurser for deres medlemmer. Endelig kommer universiteterne, som bidrager til forebyggelsesarbejdet i Danmark ved dels at bedrive forskning, som kan anvendes som en del af forebyggelsesinitiativer og dels ved at uddanne borgere. Dette lag med aktører, der primært arbejder med at ressourceopbygge og ikke direkte arbejder med kriminalitetsforebyggelse, indeholder således en klar overvægt af aktører fra interesseorganisationer på området.

Faktaboks: **En problem- eller ressourceorienteret tilgang**

Når man arbejder med forebyggelse kan man have en problemorienteret eller en ressourceorienteret tilgang. Det problemorienterede arbejde ligger særligt i det kriminalitetsforebyggende niveau, hvor fokus er på at løse et konkret problem. Den ressourceorienterede tilgang ligger primært i det opbyggende niveau, hvor fokus er på at opbygge ressourcerne inden for et givent område.

På det forebyggende niveau arbejdes der både problem- og ressourceorienteret.

Den næste gruppe af aktører arbejder på alle tre niveauer. Det gælder: 1) Kommuner og regioner, 2) Borgerrettede organisationer, f.eks. Offerrådgivningen, 3) Uafhængige råd og 4) Ministerier og styrelser, herunder sikkerdigital.dk. Kigger man endnu en gang fra venstre mod højre ses det, at de første aktører primært er offentlige aktører, som arbejder bredt med at udvikle samfundet både på et lokalt og statsligt plan. Den kommunale og regionale aktørgruppe er dog placeret længst ovre mod det opbyggende niveau sammenlignet med de resterende offentlige aktører. Det skyldes, at mange kommuner i

dag fortsat ikke i udpræget grad arbejder direkte kriminalitetsforebyggende, men i stedet arbejder primært opbyggende og forebyggende. Dette gøres f.eks. ved at tilbyde kurser i, hvordan man begår sig på nettet. Derudover afholder sikkerdigital.dk løbende webinarer for bibliotekspersonale og ansatte i kommunerne om, hvordan man som borger bedst beskytter sig selv mod identitetstyveri. I figuren ses dernæst de borgerrettede organisationer, såsom Ældre Sagen og Offerrådgivningen, der ligeledes indplacerer sig på alle tre niveauer, om end de primært befinder sig på det opbyggende og forebyggende niveau. Ældre Sagen arbejder f.eks. med kriminalitetsforebyggelse i organisationens lokalafdelinger ved at afholde arrangementer, hvor medlemmerne kan få indsigt i, hvordan man undgår IT-relateret økonomisk kriminalitet. Ministerier og styrelser, herunder sikkerdigital.dk, og uafhængige råd arbejder i højere grad også på det kriminalitetsforebyggende niveau, hvor disse aktører igangsætter aktiviteter, der har til formål at forebygge, at kriminelle handlinger finder sted eller gentager sig.

Herefter forefindes i figuren de aktører, der arbejder på både det forebyggende og kriminalitetsforebyggende niveau. Det gælder 1) Politiet, 2) Telebranchen og 3) Bankerne. Eksempelvis spænder Politiets forebyggelsesarbejde bredt og inkluderer både direkte borgerkontakt og strategisk prioritering af sager. Et klassisk eksempel på forebyggelse er, når Politiets efterforskere deltager i messer og arrangementer, hvor de har mulighed for at møde borgere ansigt til ansigt. Her underviser de blandt andet ældre borgere om trusler på nettet og giver praktiske råd til, hvordan man kan beskytte sig mod disse.

Til slut i forebyggelsesmodellen er de aktører, som udelukkende arbejder kriminalitetsforebyggende. Fælles for disse aktører er, at de i lavere grad arbejder med at opbygge borgernes ressourcer til at undgå IT-relateret økonomisk kriminalitet og i højere grad arbejder problemorienteret med at bekæmpe eller mindske IT-relateret økonomisk kriminalitet. De aktører, der placerer sig på dette niveau, er følgende: 1) Tech-branchen, 2) Fragtselskaber, 3) Købs- og salgssider og 4) Sociale medier. Feltet af aktører, der udelukkende arbejder kriminalitetsforebyggende, består dermed primært af de private aktører på området, hvis platforme bliver anvendt af kriminelle til at gennemføre IT-

relateret økonomisk kriminalitet. Alle disse aktører samarbejder derfor i variende grad med politiet om kriminalitetsforebyggende indsatser.

Kigger man på tværs af kortet over aktørernes niveauer i forebyggelsesmodellen, fremgår det desuden, at ingen af de primære aktører på området arbejder udelukkende på det opbyggende niveau.

4.4. Formelle og uformelle ansvarsområder

Generelt er der stor forskel i fordelingen af de forskellige aktørers formelle (lovpligtige) og uformelle (frivillige) ansvarsområder i forebyggelsesarbejdet. Formålet med dette afsnit er derfor at skabe overblik over disse forskelle og samtidig identificere områder, hvor der potentielt er behov for yderligere regulering, samt områder hvor frivillige initiativer kan styrkes for at forbedre den samlede indsats mod IT-relateret økonomisk kriminalitet.

Blandt aktørerne med de mest formelle ansvarsområder finder vi Politiet, bankerne, ministerier og styrelser. Disse institutioner er forpligtede ved lov og regulering til at gennemføre forebyggende initiativer, og de har klare retningslinjer og procedurer for deres arbejde. Eksempelvis er bankerne forpligtet igennem §63 i Betalingsloven til at udføre transaktionsovervågning[31].

På den anden side har vi universiteterne, fagforeningerne, erhvervsinteresseorganisationerne og borgerrettede organisationer, som typisk arbejder med en mere uformel tilgang til forebyggelse. Deres initiativer kan omfatte forskningsprojekter, informationskampagner, workshops, uddannelse og samarbejde med andre aktører, der ikke nødvendigvis er reguleret ved lov, men som alligevel bidrager væsentligt til den samlede indsats mod IT-relateret økonomisk kriminalitet.

Med i den uformelle kategori (om end tættere på det formelle end førnævnte) hører derudover tech-virksomheder, sociale medier, fragtselskaber, teleindustrien samt købs- og

[31] Konkurrence- og Forbrugerstyrelsen: https://kfst.dk/media/3cmjx45p/20210212-vejledning-om-betalingslovens-63-final-a.pdf.

salgssider. Fælles for disse aktører er, at de på nuværende tidspunkt er underlagt en vis grad af regulering. Eksempelvis er flere af aktørerne underlagt E-handelsloven[32], der har til hensigt at beskytte forbrugeren i forbindelse med køb af varer på nettet, samt Databeskyttelsesloven[33]. Flere af de interviewede aktører i vidensindsamlingen peger dog på, at disse aktører i fremtiden skal spille en endnu større rolle, når det kommer til forebyggelse af IT-relateret økonomisk kriminalitet. Nogle af de interviewede aktører peger i den forbindelse på, at der bør indføres mere lovgivning og regulering på området samt skabes et større fokus på, at den eksisterende lovgivning håndhæves. Dette vil blive gennemgået i det kommende afsnit.

4.4.1. De interviewede aktørers oplevelse af behovet for at øge formaliseringen af ansvaret på området gennem regulering og lovgivning på området

I takt med at mængden af IT-relateret økonomisk kriminalitet er steget, nævner flere af de interviewede aktører, at der er behov for øget regulering og mere lovgivning på området. Ifølge aktørerne skal formålet med en sådan regulering og lovgivning være at sikre, at de nødvendige aktører har tydeligt definerede ansvarsområder i forhold til forebyggelsen af IT-relateret økonomisk kriminalitet. De interviewede aktører peger særligt på, at der i dag er uklarhed omkring ansvaret for forebyggelse af IT-relateret økonomisk kriminalitet hos særligt store tech-virksomheder som Google eller Microsoft samt sociale medier f.eks. Meta. Denne uklarhed problematiseres i de kvalitative interviews af både videnspersoner og øvrige aktører, hvor de interviewede aktører indikerer, at der med fordel kan placeres mere ansvar hos både de store tech-virksomheder og sociale medier.

"De [tech-virksomheder] vil typisk sige, at de holder sig til lovgivningen. Der er f.eks. diskussioner om deepfakes, hvor kendte personer bliver udnyttet til f.eks. bitcoin-svindel, og det er der nogen, som gerne vil have taget ned – men problemet er, at der ikke er noget lovgivning om det her med deepfakes. Noget andet er noget med jurisdiktion, hvor

[32] Retsinformation, E-handelsloven: https://www.retsinformation.dk/eli/lta/2002/227
[33] Retsinformation, databeskyttelsesloven: https://www.retsinformation.dk/eli/lta/2018/502

der kan være forskellige love i forskellige lande. Så alt sådan noget med infrastruktur, det kan være helt forskelligt sat op - også bare i de nordiske lande. Hvor er data placeret? Hvor bliver den behandlet? I Europa eller en sky i USA? Der er et meget komplekst samspil mellem teknik og jura, som besværliggør hvor meget tech-sektoren vil forpligte sig."

- Offentlig aktør

Det fremgår herudover, at skellet mellem de formelle og uformelle ansvarsområder stiller store krav til den enkelte aktør i forhold til, hvor meget de *skal* gøre og *kan* gøre.

"Man kan gøre noget på alle niveauer. Noget af det handler om at stille nogle flere krav til udbydere [af de digitale tjenester]. De største SoMe-platforme ser jeg f.eks. som en vigtig struktur. Det samme med de største teleudbydere. De gør alle rigtig meget, men spørgsmålet er, om de nogle gange kan gøre det mere effektivt. Jeg er usikker på, om der f.eks. er ting, som nogle af dem ikke gør, men som de kunne gøre, fordi det ikke er i deres interesse."

- Vidensperson

De interviewede aktører påpeger således, at lovgivning og regulering kan bidrage til en tydeliggørelse af, hvad bestemte aktørgrupper *skal* gøre, frem for at det er op til aktørerne selv. I forlængelse heraf er det dog vigtigt at påpege, at der i februar 2024 trådte ny regulering i kraft i form af EU-forordningerne DMA[34] og DSA[35]. Forordningerne indeholder regler, som skal overholdes af de største udbydere af digitale platforme, f.eks. de store tech-virksomheder Google, Apple eller Microsoft og udbydere af sociale medier såsom Meta. Et eksempel på disse regler er, at man skal have samtykke fra brugeren, før man som tech-virksomhed eller socialt medie må sammenkoble brugerens oplysninger på tværs af platforme. På trods af ovenstående peger de interviewede aktører dog stadig på, at der fortsat mangler regulering, som har til formål at beskytte borgerne mod IT-relateret økonomisk kriminalitet ved eksempelvis at stille flere krav til udbydere af digitale tjenester

[34] Konkurrence- og forbrugerstyrelsen: https://kfst.dk/konkurrenceforhold/digitale-markeder-dma/
[35] Konkurrence- og forbrugerstyrelsen: https://kfst.dk/forbrugerforhold/digitale-formidlingstjenester-dsa/

om at fjerne kriminelt indhold på deres platforme. Ingen af de interviewede aktører har talt for at mindske formaliseringen af området ved at deregulere eller fjerne lovgivning. Aktørerne peger derfor også på, at der med fordel kan foretages en videre af analyse af behovene i forhold til lovgivning på området. Endelig oplever flere af aktørerne ligeledes et behov for større fokus på at håndhæve den eksisterende lovgivning og regulering.

4.5. Aktørernes syn på borgerens eget ansvar og arbejde med specifikke borgermålgrupper

4.5.1. Aktørernes syn på borgerens ansvar

De interviewede aktører er generelt enige om, at ansvaret for at undgå IT-relateret økonomisk kriminalitet både er individuelt og kollektivt, og at det dermed både påhviler den enkelte borger at agere ansvarligt, så risikoen for IT-relateret økonomisk kriminalitet mindskes, samtidig med at der er behov for strukturelle tiltag, der adresserer problemet på samfundsniveau. Der findes dog også nuanceforskelle blandt hhv. aktørerne fra borgerrettede interesseorganisationer, de private aktører og de offentlige aktører i forhold til, hvordan balancen mellem de strukturelle og individuelle forebyggelsestiltag bør være.

Især de interviewede aktører fra borgerrettede interesseorganisationer, f.eks. Ældre Sagen eller Offerrådgivningen, mener, at der i dag placeres et for stort ansvar hos borgerne. Disse aktører påpeger, at der med et stadig større trusselsbillede forventes for meget af borgerne og deres kompetencer og muligheder for at beskytte sig selv mod IT-relateret økonomisk kriminalitet. I stedet lægger aktørerne fra borgerrettede interesseorganisationer vægt på, at der bør være endnu større fokus på det strukturelle, samfundsmæssige ansvar i forhold til at beskytte borgerne. En af disse aktører påpeger eksempelvis, at man i den analoge verden ikke pålægger borgerne et lige så stort ansvar for at beskytte sig selv mod kriminalitet, som man gør i relation til IT-relateret kriminalitet. Derudover fortæller flere af aktørerne fra borgerrettede interesseorganisationer, at når borgere udsættes for IT-

relateret økonomisk kriminalitet, kan følelsen af skam forstærkes, hvis der yderligere lægges vægt på, at det er borgerens ansvar at beskytte sig selv.

> *"De forebyggelsesaktiviteter, som vi har set gennem mange år ("pas på", "kig efter", "vær opmærksom" osv.) gør, at det er dig som individ, som hele tiden skal gøre det rigtige og følge med i svindlernes ret innovative forretningsmodeller. Det har meget været borgerens eget ansvar. Hvis den situation havde været analog, er jeg ikke sikker på hvor meget ansvar, der var pålagt den enkelte."*
>
> - Aktør fra interesseorganisation

> *"Man skal huske på, at det ikke er dumme mennesker, der er ofre. Der er generelt en gigantisk underrapportering af disse sager. Vi ser kun toppen af det. Folk er fyldt med skyld og skam. Vi skal have gjort det lovligt at være offer. Så man tør at sige 'Jeg er blevet snydt for hele min pension', uden at folk kigger på en og tænker, at man er dum. Og myndighederne skal ikke tænke: Hvis du er så dum, kan vi ikke hjælpe dig. Det er et kæmpe problem med den skyld og skam, som vi bliver nødt til at tage virkelig alvorligt."*
>
> - Vidensperson

Omvendt er det blandt aktørerne fra den private sektor, at flest lægger vægt på, at borgerne har et ansvar for at holde sig oplyste, være opmærksomme og tænke sig om, når de begår sig på nettet. De interviewede private aktører lægger dog også i høj grad vægt på, at ansvaret også er fælles. Ifølge disse aktører ligger ansvaret således ikke kun et sted, hverken kun hos borgerne, Politiet, telesektoren eller bankerne. I stedet anser de ansvaret som delt, og mener derfor, at alle relevante aktører har en rolle i forebyggelsesarbejdet. Derudover peger de private aktører på, at der er behov for endnu flere tekniske løsninger til at forebygge IT-relateret økonomisk kriminalitet.

> *"Alle rundt om bordet har et ansvar for at bidrage til bekæmpelse af svindel - det gælder både myndighederne, bankerne, teleselskaberne, borgerne, de sociale medier mfl.. Det er ikke muligt for en aktør alene at stoppe alt svindel. Det er et fælles ansvar. Derfor er*

samarbejde helt centralt og jeg tror på, at det er sammen, vi kan styrke bekæmpelse af svindel."

- Privat aktør

Endelig er der de offentlige aktører, som placerer sig et sted imellem de interviewede aktører fra interesseorganisationer og fra den private sektor. De interviewede offentlige aktører mener, at borgerne har et ansvar for at holde sig oplyste til en vis grad, om end ansvaret for at beskytte borgerne i sidste ende ligger særligt hos de offentlige myndigheder og private aktører på området. Ligesom aktørerne fra interesseorganisationer, lægger de offentlige aktører i denne sammenhæng vægt på, at IT-relateret økonomisk kriminalitet er et stort og voksende område, hvor det er komplekst som borger at navigere i, hvordan man beskytter sig selv bedst muligt.

"Jeg synes ikke, at borgerne har så stort et ansvar i den optimale verden, men det kommer de til at få, hvis det skal batte. Det større ansvar ligger ved centraladministrationen og de større virksomheder, men for at de skal tage det ansvar, kræver det, at borgerne kræver det. Så det er svært at undgå, at de får lidt mere ansvar."

- Offentlig aktør

"Jeg vil sige, at der påhviler selvfølgelig borgerne et ansvar om at holde sig oplyste i et vist omfang. Både hvordan er man overfor hinanden, men også sådan noget med, at når der er rødt lys, skal man stoppe. Men skal kende til lovene og vide hvordan man skal agere. Især i den digitale verden er det lidt komplekst, men vi kan ikke betragte borgerne som hovedløse lemminger, som bevæger sig ukritisk rundt i infrastrukturen – det kan man ikke. Vi må kunne forvente et vist niveau at fornuft."

- Offentlig aktør

Der hersker således forskellige opfattelser aktørgrupperne imellem, af hvor stort et ansvar, som borgerne har for at beskytte sig selv mod IT-relateret økonomisk kriminalitet. Flere af aktørerne påpeger i forlængelse heraf, at det er et komplekst spørgsmål om borgernes

ansvar, idet området er nyt og voksende. Derfor kan man i lavere grad forvente, at borgerne ved, hvordan de skal beskytte sig selv sammenlignet med andre kriminalitetsformer. Flere aktører eksemplificerer dette ved, at man som borger er opmærksom på at låse sit hus, når man tager hjemmefra, og samtidig har en forståelse for de mulige konsekvenser ved at lade det stå ulåst. Omvendt kan det være svært som borger at gennemskue, hvordan man beskytter sig selv mod IT-relateret økonomisk kriminalitet og undgår, at ens digitale hjem står "ulåst". På tværs af aktørerne findes der derfor en opfattelse af, at der både skal være fokus på samfundsmæssige, strukturelle og tekniske løsninger, men også forebyggelsesinitiativer der har til formål at oplyse og bestyrke borgerne i, hvordan man bedst beskytter sig selv mod IT-relateret økonomisk kriminalitet.

4.5.2. Aktørernes arbejde med specifikke borgermålgrupper

Langt størstedelen af aktørerne på området har et bredt målgruppefokus. Det gælder særligt de offentlige og private aktører. Flere organisationer blandt aktørerne fra borgerrettede interesseorganisationer er medlemsorganisationer, hvorfor der er en større tendens til at fokusere på bestemte grupper af borgere, f.eks. ældre, forurettede eller personer med beskæftigelse inden for bestemte brancher.

Som en del af vidensindsamlingen er der gennemført en indledende kortlægning af eksisterende studier og analyser på området. Som tidligere beskrevet viser denne kortlægning, at alle voksne borgergrupper, på tværs af både alder og køn, rammes af IT-relateret økonomisk kriminalitet, men af forskellige former for IT-relateret økonomisk kriminalitet[36]. Yngre borgere udsættes i højere grad for samhandelsbedrageri, f.eks. ved køb og salg af billetter til festivaler og koncerter, mens ældre borgere i højere grad udsættes for kontaktbedrageri, f.eks. datingbedrageri (ibid.). I forlængelse heraf påpeger en stor del af de interviewede aktører, at der i dag er et misforstået stort fokus på de ældre

[36] NCIK årsrapport 2023 – En rapport om IT-relateret økonomisk kriminalitet anmeldt i 2023. https://politi.dk/-/media/mediefiler/landsdaekkende-dokumenter/statistikker/ncik/aarsrapport-om-IT-relateret-oekonomisk-kriminalitet-anmeldt-i-2023.pdf

borgere som målgruppe. De interviewede aktører oplever ikke, at der skal fokuseres mindre på de ældre borgere som målgruppe, men at der i højere grad også bør sættes fokus på at forebygge IT-relateret økonomisk kriminalitet blandt de øvrige borgergrupper.

"Vi oplever stor efterspørgsel om råd fra de ældre, hvilket også er helt relevant, men vi skal også ud over den her diskurs om, at det kun er ældre, der rammes. Så vi skal nok også prøve at gentænke den her med kun at komme ud til folk, der kalder på os. Vi vil gerne ramme flere grupper."

- Offentlig aktør

"Man lader til at være ret optaget af ældre mennesker, da det ofte er dem, der er mest sårbare. Det sker ofte på vegne af nogle antagelser om, hvem der udsættes mest. Men denne antagelse kan gøre, at man overser andre vigtige grupper. Folk, der spiller computer, er et eksempel på nogle af dem, der kan være udsatte. Jeg bruger min telefon mere end min mor og stoler måske også mere på den. Så jeg tror virkelig, at man skal være meget påpasselig ift. at antage, hvem der er mest udsatte. Hvis man kun fokuserer på en specifik gruppe, opstår der blinde vinkler, og man glemmer andre grupper."

- Vidensperson

De interviewede aktører peger således på, at der ligger et vigtigt opmærksomhedspunkt i at have fokus på alle borgermålgrupper i arbejdet med at forebygge IT-relateret økonomisk kriminalitet.

5. Udfordringerne i forebyggelsesarbejdet

5.1. Ansvarsfordelingen kan være uklar, særligt på det statslige niveau

På trods af de eksisterende samarbejdsfora på området, herunder sikkerdigital.dk[37], Mit digitale selvforsvar[38], FIT-forummet[39] og Det Kriminalpræventive Råds Udvalg for Borgernes Digitale og Daglige Tryghed[40], opleves det blandt de interviewede aktører, at ansvarsfordelingen på området kan være uklar. Dette gælder særligt i forhold til den centrale, statslige koordinering på området. Som Danmarks fælles og autoritative informationsportal om digital sikkerhed ligger ejerskabet og ansvaret for information og vejledning om digital sikkerhed på det statslige niveau hos sikkerdigital.dk[41]. Dog indgår det forebyggende arbejde i arbejdet hos flere ministerier og styrelser. Eksempelvis ligger arbejdet med Betalingsloven hos Erhvervsministeriet, hvor ministeriet i samarbejde med Finans Danmark, Forbrugerrådet Tænk, Teleindustrien og Ældre Sagen i slut 2023 blandt andet blev enige om at sænke beløbsgrænsen for straksoverførsler per døgn[42]. Samtidig varetager Justitsministeriet det formelle samarbejde med Politiet.

"Koordineringen er noget fragmenteret. Noget, der til tider kan være svært, er ansvarsplacering. Det er svært at afkode, hvilken myndighed der reelt har ansvaret for regulering og håndhævelse. Fordi det digitale rækker på tværs af mange ressortområder, ligger det hos mange."

- Aktør fra interesseorganisation

[37] Sikkerdigital.dk: https://www.sikkerdigital.dk
[38] Forbrugerrådet Tænk: https://taenk.dk/om-os/mit-digitale-selvforsvar
[39] Politi: https://politi.dk/om-politiet/samarbejde/fit-forum-mod-it-relateret-oekonomisk-kriminalitet
[40] Det Kriminalpræventive Råd: https://dkr.dk/om-os/organisationen/udvalget-for-borgernes-digitale-og-daglige-tryghed
[41] Sikkerdigital.dk: https://www.sikkerdigital.dk
[42] Erhvervsministeriet: https://www.em.dk/aktuelt/nyheder/2023/nov/kampen-mod-digitale-svindlere-styrkes

Som en konsekvens af den manglende koordinering giver de interviewede aktører udtryk for en oplevelse af mangel på ejerskab, hvilket i sidste ende kan føre til manglende prioritering af arbejdet med forebyggelse af IT-relateret økonomisk kriminalitet.

"Nogle gange mangler der en fælles forståelse for, at det her er vigtigt. Og at det nogle gange godt må gå ud over andre ting, der også er vigtige. Men når det ikke ligger oplagt i et ministerium, kan der mangle ejerskab."

- Offentlig aktør

Flere interviewede aktører fremhæver, at den centrale statslige koordinering af indsatsen til tider kan opleves som lidt tilfældig. Dette skyldes dels tvivl om, hvor opgaverne og ansvaret ligger, dels usikkerhed om hvilke aktiviteter de forskellige ministerier og styrelser foretager eller har viden om. Det forklares, at denne fragmentering kan resultere i overlappende eller ineffektive indsatser. Aktørerne peger desuden på, at den manglende statslige koordinering og ejerskab over området skaber en situation, hvor forebyggelsesindsatsen kan blive for personbåret.

"Det bliver meget personbåret. Der er helt klart nogle politikredse, der får prioriteret det mere. Men lige nu handler det om klar prioritering fra ledelsen og så interesse fra de enkelte kollegaer. Inden for nogle år vil ting nok blive mere strømlinet."

- Offentlig aktør

De interviewede aktører oplever i forlængelse heraf, at denne afhængighed af enkelte personers engagement peger på et behov for en mere systematisk tilgang, hvor klare ansvarsområder defineres, og en central koordinering sikrer, at indsatsen ikke afhænger af enkelte personers engagement. Det opleves som afgørende at etablere strukturer, der understøtter og fastholder det nødvendige ejerskab på tværs af alle relevante statslige aktører.

5.2. Behov for en bred involvering af aktører i forebyggelsesarbejdet

På tværs af interviewene er der en tendens til, at Politiet tildeles en stor rolle og ansvar for arbejdet med forebyggelse af IT-relateret økonomisk kriminalitet. Her fremhæves særligt NCIK og værdien af denne centraliserede enhed, eftersom denne form for kriminalitet ofte foregår på tværs af landegrænser og derfor kan være udfordrende at håndtere i den enkelte politikreds.

Flere af de interviewede vidanspersoner og aktører peger dog på, at denne tilbøjelighed til at placere ansvaret for forebyggelsesarbejdet hos Politiet hviler på en overvurdering af Politiets evne til at løse problemet med IT-relateret økonomisk kriminalitet på egen hånd. Generelt fremgår det af interviewene med flere aktører fra Politiet, at de er yderst afhængige af viden og input fra de øvrige aktører samt muligheden for at samarbejde om at nå ud til flest mulige borgere.

> *"Jeg køber slet ikke ind på 'Vi kan ikke gøre noget'. Det handler bare om godt samarbejde mellem Politi og banker. Politiet har fastholdt sig selv i den der meget klassiske politirolle. Det er ikke så åbent. Det bliver det klassiske myndighedsarbejde, hvor Politiet sætter sig for bordenden, og så skal man indrette sig efter deres regler. Men det dur ikke. Politiet har også brug for input ift., hvad der foregår."*
>
> - *Vidensperson*

En overvurdering af Politiets ressourcer i bekæmpelsen af IT-relateret økonomisk kriminalitet er bl.a. problematisk, fordi andre aktører, f.eks. private virksomheder og finansielle institutioner, ofte råder over mere avancerede IT-sikkerhedssystemer og specialiseret ekspertise. Ifølge Politiet og vidanspersoner er det derfor afgørende, at Politiet indgår i tæt samarbejde med disse aktører for effektivt at kunne bekæmpe denne type af kriminalitet.

I forhold til andre væsentlige aktører på området peges der i interviewene særligt på de statslige aktører, det vil sige bankerne, sociale medier, ministerier og styrelser - herunder sikkerdigital.dk.

"Det er vigtigt, at ministerierne følger området tæt og med deres kræfter sidder for bordenden for at sikre en løbende fremdrift. Dette er også vigtigt af hensyn til behovet for afklaring af lovgivningen på området, både nu og fremadrettet."

- Aktør fra interesseorganisation

Af de kvalitative interviews fremgår det, at bankerne også spiller en central rolle i forebyggelsen af IT-relateret økonomisk kriminalitet. Bankerne har i forvejen et incitament til at passe på deres kunders penge for at bevare kundernes tillid. Det fremgår derfor, at bankerne ofte bruger meget energi på at forstå de kriminelle ved blandt andet at indsamle information og udføre omfattende transaktionsanalyser. Dette er med til at give dem unikke indsigter, som positionerer dem som en af de øvrige primære aktører.

Blandt de mindre fremtrædende aktører, som alligevel er yderst væsentlige, fremhæves særligt de sociale medier (Meta, Snapchat, Tinder mfl.). Generelt beskriver disse aktører en stor velvilje og motivation for at indgå i dialog og for at engagere sig i forebyggelsen af IT-relateret økonomisk kriminalitet. Dog er det gennemgående for de kvalitative interviews med andre aktører, at de særligt savner involvering af udbyderne af de sociale medier i forebyggelsesindsatsen, hvilket udgør en stor udfordring i forhold til den nuværende forståelse for ejerskab og ansvar på området. I et interview fortæller et socialt medie dog, at de i højere grad gerne vil deltage i fælles indsatser om forebyggelse af IT-relateret økonomisk kriminalitet, især gennem bidrag til informationskampagner.

"Vi håber, at alle har en forståelse for, at der er mange led i denne her samarbejdskæde, og vi vil også rigtigt gerne deltage. Hvis det skal løses ordentligt, er det et fælles ansvar, som både ligger hos Politiet, borgerne, bankerne osv. og selvfølgelig også os. Vi vil særligt gerne spille en større rolle på informationssiden i forhold til at væbne brugere og borgere

bedre, og vi vil hele tiden prøve at blive bedre til at rydde op på egne platforme. Og så tror jeg, at mere informationsudveksling vil være gavnligt."

- *Privat aktør*

Det sociale medie udtrykker således åbenhed overfor fremtidige potentielle samarbejder på området, men ønsker ikke at uddybe yderligere, hvordan konkrete fremtidige samarbejder muligvis kan se ud.

5.3. Regler for datadeling skaber barrierer

Af vidensindsamlingen, tegner der sig et billede af, at regler for datadeling udgør en udfordring for effektiv videndeling imellem aktørerne og dermed for forebyggelse af IT-relateret økonomisk kriminalitet. Strenge databeskyttelseslove og compliance-krav kan gøre det vanskeligt at dele data, hvilket kan betyde, at kriminelle aktiviteter ikke opdages eller kortlægges fuldt ud. Samtidig er det væsentligt, at borgernes følsomme data beskyttes. Flere aktører peger derfor på, at det er nødvendigt at undersøge, hvordan man kan sikre effektiv videndeling på tværs og samtidig bevare beskyttelse af borgernes følsomme data.

***Faktaboks:* Databeskyttelsesloven**

Databeskyttelsesloven er en implementering af EU's General Data Protection Regulation (GDPR) i dansk lovgivning og trådte i kraft i maj 2018, to år efter GDPR blev vedtaget i Europa-Parlamentet. Databeskyttelsesloven regulerer beskyttelsen af persondata og pålægger organisationer at sikre personoplysninger mod uautoriseret adgang og misbrug, således at den enkelte borger i højere grad er beskyttet mod trusler som hacking og datatyveri.

Kilde: Retsinformation, databeskyttelsesloven: https://www.retsinformation.dk/eli/lta/2018/502

"Videndeling er helt centralt i bekæmpelse af svindel. Bankerne må i dag kun dele oplysninger om svindel på et meget overordnet niveau. Det er vores opfattelse, at det vil styrke bekæmpelsen af svindel væsentligt, hvis vi må dele detaljerede oplysninger om kontonumre og kunder, som begår svindel mellem bankerne. Endvidere bør

muligheden for videndeling med andre relevante aktører også styrkes. Mere sammenstilling af data på tværs ville helt klart føre til bedre kortlægning af billedet på IT-relateret økonomisk kriminalitet."

- Privat aktør

"Det, som vi forsøger at gøre, er at hindre det, vi kalder spoofede SMS'er. Vi har lavet forskellige tiltag, hvor vi kan filtrere SMS'er, vi har også lavet tiltag mod spoofede opkald. Vi har dog udfordringer med, hvad det er for en regulering, der gælder for os. Vi vil rigtig gerne gøre en hel masse. Men den der afklaring af, hvad vi må, den mangler. Så det handler om, at anden lovgivning lægger nogle begrænsninger på, hvad vi kan og må. Det gør, at vi ikke kan lave lige så effektive løsninger mod svindel, som vi egentlig godt ville kunne."

- Privat aktør

De interviewede aktører oplever, at når kun overordnede data må deles, er det svært at foretage dybdegående analyser, som ellers ville kunne afsløre mønstre og sammenhænge i kriminaliteten. De oplever, at man uden adgang til detaljerede oplysninger får en fragmenteret forståelse af situationen, hvilket kan forsinke evnen til at reagere effektivt på trusler.

Derudover peger Politiet ligeledes på, at problematikken ikke kun gælder inden for de danske landegrænser, men også på et internationalt niveau. Politiet fremhæver, at en bank eksempelvis kan drives fra Litauen med litauisk CVR-nummer, hvilket kan gøre det vanskeligt for danske myndigheder at få direkte adgang til vigtige oplysninger. Det skyldes, at Politiet ikke må efterforske i udlandet eller anmode om oplysninger uden at gå gennem en tung bureaukratisk proces, hvilket kan forsinke arbejdet betydeligt. Der er derfor et stærkt ønske om at få etableret en fælles international aftale, der giver mulighed for at indhente nødvendige oplysninger, også fra relevante institutioner i udlandet.

5.4. Et svært område at lovgive omkring

Blandt aktørerne og videnspersonerne i denne undersøgelse er der en generel forståelse for, at regulering og lovgivning er vigtigt i forhold til at skabe incitament for at arbejde med forebyggelse af IT-relateret økonomisk kriminalitet. Dog peges der samtidig på, at det kan være svært at følge med svindlerne lovgivningsmæssigt, idet erfaringen viser, at svindlerne og kriminalitetsformerne flytter sig i takt med lovgivningen.

"Lovgivning har helt klart en positiv effekt for forebyggelsesarbejdet, men [eksempel med krav om identifikation] illustrerer også de problemer, der kan være med specifik lovgivning. Så stiger det [svindlen] bare tilsvarende på andre områder. Det med at stille krav er egentlig smart nok, men vandet finder altid en vej."

- Offentlig aktør

"Der er også lidt en tendens til, at lovgivningen bliver enormt detaljeret. Nogle gange ville noget mere overordnet rammelovgivning, som gik lidt mere på udfaldet, være at foretrække."

- Offentlig aktør

I forlængelse heraf peger de interviewede aktører derfor på, at der fremfor meget detaljeret lovgivning i højere grad er behov for agilitet i lovgivningen for at sikre effektive indsatser.

"Det der er ret afgørende, når du skal bekæmpe svindel, er agilitet. Vi skal hele tiden have en bevægelsesfrihed, så vi kan reagere hurtigt. Du kan ikke lave en formel på at bremse svindel. Lovgivning, der f.eks. siger 'stop alle betalinger over 10.000 DKK og til bestemt IP-adresse', kan stoppe nogle ting, men hjælper ikke i det store billede. Hvis de [kriminelle] ved præcis, hvordan vi gør, finder de en måde at komme uden om."

- Privat aktør

Aktørerne peger således ikke på, at nogen konkret lovgivning er forældet. I stedet peger aktørerne på et behov for, at man i forebyggelsesarbejdet fortsat arbejder med lovgivningen og reguleringen på området i en mere agil og overordnet form, så den lettere kan følge med svindlen.

6. Kompetencer, styrker og muligheder

Blandt de interviewede aktører er der blandede opfattelser af, hvor beredte vi er i Danmark i forhold til fremtidens cybertrusler mod borgerne samt stigningen i hastighed og kompleksitet af kriminaliteten.

Offentlige aktører oplever generelt, at vi ikke er helt beredte, men anerkender at det er svært at vurdere præcist. Nogle nævner, at vi i Danmark kan være mere fremsynede og proaktive, end vi er i dag. Flere gange fremhæves England som et land, vi retter blikket mod i forhold til at forudsige kommende problematikker. Aktører fra interesseorganisationer vurderer, at man i Danmark er blevet mere opmærksom på økonomisk svindel på nettet, men at der også eksisterer en falsk tryghed. De peger derfor på, at der er behov for at øge opmærksomheden på problemet blandt borgerne. Private aktører mener i højere grad, at vi er beredte i Danmark og udtrykker generelt en større optimisme. De peger på, at der er etableret gode samarbejder, og at mange tager ansvar. Flere nævner dog, at det er et konstant kapløb, da der hele tiden opstår nye metoder for svindel, hvilket gør det udfordrende at være tilstrækkeligt beredt.

På tværs af de kvalitative interviews fremhæves desuden, at det vil være gavnligt med mere internationalt samarbejde både på et strukturelt plan (fælles platforme, kommunikationskanaler eller arbejdsgrupper, der muliggør samarbejde og informationsudveksling på tværs af lande) og på et strategisk plan (fælles mål, visioner og langsigtede planer for, hvordan man skal tackle problemer eller udnytte muligheder sammen).

6.1. Værdien af tværsektorielt samarbejde

Flere aktører fremhæver værdien af tværsektorielle samarbejder. De forskellige sektorer har forskellige indgangsvinkler, kompetencer og styrker, hvilket gør, at flere aktører kan se en stor værdi i at samarbejde på tværs. Desuden fremhæver flere af aktørerne de værdifulde tværsektorielle samarbejdsfora, der allerede eksisterer i dag. Det gælder blandt andre sikkerdigital.dk[43], Mit digitale selvforsvar[44], FIT-forummet[45] og Det Kriminalpræventive Råds Udvalg for Borgernes Digitale og Daglige Tryghed[46].

"Samarbejder er super vigtigt og en god måde ift. at holde os opdaterede. At arbejde med forebyggelse af IT-relateret økonomisk kriminalitet kræver, at man løbende taler med forskellige aktører. Det er meget sjældent, at vi kan lave tiltag, der kun involverer vores eget område. Det går typisk på tværs af mange ministerier og områder, så det er helt afgørende med samarbejde på tværs."

- *Offentlig aktør*

Eksempelvis har erhvervsorganisationen og arbejdsgiverforeningen Dansk Erhverv adgang til virksomheders oplevelser med sager om CEO Fraud og kopiering af hjemmesider, hvilket aktører som Politiet kunne have gavn af at få viden om. Derudover spiller bankerne en central rolle både før, under og efter svindlen foregår. De har derfor også et indgående kendskab til de kriminelles manipulationsstrategier, og hvilke konsekvenser der er for ofre af svindel. Andre aktører, såsom Ældre Sagen, har viden om specifikke udsatte målgrupper og kan derfor bidrage med viden om, hvordan svindel overfor disse målgrupper kan håndteres. Flere aktører nævner, at myndighederne ikke nødvendigvis er de første til at have kendskab til, hvad der foregår på området, men at de til gengæld har direkte adgang til regulering og lovgivning, hvilket gør dem til centrale aktører at samarbejde med. Af netop denne årsag fremhæver flere desuden, at

[43] Sikkerdigital.dk: https://www.sikkerdigital.dk
[44] Forbrugerrådet Tænk: https://taenk.dk/om-os/mit-digitale-selvforsvar
[45] Politi: https://politi.dk/om-politiet/samarbejde/fit-forum-mod-it-relateret-oekonomisk-kriminalitet
[46] Det Kriminalpræventive Råd: https://dkr.dk/om-os/organisationen/udvalget-for-borgernes-digitale-og-daglige-tryghed

samarbejdsfora som sikkerdigital.dk er gode, da de muliggør udveksling af erfaringer og viden med myndighederne.

Derudover har Politiet en altoverskyggende rolle i forhold til at opklare og retsforfølge. Adskillige aktører nævner og fremhæver FIT-forummet som et værdifuldt netværk af private og offentlige aktører i samarbejdet om at forebygge og mindske IT-relateret økonomisk kriminalitet.

"FIT-forum lyder for mig som det helt rigtige. At Politiet har samarbejde med branchen. Jeg tænker, at det er den vej, vi skal. At vi ikke bare sidder i hver vores sektor og forsøger at knække koden."

- Offentlig aktør

Disse eksempler viser, hvordan forskellige aktører sidder inde med forskellig viden på området. Der er dermed et potentiale for, at aktørerne kan supplere hinanden, og det fremhæver, at samarbejde mellem aktørerne er essentielt, således at denne viden bliver delt og aktiveret de relevante steder. Konkret peger flere aktører på, at der er et stort potentiale i at henvise til hinandens initiativer. Eksempelvis fremhæves det, at aktører med fordel kan henvise til sikkerdigital.dk eller Cyberhotline for digital sikkerhed på deres egne hjemmesider for at styrke den fælles indsats.

6.2. Lovgivning og datadeling i bekæmpelsen af IT-relateret økonomisk kriminalitet

Udover at fremhæve potentialet i at styrke organiseringen og koordineringen mellem de forskellige aktører, tegner denne undersøgelse et billede af et behov for mere viden om, hvordan aktørerne skal forholde sig til gældende lovgivning. Dette gælder f.eks. i forhold til databeskyttelse. Samlet set råder aktørerne over omfattende indsigt, der kan gavne forebyggelsen af IT-relateret økonomisk kriminalitet. Jævnfør afsnit 5.3. betyder Databeskyttelsesloven, at der er behov for at finde løsninger på, hvordan videndeling og

samkøring af data kan ske, samtidig med at borgernes følsomme data beskyttes. Vidensindsamlingens indsigter peger på et stort behov for og potentiale i at se nærmere på hvilke løsninger, der kan imødekomme de lovgivningsmæssige barrierer, der kan opstå.

I forlængelse af dette behov for løsninger på, hvordan aktører kan dele indsigter uden at være i strid med regler for databeskyttelse, peger afsnit 5.4. på et behov for fleksibel lovgivning.

På trods af, at feltet i højere grad kalder på agilitet fremfor detaljeret lovgivning, understreger de interviewede aktører samtidig, at lovgivning er vigtig i forhold til flere parametre. Først og fremmest er det med til at skabe incitament og ejerskab blandt aktørerne. Derudover peger flere aktører på vigtigheden og værdien af borgernes retsfølelse. Flere aktører beskriver, hvordan retsfølelsen er helt afgørende for, at vi fortsat kan tale om Danmark som et tillidssamfund. Selvom der kan være mange grunde til ikke at retsforfølge (kompleksitet, tid, manglende konsekvenser mfl.), kan det dermed være problematisk for både borgernes og virksomhedernes retsfølelse, hvis man for ofte oplever, at sager bliver henlagt:

”Der er f.eks. mange unge mennesker, som oplever at der ikke sker noget, fordi svindlen f.eks. handler om småbeløb. Så der ligger jo et kæmpe mørketal for Politiet. Men man skal ikke undervurdere hvad det betyder for ofrene, når tilbagemeldingen fra os er, at sagen er henlagt.”

- Offentlig aktør

I stedet for at fokusere udelukkende på økonomi og opklaringsrater, peger flere interviewede aktører på, at man i det fremtidige arbejde med IT-relateret økonomisk kriminalitet også bør anerkende værdien af at beskytte borgernes retsfølelse. Dette kan bidrage til at opretholde tilliden i samfundet, selvom det potentielt kræver mere specialiseret og tidskrævende efterforskning.

6.3. Stor viden om ofrene – mindre viden om de kriminelle

I forlængelse af udfordringen med svære efterforskningsvilkår grundet kompleksiteten og hastigen af udviklingen, peger flere aktører på en mangel på viden om dem, som begår IT-relateret økonomisk kriminalitet. Det fremhæves, at man på tværs af sektorer har stor viden om ofre for IT-relateret økonomisk kriminalitet og dermed også en viden om, hvordan man bedst muligt oplyser borgerne og hjælper ofrene, hvis uheldet er ude.

"Vi ved rigtig meget om, hvem de forurettede er. Men vi er ikke så gode til at kigge på, hvem de kriminelle er. En ting er at hjælpe ofrene, men det kunne være rigtig spændende at vide mere om forbryderne, der hvor de inspireres, rekrutteres osv. Vi tænker hele tiden på forebyggelse ift. de forurettede, men der ligger virkelig også et stort potentiale i at tænke på, hvem forbryderne er, så vi kan lave indsatser målrettet dem."

- Offentlig aktør

Dette underbygges også af en af vidensindsamlingens interviewede videnspersoner:

"Jeg synes, at det er interessant, at vi diskuterer forebyggelse, men relativt lidt efterforskning/retsforfølgelse. Jeg er dog med på, at det er svært, når det ofte er internationalt og generelt krydser mange grænser."

- Vidensperson

Denne mangel på viden om de kriminelles identitet og operationer udgør ifølge flere aktører en begrænsning for effektiviteten af forebyggelsesstrategier. Der peges på et behov for at rette mere opmærksomhed mod at identificere og forstå kræfterne bag IT-relateret økonomisk kriminalitet for at målrette indsatserne mere effektivt i fremtiden.

6.4. Potentiale for mere strategiske oplysningsindsatser

Med henblik på fremtidige forebyggelsesstrategier fremhæver flere aktører en central pointe om behovet for en mere strategisk tilgang til oplysningsarbejdet. Oplysningskampagner går igen som den foretrukne metode i forebyggelsesarbejdet, men der kan være et potentiale i at tænke mere i, hvad der rent faktisk skaber forandringer. Eksempelvis fremhæver flere aktører, at der i dag er behov for en samtale om, hvordan man bedst skaber forandring og sikrer, at indsatserne ikke er forvirrende for borgerne. Nogle aktører kommenterer i forlængelse heraf, at det kan virke forvirrende for borgerne, at myndighederne eksempelvis kommunikerer med borgerne via SMS med links i, samtidig med at borgerne frarådes at klikke på links i SMS'er. Den reelle adfærdsændring opleves derfor som svær at gennemføre, så længe indsatserne ikke er koordinerede.

"Vi er gode til oplysning og formidling. Men jeg tror først, det ændrer sig, når der er en reel adfærdsændring. Det er stadig meget nyt at tænke i de baner, men når vi er ude og holde oplæg, kan vi f.eks. blive bedre til at tænke i, hvem vi skal hive ind, der ved noget om det. F.eks. kunne vi [ifm. oplæg] alliere os med nogle teknikere, der har tid til lige at sidde og hjælpe med at lave nogle sikre indstillinger i elevernes telefoner."

- Offentlig aktør

Derudover udtrykkes der også et stort potentiale i at tænke strategisk i forhold til, hvordan man som aktør bedst muligt når ud til flest borgere. Eksempelvis påpeger nogle aktører, at selv ved målretning af adskillige kampagner mod voksne borgere, ændrer dette ikke den kendsgerning, at voksne borgere er travle og ikke har tid til at holde sig løbende opdateret om nye trusler og den seneste udvikling inden for IT-relateret økonomisk kriminalitet. I den forbindelse beskriver flere aktører gode erfaringer med at nå disse borgere gennem deres arbejdspladser. Ligeledes fremhæves det, at det kan være gavnligt at tænke strategisk i forhold til, hvilke grupper der kan målrettes og bruges til at ramme flest slutgrupper.

"Hvis vi rammer nogle af dem, der har med mennesker at gøre, kan vi potentielt ramme rigtig mange på sigt. En politikreds har haft god erfaring med at uddanne

rengøringspersonale ifm. oplysning af ældre. Så kan de 70 personer lige pludselig nå ud til 4000-6000 borgere. Og rengøringspersonalet oplevede også en stor værdi af at have noget at snakke med de ældre om."

- Offentlig aktør

-

Et andet eksempel er f.eks. webinarer fra sikkerdigital.dk, hvor der undervises i svindeltyper, forebyggelse og identitetstyveri. Denne undervisning kan f.eks. målrettes personale fra biblioteker, borgerservice og kommunen, som har hyppig kontakt til borgere, og som formidler om digital sikkerhed.

Der påpeges således i interviewene et behov for, at 1) Der foretages en større koordinering mellem aktørerne i forhold til oplysningsindsatser, så borgere modtager de samme budskaber på tværs af kampagner, samt 2) At man koordinerer sin oplysningsindsats efter hvilke bredere slutgrupper, man ønsker at nå.

På trods af at en stor del af aktørerne peger på en mere koordineret indsats omkring oplysningskampagner, fremgår det i Moos-Bjerres interviews med videnspersoner på området, at der i forskningen og generelt er begrænset viden om den reelle effekt af oplysningskampagner. Forskere peger derfor på, at det er svært at vurdere, hvorvidt denne forebyggelsesstrategi er effektiv[47]. Dog peger forskningen, ligesom de interviewede aktører, på, at det er vigtigt, at man laver klarere og tydeligere kampagner med ensrettede budskaber, samt at kampagnerne er rettet mod bestemte borgermålgrupper (ibid.). Den fortsatte mangel på tydelig evidens for effekten af oplysningskampagner indikerer dog også, at disse ikke kan stå alene som forebyggelsestiltag.

[47] Sipma, T. et. al. (2022): "Victims of cybercrime" i W.v.s., Oerlemans, J-J, Kranenbarg, M.W. (2022): *Essentials in cybercrime. A crimilogical overview for education and practice*

7. Metodebilag

Vidensindsamlingen, som er gennemført i perioden april til august 2024, er baseret på en Social Netværksanalyse (SNA), som er en sociologisk analyseform, hvor aktørers roller og interaktioner i et netværk analyseres. SNA'en sikrer en grundig analyse af aktørernes ansvarsfordeling, rollefordeling og samarbejde.

Todelt desk research

Moos-Bjerre har gennemført en systematisk desk research af feltet omkring forebyggelse af IT-relateret økonomisk kriminalitet målrettet voksne. Desk researchen har haft et todelt fokus: 1) at kortlægge den eksisterende viden på området, og 2) at foretage en indledende aktørkortlægning i form af desk research af hvilke aktører, der arbejder med forebyggelse af IT-relateret økonomisk kriminalitet rettet mod voksne borgere.

1) Kortlægning af den eksisterende viden på området
   I desk researchen af den eksisterende viden på området har Moos-Bjerre identificeret og gennemgået centrale og relevante litteraturstudier, offentlige rapporter og analyser, der belyser forebyggelse og erfaringer med økonomisk og IT-relateret kriminalitet rettet mod borgere. Moos-Bjerre har desuden identificeret de eksisterende retningslinjer og lovgivningen på området gennem officielle, statslige hjemmesider som Retsinformation.dk og Politiets hjemmeside.

2) En indledende aktørkortlægning
   I desk researchen i forbindelse med den indledende aktørkortlægning af området har Moos-Bjerre taget udgangspunkt i en række aktørkategorier: Politi, ministerier og styrelser, offentlige institutioner, banker, telebranchen, tech-branchen, universiteterne, fagforeningerne, kommuner og regioner, interesseorganisationer, fragtselskaber samt købs- og salgssider.

Den indledende aktørkortlægning er gennemført ved hjælp af aktørernes hjemmesider, hvor aktørernes arbejde og niveauet de arbejder på samt aktørernes fokus, målgruppe og muligheder i relation til forebyggelsesarbejdet er blevet identificeret.

Interviews med vidanspersoner

Moos-Bjerre har i forlængelse af desk researchen gennemført fem kvalitative interviews med vidanspersoner med indsigt i det juridiske og forskningsmæssige inden for IT-relateret økonomisk kriminalitet rettet mod borgerne. Vidanspersonerne er udvalgt i samarbejde med Det Kriminalpræventive Råd ud fra en bruttoliste udarbejdet af Moos-Bjerre. Interviewene blev gennemført over Microsoft Teams og havde en varighed på ca. 35-40 minutter. Følgende vidanspersoner har deltaget i interviewene:

Andreas Lieberoth: Lektor i pædagogisk psykologi ved DPU på Aarhus Universitet (AU)
Rasmus Munksgaard: Lektor på Aalborg Universitet (AAU)
Jens Myrup Pedersen: Professor i cybersikkerhed Aalborg Universitet (AAU)
Mads Bryde: Professor i formueret ved Københavns Universitet (KU)
Sune Gabelgaard: Chef for forebyggelse af økonomisk kriminalitet, Vipps MobilePay
Henning Mortensen: Formand for Rådet for Digital Sikkerhed samt CISO/CPO i Brdr. A&O Johansen

Alle interviewene er gennemført ved hjælp af en semistruktureret interviewguide, som havde til formål at give indsigt i vidanspersonernes indsigt i, hvilke borgergrupper, der særligt rammes af økonomisk kriminalitet, hvilke former for IT-relateret økonomisk kriminalitet, der er særligt udbredte, samt hvilke huller og muligheder de så i forhold til de nuværende aktørers arbejde med forebyggelse i dag. Interviewene omhandlede desuden vidanspersonernes generelle billede af, hvilke aktører der er på området i dag samt de gældende retningslinjer og lovgivning på området.

Kvalitative interviews med aktører på området

Moos-Bjerre har gennemført i alt 22 kvalitative interviews med identificerede aktører på området. Interviewene er blevet gennemført med en semistruktureret interviewguide, hvor dele af interviewguiden bestod af mere overordnede spørgsmål om området, imens andre dele indeholdt flere lukkede spørgsmål om f.eks. organisationernes samarbejde med andre aktører. Formålet med denne vekslen var at sikre en åbenhed i interviewene, hvor nye temaer og interessante pointer kunne komme frem, og samtidig sikre svar på de lukkede spørgsmål om aktørernes samarbejde, som skulle bruges i SNA'en.

Udvælgelsen af aktørerne til de kvalitative interviews er sket i samarbejde med Det Kriminalpræventive Råd, som i de fleste tilfælde har udpeget en relevant kontaktperson i organisationen. Udvælgelsen er bl.a. sket med henblik på at sikre repræsentation fra så mange relevante brancher som muligt. Organisationerne har i flere tilfælde selv haft mulighed for at identificere og foreslå de medarbejdere, der bedst kunne repræsentere organisationens erfaringer og viden om IT-sikkerhed. I nogle tilfælde resulterede dette i, at organisationerne identificerede flere relevante repræsentanter i organisationen. I disse tilfælde blev der afholdt gruppeinterviews, hvor flere aktører fra samme organisation deltog. I andre tilfælde, hvor organisationen ikke fremlagde specifikke forslag, tog Moos-Bjerre initiativ til at finde en kontaktperson, som derefter henviste til en relevant medarbejder.

I denne undersøgelse repræsenterer aktørerne de organisationer, som de er ansat i, og deres udtalelser reflekterer således organisationens holdninger og erfaringer med forebyggelse af IT-relateret økonomisk kriminalitet samt deres samarbejdspraksis. Aktørernes udsagn kan dog afspejle deres individuelle kendskab og perspektiver, hvilket indebærer en risiko for bias. For at sikre gennemsigtighed er der nedenfor specificeret, hvilke konkrete personer der er blevet interviewet:

Nationalt Center for IT-Kriminalitet (NCIK): Kresten Munksgaard, Chef for Forebyggelse og Analyse

Københavns Politi: Bjarke Dalsgaard Madsen, Vicepolitiinspektør og leder af Afd. for Økonomisk Kriminalitet

Syd- og Sønderjyllands Politi: Karo Bolding Aaen, Kriminolog

Fyns Politi: Michael Lichtenstein, Vicepolitiinspektør

Tidligere Digitaliseringsstyrelsen, nu Ministerium for Samfundssikkerhed og Beredskab: Morten Rosted Vang, Chef for Kontor for cyber- og informationssikkerhed samt digitale kompetencer

Finanstilsynet: Tobias Thygesen, Chef for kontor for Fintech, Betalingstjenester og Governance

Justitsministeriet: Maria Carlsson, Chef for Politikontoret

Erhvervsministeriet: Jonas Wulff, Fuldmægtig

Det Kriminalpræventive Råd: Tania Schimmel, Forebyggelseschef

Danske Bank: Niels Halse, chef for Afd. for svindelbekæmpelse

Teleindustrien: Jakob Willer, Direktør

Meta Nordic: Martin Ruby, Politisk chef

Nets: Peter James Stark, Head of Public Affairs Europe; Jesper Hjortshøj Larsen, Fraud & AML Analyst; Emil Gade, Fraud Intelligence

IDA: Grit Munk, Chefkonsulent

KL: Jette Larsson, Projektchef (Digitalisering og Teknologi)

Københavns Kommune: Ingeborg Degn, Chef for Sikker By

Forbrugerrådet Tænk: Ulla Malling, Projektchef; Malene Eskildsen, Udviklingskonsulent

Finans Danmark: Mette Stürup, Kontorchef

Offerrådgivningen: Dorte Kallestrup Mortensen, Sekretariatsleder

Dansk Industri: Andreas Holbak Espersen, Digitaliseringspolitisk Chef

Ældre Sagen: Louise Kambjerre Scheel, Seniorkonsulent

Dansk Erhverv: Henrik Lundgaard Sedenmark, Fagchef for betalinger og detailsikkerhed

Befolkningsundersøgelse

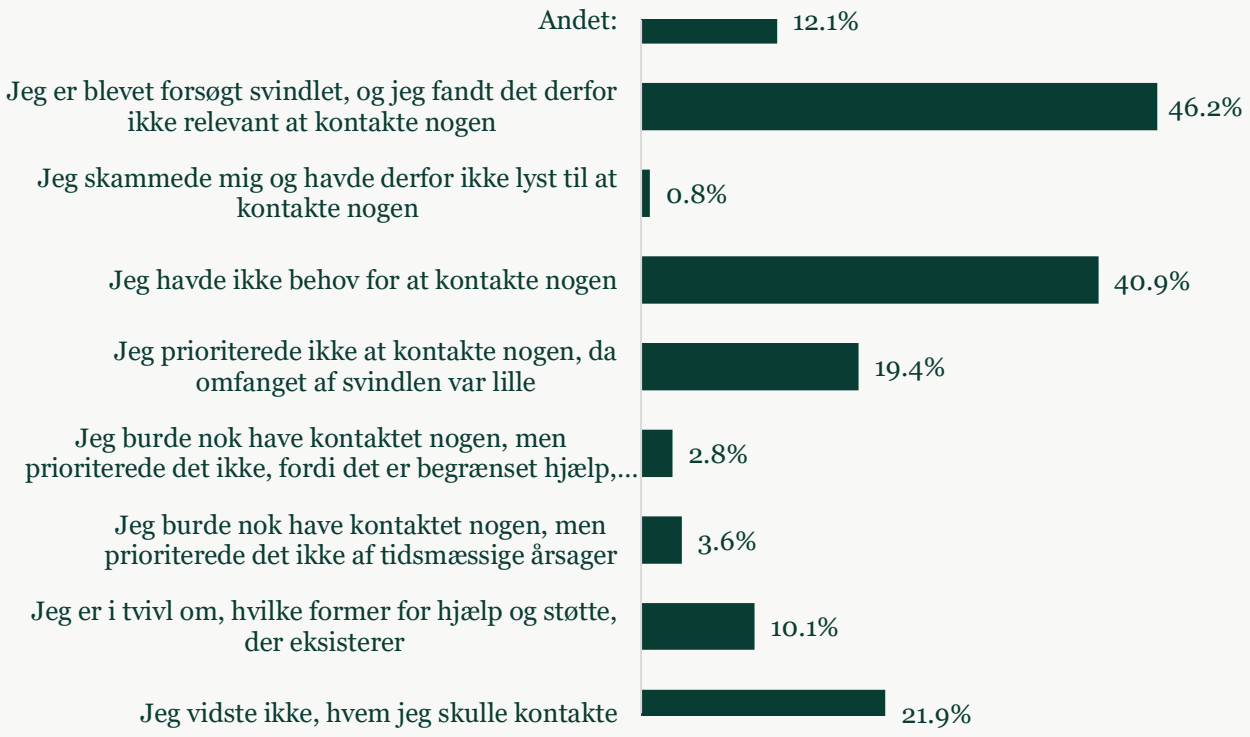
Moos-Bjerre har gennemført en survey blandt et nationalt repræsentativt udsnit af danske borgere over 18 år. I alt har 1025 personer besvaret spørgeskemaundersøgelsen. Formålet med befolkningsundersøgelsen var at undersøge borgernes kendskab til og oplevelse af de aktører, der arbejder med forebyggelse af IT-relateret økonomisk kriminalitet. Befolkningsundersøgelsen er gennemført via dataleverandøren Norstats elektroniske befolkningspanel, som er det største i Danmark og er af høj kvalitet.

Befolkningsundersøgelsen er gennemført efter, at interviewene med aktørerne på området blev gennemført. Det har derfor ikke været muligt i interviewene at spørge aktørerne ind til befolkningsundersøgelsens resultater. Af samme årsag fremgår befolkningsundersøgelsens resultater kun i kapitel 3 og ikke i vidensindsamlingens øvrige kapitler.

8. Bilag: Supplerende resultater fra befolkningsundersøgelse

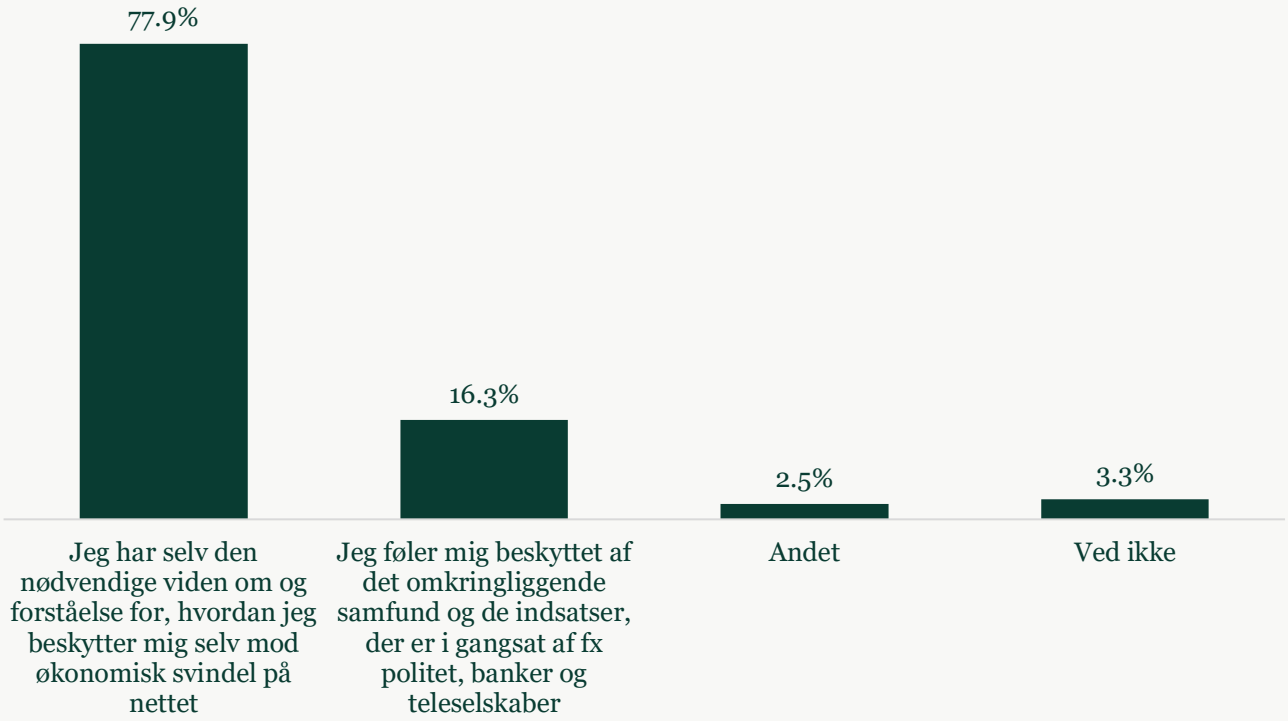
Dette bilag indeholder tre supplerende resultater fra befolkningsundersøgelsen.

Figur 1: Hvad er årsagen til, at du ikke kontaktede nogen, da du blev udsat for økonomisk svindel på nettet eller et forsøg herpå? (Fx politiet, banken, forsikringsselsskab eller lignende)



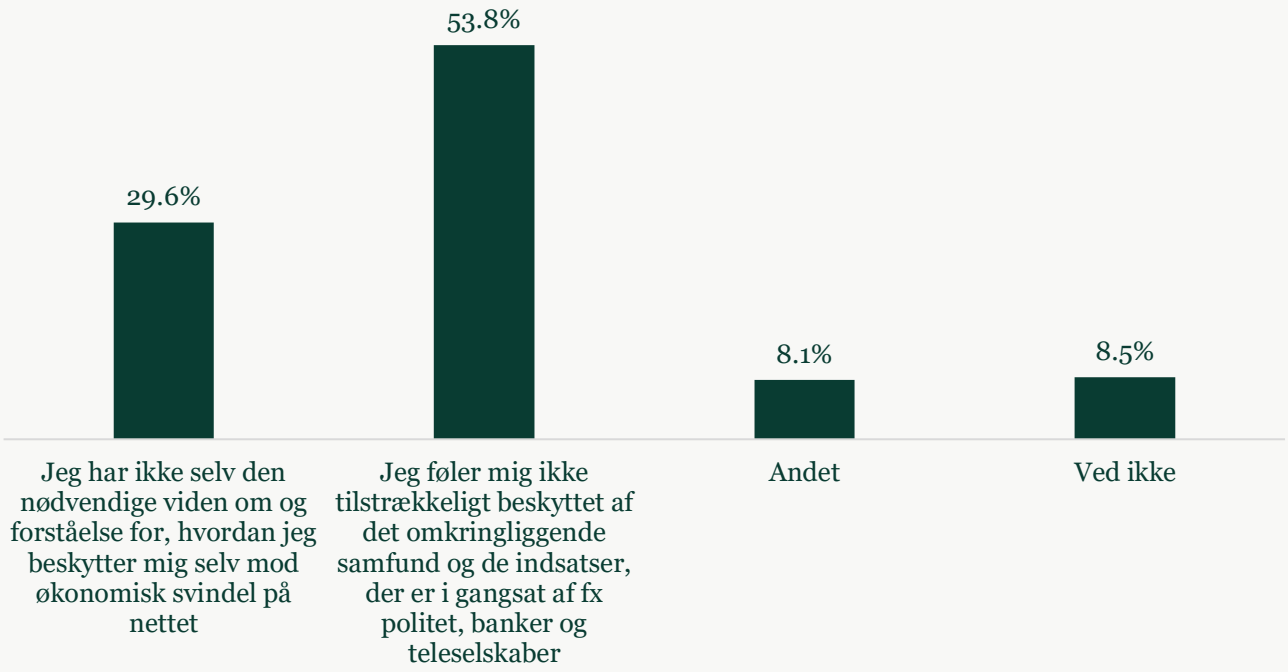
Note: n = 247. Det er kun personer, der har svaret, at de ikke kontaktede nogen i forbindelse med, at de blev enten udsat for eller forsøgt udsat for økonomisk svindel på nettet, der har besvaret dette spørgsmål.

Figur 2: Hvad er den primære årsag til, at du i høj grad eller nogen grad føler dig beskyttet mod økonomisk svindel på nettet?



Note: n = 480. Det er kun personer, der har svaret, at de i høj eller nogen grad føler sig beskyttede mod økonomisk svindel på nettet, der har besvaret dette spørgsmål. De respondenter, der angivet "Andet" uddyber eksempelvis, "At de har en god sikkerhed/Firewall på deres computer", "At de ikke handler meget på nettet" eller "At de er gode til at bruge deres sunde fornuft og tage forbehold selv".

Figur 3: Hvad er den primære årsag til, at du i mindre grad eller lav grad føler dig beskyttet mod økonomisk svindel på nettet?



Note: n = 223. Det er kun personer, der har svaret, at de i mindre eller lav grad føler sig beskyttede mod økonomisk svindel på nettet, der har besvaret dette spørgsmål. De respondenter, der har angivet 'Andet' har uddyber eksempelvis: "Der er så meget svindel", "Det er svært at finde rundt i" og"Svindlerne bliver bedre og bedre". Enkelte skriver desuden, at der ikke er tilstrækkelig håndhævelse eller straf, og at tech-virksomhederne ikke er gode nok til at øge sikkerheden.