Erhvervsudvalget 2024-25
ERU Alm.del - Bilag 81
Offentligt

FINANS DANMARK

Styrket bekæmpelse af digital svindel

Svindel Task Forcens 18 anbefalinger

November 2024

Indhold

Forord

Digital svindel er desværre blevet en del af danskernes hverdag. Vi kender den alle sammen - og en del af os er blevet ofre for den eller har venner, familie eller bekendte, som er. For nogle med store økonomiske og personlige konsekvenser. Det kan vi ikke leve med som samfund.

I december 2023 nedsatte Finans Danmark Svindel Task Forcen. Målet har været at finde nye løsninger og komme et skridt foran i bekæmpelsen af den omfattende kriminalitet. Svindel Task Forcen har gennemført en grundig analyse af de processer, metoder, målgrupper, interessenter og it-systemer, der kommer i spil i forhold til den stigende digitale svindel.

I løbet af vores arbejde har vi fokuseret på de svindeltyper, der har de største økonomiske og menneskelige konsekvenser for ofrene. Vi har derfor især lagt vægt på at identificere anbefalinger, der kan beskytte privatpersoner mod livspåvirkende svindel. Vi har i vores anbefalinger arbejdet med alle svindlens faser, og vi har taget udgangspunkt i de nøgleaktører, som har en særlig mulighed for at kunne reducere svindlen.

Men arbejdet har ikke været let. Svindel Task Forcen har under udarbejdelsen af anbefalingerne måtte forholde sig til en række dilemmaer. Som så ofte ved den hastige teknologiudvikling, så balancerer vi på den ene side ønsket om at skabe et lettere og sikrere liv for brugerne. Og på den anden side hensynet til de etiske dilemmaer der følger med. Det kan være i forhold til beskyttelse af privatlivet og brugerens handlefrihed og så de praktiske implikationer som tid, økonomi og brugervenlighed.

Digital svindel er dynamisk og en trussel i konstant udvikling. Kriminelle tilpasser sig hurtigt nye teknologier og samfundsændringer, hvilket gør det nødvendigt for myndigheder, banker, teleselskaber, sociale medier og mange andre hele tiden at tilpasse værktøjskassen. Arbejdet stopper derfor ikke her. Der vil løbende være behov for at udvikle nye tiltag i kampen mod svindel, og vi opfordrer derfor også til et fortsat stærkt samarbejde mellem især nøgleaktørerne. Bekæmpelse af svindel er en fælles opgave, og én aktør kan ikke gøre det alene.

Det er med stor glæde, at jeg præsenterer denne afrapportering fra Svindel Task Forcen. I en tid, hvor digital svindel udgør en stigende trussel mod både privatpersoner og tilliden til det digitale samfund, er arbejdet mere relevant end nogensinde. Med anbefalingerne forventer vi at kunne bidrage til en bedre og mere effektiv bekæmpelse af digital svindel i Danmark.

Jeg vil gerne takke alle medlemmer af Svindel Task Forcen for deres engagement. Svindel Task Forcen er bredt sammensat med repræsentanter fra politiet, Det Kriminalpræventive Råd, Teleindustrien, cybersikkerheds- og techeksperter og banker. Gruppens ekspertise, bidrag og frugtbare samarbejde har været afgørende for udarbejdelsen af denne rapport. Jeg vil også gerne rette en særlig tak til de mange andre interessenter, som gennem både oplæg, videndeling og møder har bidraget med erfaringer og gode forslag til anbefalinger. Jeg håber, at vores anbefalinger vil blive taget godt imod til gavn for alle, der ønsker at beskytte sig mod digital svindel.

Christiane Vejlø
Formand for Svindel Task Forcen

Digital svindel

I år 2000 blev der registreret 221 bankrøverier i Danmark. I 2022 blev der for første gang ikke registreret et eneste. Men det betyder langt fra, at de kriminelle er forsvundet. For de kriminelle er i stedet blevet digitale, og rigtig mange danskere bliver ofre for digital svindel. Derfor er det vigtigt, at vi som samfund konstant har fokus på at bekæmpe digital svindel.

Sådan ser det ud i dag

Justitsministeriets offerundersøgelse 2005-2023 viser, at 189.000 personer i alderen 16-79 år i 2023 blev udsat for kriminalitet begået på internettet.[1] Samtidig er halvdelen af befolkningen bekymrede for at blive udsat for svindel. Det viser en Epinion-undersøgelse, gennemført for Finans Danmark i 2023.

Svindel Task Forcen har valgt at sætte fokus på at styrke kampen mod den digitale svindel, som har store økonomiske og menneskelige konsekvenser. Det gælder især de svindeltyper, hvor ofrene risikerer at tabe store beløb, hvor tillid og tryghed sættes under pres, og hvor svindlen risikerer at tage en livspåvirkende karakter både økonomisk og menneskeligt. Derfor har Svindel Task Forcen i arbejdet haft fokus på initiativer, som kan begrænse disse svindeltyper – det gælder navnlig netbankssvindel, kærlighedssvindel og investeringssvindel.

Tal fra Danmarks Nationalbank og Finans Danmark viser, at det i 2023 lykkedes de kriminelle at slippe afsted med samlet 464 mio. kroner relateret til netbank-, investerings-, kærligheds- og betalingskortsvindel, jf. figuren. Det er knap 108 mio. kroner mere end i 2022. En stigning på 30 procent.

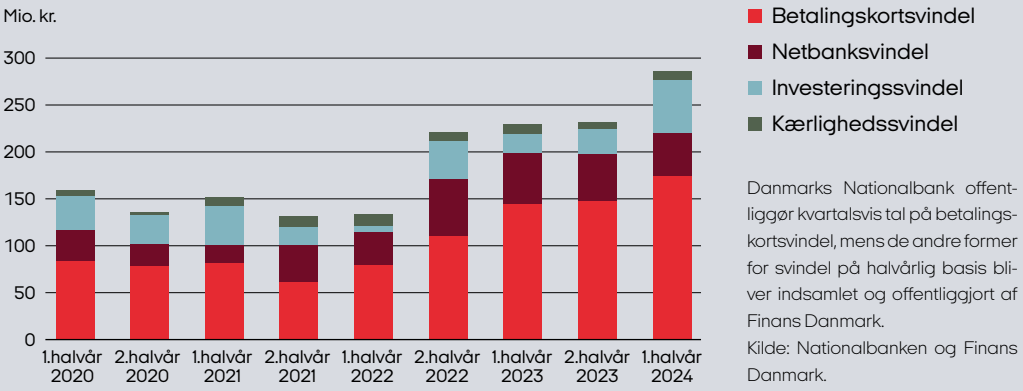
Det højere niveau for svindel er fortsat ind i 2024. I første halvår 2024 var tabet i forbindelse med netbank-, investerings- og kærlighedssvindel på 111 mio. kroner. For misbrug af betalingskort var der et tab på 176 mio. kroner, hvilket er mere end en fordobling siden første halvår 2022, jf. figuren.

Svindlerne udvikler hele tiden nye metoder for at narre folk, og derfor er det vigtigt at være opmærksom på de nyeste svindeltrends. De tilpasser sig konstant nye teknologier og samfundsændringer.

De kriminelle får oftest kontakt til deres ofre gennem fuptelefonopkald, sms'er, e-mails, falske hjemmesider eller sociale medier.

[1] Udsathed for vold og andre former for kriminalitet, Justitsministeriet m.fl., 2024. www.justitsministeriet.dk/wp-content/uploads/2024/05/Offerrapport-2005-2023.-Hovedtal.pdf

Omfanget af betalingssvindel



Danmarks Nationalbank offentliggør kvartalsvis tal på betalingskortsvindel, mens de andre former for svindel på halvårlig basis bliver indsamlet og offentliggjort af Finans Danmark.
Kilde: Nationalbanken og Finans Danmark.

Net- og mobilbanksvindel

Kriminelle overtaler offeret til at overføre sine penge til den kriminelle eller afgive personlige oplysninger, som den kriminelle kan bruge til at overtage offerets net- og mobilbank.

Investeringssvindel

Kriminelle stjæler penge fra offeret ved at lokke med lukrative investeringsmuligheder, ofte gennem svindelannoncer på sociale medier.

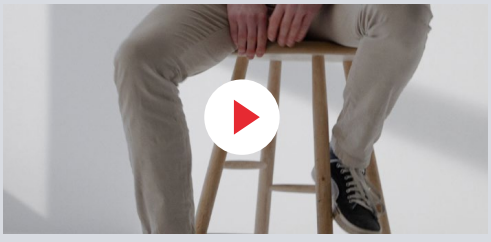
Kærlighedssvindel

Kriminelle udgiver sig for at søge venskab og kærlighed overfor offeret. Undervejs i dialogen får den kriminelle overtalt offeret til at overføre penge.

Betalingskortsvindel

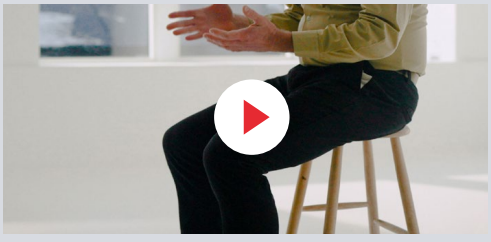
Kriminelle lokker f.eks. offeret til at bruge sit betalingskort på falske hjemmesider. Offeret betaler f.eks. for varer, der aldrig modtages.

Personlige svindelhistorier fra sikkerbank.dk



Aksels historie handler om netbanksvindel

www.sikkerbank.dk



Claus' historie handler om kærlighedssvindel

www.sikkerbank.dk

Netbanksvindel

Netbanksvindel dækker over, at de kriminelle lokker ofrene til selv at gennemføre en betaling til en konto, kontrolleret af de kriminelle. Det kan være ved at narre offeret til at tro, at personen i telefonen ringer fra banken eller politiet for at advare offeret om, at vedkommende er ved at blive svindlet. Når kontakten er skabt, og tilliden er etableret, får den kriminelle offeret til at overføre penge fra sin egen konto til de kriminelles. Det sker f.eks. under påskud af, at pengene skal flyttes til en sikker konto for at undgå yderligere svindel. Alternativt kan det også ske, at en svindler lokker kunden til at overdrage sit MitID til svindleren.

Kærlighedssvindel

Kærlighedssvindel dækker over svindelsager, hvor de kriminelle anvender falske profiler, der udgiver sig for at søge venskab eller kærlighed, mens de over en længerevarende dialog med offeret får vedkommende til at overføre penge. Det kan f.eks. være, at den kriminelle påstår at være blevet syg, og vedkommende har brug for hjælp til at betale en hospitalsregning. Eller den kriminelle beder om penge til at kunne rejse til Danmark for at besøge offeret. Men ingen af delene er sande, og offeret mister pengene. Udover at lide økonomiske tab bliver ofrene for især denne type svindel ofte også stærkt følelsesmæssigt berørt og oplever et markant tillidssvigt i kommunikationen med svindleren. Dette kan få store alvorlige og menneskelige konsekvenser.

Investeringssvindel

Investeringssvindel dækker over svindelsager, hvor ofrene tror, at de investerer deres penge i reelle investeringsprodukter, men investeringen er falsk. Mange investeringssvindelsager opstår via falske reklamer på sociale medier. Det er særligt historier om kendte, der angiveligt skulle have investeret i f.eks. kryptovaluta og har "tjent" mange penge på det. Nu anbefaler de andre at gøre det samme. Men opslagene er falske og ofte med manipulerede billeder og video af den kendte. Når først offeret er lokket ind i universet af den kriminelle, forsøger den kriminelle - ofte gennem længere tid - at få offeret til at investere flere og flere penge.

Betalingskortsvindel

Betalingskortsvindel dækker over forskellige typer af svindel, hvor betalingskortet bliver mis-

Phishing og smishing

Phishing er en form for it-relateret kriminalitet, hvor kriminelle forsøger at narre ofrene til at afsløre fortrolige oplysninger som adgangskoder eller kreditkortnumre. Dette sker ofte gennem falske e-mails, sms'er (smishing) eller beskeder på sociale medier, der ser ud til at komme fra troværdige kilder. Når man klikker på et link og indtaster sine oplysninger på en falsk hjemmeside, bliver de sendt direkte til de kriminelle, som kan misbruge dem.

brugt. Misbruget med betalingskort faldt i en længere årrække frem til 2021. Det hænger i høj grad sammen med nye sikkerhedsforanstaltninger og nye europæiske regler for godkendelse af betalinger. Siden 2021 er kortmisbruget dog steget, fordi kunderne handler mere på udenlandske hjemmesider, og fordi svindlerne har fundet nye metoder til at misbruge betalingskort.

Et eksempel på en ny metode er wallet-baseret svindel, hvor svindleren indrullerer offerets betalingskort i sin egen Wallet, f.eks. Apple Pay, som herefter bliver misbrugt til betalinger. Et andet eksempel er falske bankbude. Her ringer de kriminelle til ofrene og udgiver sig for at være fra banken. De advarer om mistænkelig aktivitet, der gør, at kundens betalingskort skal udskiftes, og at offeret skal oplyse pinkoden. De falske bankbude henter herefter kortet fysisk hos offeret og misbruger det hurtigt til at hæve kontanter og foretage køb.

Svindlerne bruger også i høj grad phishing og smishing. De kriminelle sender falske e-mails og sms'er, der ser ud til at komme fra en bank eller en anden troværdig part. De indeholder et link til en falsk hjemmeside, hvor offeret bliver bedt om at indtaste sine kortoplysninger. De kriminelle bruger derefter disse oplysninger til at misbruge betalingskortet.

Sådan bliver svindlen bekæmpet i dag

Bekæmpelse og forebyggelse af it-relateret økonomisk kriminalitet er en stor opgave, der kræver en koordineret indsats fra både offentlige og private aktører.

Det er også en dynamisk opgave, da de kriminelle hele tiden finder nye metoder til at franarre eller stjæle penge fra bankkunderne på, blandt andet ved at bruge ny teknologi. Aktørerne, der er involveret i bekæmpelsen og forebyggelsen varetager forskellige roller og samarbejder på en række områder om forebyggelse.

Bankerne

Bankerne har i en lang årrække arbejdet med at forbedre indsatserne mod digital svindel og stopper en væsentlig del af den svindel, som finder sted.[2]

[2] Danskere svindles fortsat for millioner – men oplysning og initiativer begynder at virke, Finans Danmark 2024. www.finansdanmark.dk/nyheder/2024/september/danskere-svindles-fortsat-for-millioner-men-oplysning-og-initiativer-begynder-at-virke

Bankerne bruger blandt andet teknologi til at stoppe usædvanlige transaktioner. Alle banker har sænket beløbsgrænsen for straks-overførsler til 50.000 kroner eller mindre om dagen. Det kan bl.a. være en del af årsagen til, at det gennemsnitlige tab pr. sag er faldet i løbet af det seneste år.

MitID spiller en vigtig rolle i kriminalitetsforebyggelsen. MitID er en tofaktor digital identitets- og autentificeringsløsning, der beviser, hvem brugerne er over for f.eks. en netbankløsning. Det gør det sværere for kriminelle at svindle. Sammen med det offentlige investerer bankerne løbende i hele tiden at forbedre sikkerheden i MitID.

FIT

FIT er et samarbejdsforum, der samler aktører fra forskellige sektorer for at koordinere indsatsen mod it-relateret økonomisk kriminalitet. FIT er ledet af politiet og arbejder med at udveksle viden, skabe netværk og udvikle forebyggende initiativer. Det omfatter medlemmer fra både offentlige og private organisationer, der alle bidrager med deres ekspertise.

I 2023 arbejdede op mod 500 bankmedarbejdere med at bekæmpe svindel, og bankerne brugte alene i 2023 750 mio. kroner på det.[3] De kommende år forventer bankerne at fortsætte med at investere kraftigt i bekæmpelse af svindel. Derudover bruger bankerne betydelige ressourcer til bekæmpelse af hvidvask, terrorfinansiering og anden it-relateret økonomisk kriminalitet.

Bankerne har også fokus på oplysning. I 2024 lancerede bankerne en stor fælles kampagne "Sikker bank – sammen", der har nået over 50 millioner eksponeringer via annoncer på sociale medier, TV-reklamer, biografreklamer og avisannoncer.

Politiet

Politiet spiller en afgørende rolle i forebyggelse, efterforskning og opklaring af it-relateret økonomisk kriminalitet. National Center for it-Kriminalitet (NCIK), koordinerer indsatsen mod it-relateret økonomisk kriminalitet. NCIK foretager en visitation og indledende efterforskning i sagerne, inden sagerne sendes videre til den relevante politikreds, der foretager efterforskning med henblik på at rejse sigtelse. Politiet informerer også borgerne om sikker digital adfærd, f.eks. ved lokale borgerarrangementer. NCIK har også oprettet et Forum for it-relateret Økonomisk Kriminalitet (FIT).

Øvrige offentlige myndigheder

Erhvervsministeriet, Ministeriet for Samfundssikkerhed og Beredskab samt Digitaliseringsministeriet har ansvar for lovgivning og regulering på området for digital sikkerhed. Ministeriet for Samfundssikkerhed og Beredskab har ansvaret for at koordinere Den Nationale Strategi for Informations- og cybersikkerhed og for Sikker-

[3] Kampen mod digital svindel, Finans Danmark 2023. www.finansdanmark.dk/media/wbkjrcgy/kampen-mod-digital-svindel_2023.pdf

digital.dk, som tilbyder vejledning om digital sikkerhed og forebyggelse af svindel. Ministeriet har også ansvaret for Cyberhotline for digital sikkerhed, som blandt andet tilbyder vejledning om svindel samt hjælp til ofre, der har fået misbrugt deres identitet.

Tech-virksomheder og sociale medier

Både Tech-virksomhederne og de sociale medier spiller en vigtig rolle, da meget svindel starter på de sociale platforme. Med EU-forordningen om digitale tjenester, som er trådt i kraft i 2024, skal de sociale medier blandt andet hurtigt fjerne eller blokere ulovligt indhold, når de bliver opmærksomme på det. Det inkluderer indhold, der overtræder nationale love eller EU-lovgivning. Konkurrence- og Forbrugerstyrelsen fører tilsyn

EU-forordningen om digitale tjenester

For at sikre et trygt og pålideligt onlinemiljø har udbydere af digitale formidlingstjenester, f.eks. Facebook, pligt til at efterleve en række regler. Reglerne følger af EU-forordningen om digitale tjenester, der på engelsk hedder 'Digital Services Act'.

Kilde: Konkurrence- og Forbrugerstyrelsen.

med forordningen. Hvis styrelsen modtager klager over en platform, som hører under et andet medlemslands tilsyn, vil den videreformidle klagen til dette lands tilsynsmyndighed.

Tech-virksomhederne udvikler løbende teknologiske løsninger for at beskytte brugerne og fjerne falske profiler.

Telebranchen

Telebranchen har implementeret tekniske løsninger for at forhindre svindel. Telebranchen tilbyder løsninger til virksomheder, organisationer og myndigheder, som kan beskytte kritiske fastnetnumre mod spoofing. Endvidere tilbydes løsninger, hvor selskaber, organisationer og myndigheder kan få beskyttet deres sms afsender identitet mod spoofing. Derudover har nogle teleselskaber etableret svindelreducerende løsninger, f.eks. DNS-blokering af skadelige hjemmesider.

Flere teleselskaber arbejder også med at oplyse deres kunder om sikker digital adfærd. De samarbejder med myndigheder og andre aktører for at udvikle effektive forebyggelsesstrategier.

Spoofing

Spoofing er, når kriminelle ændrer, hvordan deres telefonnummer vises ved opkald og dermed foretager opkald, hvor de gemmer sig bag et telefonnummer, f.eks. politiets eller bankens. Derfor kan det se ud som om, at man bliver ringet op fra et troværdigt telefonnummer, selvom det er fra en svindler.

Samme metode anvendes til at sende falske sms'er.

Domain Name System-blokering (DNS-blokering)

En DNS-blokering er en metode, hvor internetudbydere (ISP'er) forhindrer adgang til bestemte domæner eller websteder.

Råd og Organisationer

Det Kriminalpræventive Råd (DKR) er et offentligt råd nedsat af Justitsministeriet. DKR arbejder f.eks. med svindelforebyggelse i forhold til borgere, myndigheder m.m. Arbejdet sker blandt andet gennem medlemssamarbejdet i "Udvalget for Borgernes Digitale og Daglige Tryghed". DKR samler også dansk og international forskning og udgiver råd om forebyggelse af it-relateret økonomisk kriminalitet. DKR har udarbejdet rapporten "Ansvars- og rollefordelingen i forebyggelsen af IT-relateret økonomisk kriminalitet rettet mod voksne borgere".[4]

Organisationerne arbejder især med oplysningskampagner og rådgivning om, hvordan man kan beskytte sig mod it-relateret kriminalitet.

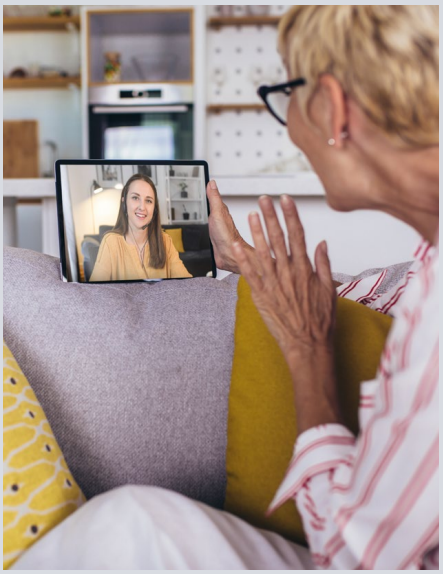
Forbrugerrådet Tænk har udviklet app'en Mit Digitale Selvforsvar i samarbejde med DKR og Trygfonden. App'en advarer brugere om digitale trusler, aktuelle svindelkampagner samt giver råd om sikker online adfærd. Mit digitale selvforsvar er et vigtigt værktøj til at øge bevidstheden

[4] Det kriminalpræventive Råd, oktober 2024, www.dkr.dk/Media/638639086047949912/Ansvars-%20og%20rollefordelingen%20i%20forebyggelsen%20af%20IT-relateret%20%C3%B8konomisk%20kriminalitet%20rettet%20mod%20voksne%20borgere.pdf

Scenariet for et deepfake opkald

Anna modtager et opkald fra, hvad der ser ud til at være hendes datter. Stemmen og ansigtet på videoopkaldet ligner præcis hendes datter, og "datteren" beder Anna om at overføre en stor sum penge til en ny bankkonto, da hun hævder, at hun har brug for pengene til en akut situation.

Svindlerne har brugt deepfake teknologi til at skabe en video af Annas datter, der taler direkte til Anna. Videoen er så overbevisende, at Anna ikke tvivler på, at det virkelig er hendes datter. Anna overfører pengene til den angivne konto, men senere opdager hun, at det hele var svindel.



om digitale farer og styrke brugernes evne til at forsvare sig mod dem.

Ældre Sagen yder en stor indsats for at oplyse deres medlemmer om digital svindel gennem Ældre Sagens hjemmeside, kurser og frivilligt arbejde (særligt Ældre Sagens it-frivillige).

Anvendelse af fremtidens teknologi til svindel

I takt med at teknologien udvikler sig, bliver svindelen mere sofistikeret og sværere at opdage. Det forventes, at en stor trussel i fremtiden vil være svindel baseret på nye teknologier, herunder kunstig intelligens. Et eksempel herpå er brugen af deepfake teknologi, som bruger kunstig intelligens til at skabe realistiske videoer og lydoptagelser, der kan få det til at se ud, som om en person siger eller gør noget, de faktisk ikke har sagt eller gjort. Denne teknologi kan misbruges af svindlere, som i praksis bruger en anden persons stemme og endda ansigt som hånddukke mod deres vilje.

Deepfakes kan bruges til at udføre bedrageri, identitetstyveri, svindel med finansielle transaktioner og endda politisk manipulation. Derudover kan kunstig intelligens bidrage til at analysere store mængder data for at finde sårbarheder, som svindlere kan udnytte. Kunstig intelligens vil derfor i fremtiden udgøre en betydelig trussel i forhold til svindel.

På den anden side spiller kunstig intelligens også en afgørende rolle i bekæmpelsen af svindel. Systemer, baseret på kunstig intelligens, kan analysere store mængder data i realtid for at identificere mistænkelige mønstre og adfærd, som mennesker har sværere ved at fange, f.eks. kan man bruge kunstig intelligens til at overvåge

finansielle transaktioner og opdage usædvanlige aktiviteter, der kan indikere svindel.

Kunstig intelligens kan man bruge til at forbedre sikkerhedssystemer ved, at de konstant kan lære og tilpasse sig til nye svindelmetoder. Kunstig intelligens kan også være med til at verificere identiteter gennem biometrisk data som ansigtsgenkendelse og stemmeanalyse, hvilket gør det sværere for svindlere at bruge falske identiteter.

Kunstig intelligens kan altså udgøre en betydelig trussel i forhold til svindel, men kunstig intelligens kan også være med til at forbedre sikkerheden og beskytte virksomheder og forbrugere. Deep fakes er blot et eksempel på, hvordan ny teknologi kan udgøre en udfordring i bekæmpelse af svindel. Teknologien udvikler sig konstant, og der kan komme andre teknologier, som vil være en udfordring i forhold til svindel. Der er derfor behov for løbende at tilpasse bekæmpelsen af svindel i forhold til de nye teknologier.

Svindel Task Forcens arbejde i 2024

Finans Danmark nedsatte i december 2023 en Svindel Task Force. Den fik til opgave at gennemføre en 360 graders analyse af de processer, metoder og teknologier, der bliver anvendt af de kriminelle. Målet var at finde nye løsninger og komme et skridt foran i bekæmpelsen af den omfattende kriminalitet.

Svindel Task Forcen er bredt sammensat med repræsentanter fra politiet, Det Kriminalpræventive Råd, Teleindustrien, en række cybersikkerheds- og techeksperter samt banker. Formand for Svindel Task Forcen er fremtidsanalytiker og digital strateg Christiane Vejlø.

Sådan har Svindel Task Forcen arbejdet

Svindel Task Forcen har afholdt otte møder.

Svindel Task Forcen har valgt at sætte fokus på at styrke kampen mod den digitale svindel, som har store økonomiske og menneskelige konsekvenser. Det gælder især de svindeltyper, hvor ofrene risikerer at tabe store beløb, hvor tillid og tryghed sættes under pres, og hvor svindlen risikerer at få en livspåvirkende karakter både økonomisk og menneskeligt. Derfor har Svindel Task Forcen særligt arbejdet med initiativer, som kan begrænse disse svindeltyper – det drejer sig om netbankssvindel, kærlighedssvindel, investeringssvindel og betalingskortsvindel. Selvom betalingskortsvindel har været stigende, er det også en svindeltype, hvor kunden har mulighed for at gøre indsigelse over det svindlede beløb til banken, og beløbene er typisk mindre end ved andre svindeltyper. Det er derfor langt overvejende en form for digital svindel, der ikke har livspåvirkende karakter. Ikke desto mindre kan svindelformens hyppighed risikere at få en negativ effekt på den enkeltes incitament og tillid til at handle på nettet. Derfor er betalingskortsvindel også et fokusområde.

Arbejdet har været struktureret ud fra et "før, under og efter"-perspektiv. På den måde er hele svindelforløbet blevet afdækket, og Svindel Task Forcen er kommet 360 grader rundt om svindlen.

Svindel Task Forcen har også set på effekten af anbefalingerne i forhold til, hvad det betyder for anvendelsen af de digitale løsninger. Det vil sige, at der har været fokus på, at de anbefalinger, Svindel Task Forcen kommer med, også kan realiseres.

Svindel Task Forcen og Task Forcens sekretariat i Finans Danmark har været i dialog med

Svindel Task Forcens medlemmer

Christiane Vejlø, formand
Fremtidsanalytiker og ekspert i forholdet mellem mennesker og teknologi. Medlem af Dataetisk Råd

Jakob Willer
Direktør i teleselskabernes brancheorganisation, Teleindustrien

Ann Fonseca Jørgensen
Senior IAM Specialist hos cybersikkerhedsvirksomheden Truesec

Jens Myrup Pedersen
Professor i cybersikkerhed, Institut for Elektroniske Systemer på Aalborg Universitet i København. Landstræner for det danske cyberlandshold og medlem af Cybersikkerhedsrådet

Lone Juul Dransfeldt Christensen
Head of Offensive Security Services, CHO hos cybersikkerhedsvirksomheden Dubex. Certificeret Hacker

Mikkel Hippe Brun
Datalog og Iværksætter. Medstifter af Tradeshift, bestyrelsesmedlem i ZTLment, Head of platform i Session

Morten Tandle
Ekspert i digital sikkerhed og leder af Nordic Financial CERT. Nordic Financial CERT driver en delingshub for nordiske finansielle institutioner mod cyberangreb og digital svindel, samt trusselvurderinger og anti-phishing tjeneste

Tania Schimmel
Forebyggelseschef hos Det Kriminalpræventive Råd

Jesper Kracht
Centerchef hos Nationalt Center for it-relateret økonomiske kriminalitet, National enhed for Særlig Kriminalitet

Medlemmer fra bankerne

Casper Gjerris
It-direktør i Lån & Spar Bank

Mads Skovlund Pedersen
Bankdirektør med ansvar for privatkunder og Country Senior Executive hos Nordea Danmark. Næstformand i Finans Danmark

Mark Wraa-Hansen
Direktør for privatkunder i Danske Bank

Peter Schleidt
Bankdirektør i Jyske Bank med direktionsansvar for bl.a. forretningsservice og forebyggelse af finansiel kriminalitet

Tonny Thierry Andersen
Koncerndirektør i Nykredit

en række forskellige aktører på området, der enten har holdt oplæg på Task Forcens møder eller delt deres ekspertise ved bilaterale møder. Det gælder blandt andet Ældre Sagen, Forbrugerrådet Tænk, Center mod Økonomisk It-svindel, foreningen Digitalt Ansvar, Digitaliseringsstyrelsen, Offerrådgivningen, sociale medier, tech-virksomheder samt forskere på området. Sekretariatet har tillige været i dialog med de øvrige nordiske landes bankforeninger. Der er også indsamlet historier og erfaringer fra ofre.

Etiske dilemmaer

Svindel Task Forcen har under udarbejdelsen af anbefalingerne forholdt sig til en række dilemmaer. Svindel Task Forcen har i behandlingen haft fokus på at balancere anbefalingerne ved på den ene side at gøre det lettere og mere effektivt at bekæmpe svindel – og på den anden side at tage hensyn til de etiske dilemmaer og praktiske implikationer ved de konkrete anbefalinger.

Generelt er det et dilemma, at det på den ene side skal være nemt at foretage betalinger uden gener for kunderne, mens sikkerheden på den anden side skal være i top. Med det følger flere trin og klik. Det kan gøre det lidt mere besværligt for kunden at bruge digitale løsninger.

Vi finder det væsentligt at påpege, at der med de fleste tiltag, som har til formål at komme svindel til livs, vil opstå dilemmaer.

Der er et dilemma i at beskytte kunden mod svindelhjemmesider på den ene side og hensynet til netneutralitet med et frit og åbent internet på den anden side (Anbefaling 1). Der kan også være risiko for, at en blokeringsordning for internettrafik over tid kan blive udvidet til andre områder og dermed være en glidebane i forhold til et frit og åbent internet.

Det er et dilemma i anbefalingen om etablering af et sms-spamfilter (Anbefaling 2), at når man screener forbrugernes sms'er for skadelige links og dermed reducerer antallet af potentielle ofre for svindel, så rejser det samtidig væsentlige spørgsmål i forhold til databeskyt-

Netneutralitet

Netneutralitet sikrer, at forbrugerne har adgang til et frit og åbent internet. Dette indebærer, at internetudbydere skal behandle al trafik lige, og at forbrugerne har ret til frit at få adgang til indhold på nettet og bruge de tjenester og det udstyr, de ønsker. Det er reguleret i en EU-forordning.

telseshensyn og indgreb i brevhemmeligheden. Et flertal af Svindel Task Forcens medlemmer støtter anbefalingen. To medlemmer af Svindel Task Forcen kan ikke støtte anbefalingen.

Et andet dilemma handler om datadeling. Datadeling kan på den ene side bidrage til indsigt i de kriminelles aktiviteter og transaktioner, men på den anden side øger det også overvågningen samt risikoen for datalæk og misbrug af personlige oplysninger. Et eksempel på det er anbefalingen om at reducere antallet af spoofede opkald (Anbefaling 3). Det gælder også for anbefalingen om at dele data fra teleselskaberne til bankerne (Anbefaling 12) og anbefalingen om bedre at kunne dele data mellem aktører ved svindelbekæmpelse (Anbefaling 17).

Anbefalingen om obligatorisk registrering af taletidskort (Anbefaling 4) kan på den ene side medvirke til at gøre det vanskeligere for de kriminelle at udføre deres aktiviteter. På den anden side kan der i obligatorisk registrering af taletidskort være en udfordring i forhold til retten til privatliv, f.eks. kan personer, som bliver forfulgt, have behov for anonym kommunikation. Et flertal af Svindel Task Forcens medlemmer støtter anbefalingen. To medlemmer af Svindel Task Forcen kan ikke støtte anbefalingen.

Anbefalingen om indførelsen af en såkaldt trusted flagger (Anbefaling 5), som kan bidrage til hurtigere og mere effektivt at fjerne indhold på f.eks. sociale medier, rejser spørgsmålet om censur. Det er nødvendigt at fjerne svindelrelateret indhold hurtigt, men det må ikke misbruges til at undertrykke lovlig og legitim kommunikation.

Anbefalingen om at verificere brugernes identitet på sociale medieprofiler (Anbefaling 6) kan på den ene side forhindre oprettelsen af falske profiler. På den anden side kan obligatorisk to-trins godkendelse påvirke brugervenligheden negativt, og nogle brugere kan være bekymrede over at skulle dele deres telefonnummer eller e-mailadresse med sociale medieplatforme for at kunne bruge to-trins godkendelse.

I forhold til anbefalingen om fastfrysning af penge ved svindelmistanke (Anbefaling 9) kan dette på den ene side beskytte mod svindel og økonomiske tab. På den anden side kan det skabe situationer, hvor bankerne ved falske positive tilbageholder kundernes penge, hvilket kan påvirke muligheden for at kunne betale.

Svindel Task Forcen har i arbejdet med anbefalingerne tilstræbt at finde den rette balance i disse dilemmaer. F.eks. har Svindel Task Forcen lagt vægt på, at delingen af data altid skal ske på en dataminimerende måde, hvor kun nødvendige oplysninger deles, og hvor der er klare retningslinjer for og gennemsigtighed i, hvordan processerne forløber, og hvordan data anvendes.

For at afdække dataetiske opmærksomhedspunkter og bias har Svindel Task Forcen inddraget Dataetisk Råd og modtaget rådets perspektiver på de enkelte anbefalinger. Rådets perspektiver har dannet grobund for videre drøftelser i Svindel Task Forcen om nødvendige dataetiske overvejelser og afvejninger.

Svindel Task Forcens anbefalinger

Svindelbekæmpelse kan sammenlignes med et evigt våbenkapløb, hvor svindlere konstant udvikler nye og mere sofistikerede metoder for at undgå at blive stoppet, mens banker, myndigheder og andre aktører konstant arbejder på at bekæmpe kendte trusler og forudse og bekæmpe nye.

Derfor er det også et arbejde, som ikke stopper med Task Forcens anbefalinger. Der vil fortsat være et behov for, at der bliver udviklet nye tiltag, der kan forhindre svindel. Der er ikke én aktør, som kan løse problemet alene, og der er behov for et stærkt samarbejde.

Svindel Task Forcen anbefaler, at der løbende følges op på tiltag, der er implementeret, og på muligheden for at anvende nye og bedre teknologier til beskyttelse af kunderne.

Svindel Task Forcen kommer med 18 konkrete anbefalinger. Anbefalingerne er opdelt i tre faser:

- I "før"-fasen er der fokus på anbefalinger, som kan forebygge svindel og forhindre kontakten mellem svindler og offer.
- I "under"-fasen er fokus på anbefalinger, der kan stoppe og bekæmpe svindlen, mens den udføres.

- I "efter"-fasen er der tale om anbefalinger, som kan være med til at forhindre, at de kriminelle fortsætter med at svindle.

Det skal bemærkes, at der efter Svindel Task Forcen har afsluttet sit arbejde, men inden Svindel Task Forcens anbefalinger er offentliggjort, er blevet indgået en aftale om tre af anbefalingerne med Finans Danmark, Ældre Sagen, Forbrugerrådet Tænk, Teleindustrien, Digitaliseringsministeriet og Erhvervsministeriet den 14. november 2024. Det drejer sig om sms-spamfilterfirewall (Anbefaling 2), bedre beskyttelse af fastnet- og mobilnumre mod spoofing (Anbefaling 3) og bedre phishing beskyttelse i MitID (Anbefaling 13).

Faser i en svindelproces

Kontakt etableres
Før-fasen

- Sociale medier
- Telefonopkald
- sms
- e-mail

Svindlen sker
Under-fasen

- Netbank
- MitID
- Falsk investering
- Overtalelse

Efterforskning og hjælp
Efter-fasen

- Politiefterforskning
- Offerrådgivning
- Forsøg på tilbage-betaling

> Det er afgørende, at svindlen bliver stoppet så tidligt som muligt, før svindleren kommer i kontakt med offeret. Derfor har Svindel Task Forcen haft stort fokus på de redskaber, som ligger tidligt i svindel-processen.

Før-fasen: Anbefaling 1-8

I dag får svindlere især kontakt til ofrene gennem e-mail, telenettet og sociale medier.

På telefonen bliver ofrene kontaktet af svindlere, som udgiver sig for at være fra f.eks. banken eller politiet, eller de modtager sms'er med falske links eller oplysninger. Svindlerne kan virke meget troværdige, når de skal overtale offeret, og ofte lykkedes de med at udnytte bankens, politiets eller fragtfirmaets telefonnummer, så det for offeret ser ud som om, at der faktisk er tale om en seriøs troværdig afsender.

På sociale medier som Facebook, Instagram, Snapchat og TikTok har svindlere ofte held med at lokke ofre til at overføre penge eller oplysninger, f.eks. gennem falske annoncer. Det er nemt for de kriminelle at gemme sig bag falske eller hackede profiler og målrette deres aktiviteter mod helt almindelige brugere.

Det er afgørende, at svindlen bliver stoppet så tidligt som muligt, før svindleren kommer i kontakt med offeret. Derfor har Svindel Task Forcen haft stort fokus på de redskaber, som ligger tidligt i svindelprocessen, og som kan være med til at forhindre kontakt mellem offer og kriminel i første omgang.

1. Bedre blokering af svindelhjemmesider

Svindelsituation

Ofre modtager falske e-mails og sms'er eller scanner QR koder, der alle indeholder links, som fører til svindelhjemmesider, der lokker personlige oplysninger eller penge ud af ofrene. Svindelhjemmesider ligner valide hjemmesider.

Anbefaling

Svindel Task Forcen anbefaler, at der hos alle teleselskaber bliver etableret en supplerende beskyttelse af kunderne, baseret på DNS-blokering af skadelige hjemmesider, så alle privatkunder og virksomheder bliver bedre beskyttet.

DNS-blokering vil kunne forhindre, at brugere, der klikker på disse links, kommer ind på sider med f.eks. phishing, malware, falske webbutikker eller forsøg på identitetstyveri. DNS-blokering giver en bred beskyttelse, da blokeringen ikke er afhængig af, hvilken beskedtjeneste eller e-mail konto der anvendes. Effektiviteten forudsætter tæt samarbejde mellem telebranchen og sikkerhedsbranchen for at opnå en hurtig opdatering.

Svindel Task Forcen anbefaler desuden, at der fra offentlig side bliver etableret en fælles kilde til, hvilke hjemmesider der skal blokeres (uden domstolskendelse), suppleret med input fra relevante parter, f.eks. politiet, Center for Cybersikkerhed og finanssektoren.

For at sikre, at løsningen ikke er i strid med netneutralitetsprincippet, skal det være muligt for kunder at fravælge beskyttelsen.

DNS-blokering vil kunne medvirke til, at brugere, der klikker på svindellinks, ikke kommer ind på svindelhjemmesider.

2. Sms-spamfilter mod svindel sms'er

Svindelsituation

Ofre modtager falske sms'er fra svindlere, som har til formål at lokke personlige oplysninger ud af ofrene. Sms'en ser ud til at komme fra f.eks. en bank eller PostNord og indeholder links, som fører til en falsk hjemmeside.

Det kan føre til identitetstyveri og økonomiske tab for offeret.

Anbefaling

Svindel Task Forcen anbefaler, at der etableres en "sms-firewall" hos mobilselskaberne. Et sms-spamfilter fungerer omtrent på samme måde som et spamfilter på en e-mail konto.

Mobilselskaberne vil analysere mønstre i sms-trafikken ved brug af bl.a. kunstig intelligens og foretage en teknisk analyse af indholdet af sms'er. Hvis der er tydelige tegn på svindel, vil sms'en blive blokeret og vil derfor ikke nå frem til modtageren. Afsender får ikke besked om, at sms'en ikke er kommet frem. Der vil ikke være fysiske personer involveret i screeningen af indholdet af sms'erne.

Filtrering af sms'er anvendes i dag i flere EU-lande, hvor f.eks. Tyskland, Finland, Belgien, Sverige og Polen har implementeret forskellige variationer af sms-filtrering.[5]

Hvis løsningen ikke kan etableres inden for den eksisterende lovgivning, er det Svindel Task Forcens anbefaling, at der bliver etableret en særskilt hjemmel. Det er vigtigt af hensyn til sikkerheden og troværdigheden af sms'er, at løsningen udelukkende bliver anvendt til styrkelse af sikkerheden og ikke bliver brugt eller udvidet til andre formål. Ideelt set vil et sms-spamfilter skulle implementeres med en mulighed for forbrugerne at melde sig ud.

Anbefalingen vil medføre, at langt færre skadelige sms'er når frem til potentielle ofre.

3. Bedre beskyttelse af fastnet- og mobilnumre mod spoofing

Svindelsituation

Ofre modtager opkald, der fremstår, som om de kommer fra f.eks. politiet eller banken. I virkeligheden kommer opkaldet fra udlandet fra en svindler, som har gemt sig bag et "spoofet" dansk nummer. Svindleren benytter spoofing til at øge troværdigheden af sit opkald og derved lokke offeret til at afsløre personlige oplysninger eller til at overføre penge til konti, som svindleren har adgang til.

Anbefaling

Svindel Task Forcen anbefaler at udvide den eksisterende spoofingbeskyttelse i Danmark til at omfatte både fastnet- og mobilnumre mod spoofede opkald fra udlandet. Spoofede opkald fra Danmark kan man lettere spore og retsforfølge.

Anbefalingen indebærer, at teleselskaberne skal undersøge, om det nummer, opkaldet

[5] Teleindustrien/Mavenir, 2024

kommer fra, befinder sig i hjemmenettet eller er i udlandet. Hvis ejeren af nummeret er i Danmark, kan opkaldet ikke være fra vedkommende, når opkaldet kommer fra udlandet. I så fald skal det blokeres. Funktionen vil udelukkende videregive et "ja" eller "nej" til, om kunden er i hjemmenettet. Kunden kan ikke slå funktionen fra.

I dag findes løsningen i både Sverige og Finland.[6] Efter ordningen trådte i kraft i Finland i november 2023, er op til 200.000 svindelopkald forhindret dagligt.[7]

Anbefalingen vil styrke sikkerheden i telenettet og markant forhindre antallet af svindelopkald.

4. Obligatorisk registrering af taletidskort

Svindelsituation

Svindlerne anvender uregistrerede taletidskort, når de ringer til ofre for at overtale dem til at udlevere penge eller oplysninger. Det er vanskeligt at spore, da taletidskortkunder ikke bliver registreret, og derfor er anonyme, når de køber taletidskort.

Anbefaling

Svindel Task Forcen anbefaler, at der bliver indført registrering af navn og CPR-nummer ved køb af taletidskort. Ligesom vi kender det fra et almindeligt telefonabonnement. Ved at lukke eller besværliggøre muligheden for anonyme taletidskort, gør man det sværere for de kriminelle.

Den tidligere regering indførte ved lov, at købere af taletidskort fra den 1. januar 2022 skulle registrere sig med navn og CPR-nummer. Reglen blev indført for at begrænse brugen af taletidskort til kriminelle formål som f.eks. bandekriminalitet. Reglerne er imidlertid ikke implementeret, da Justitsministeriet ikke har udstedt en bekendtgørelse om dette. Svindel Task Forcen anbefaler, at Justitsministeriet snarest muligt udsteder en bekendtgørelse, hvorefter teleselskaberne er forpligtigede til at registrere købere af taletidskort. I Norge, Tyskland, Belgien, Spanien, Italien, Frankrig og Grækenland er der indført forbud mod uregistrerede taletidskort.[8]

Der er dog også legitime formål for anonyme taletidskort. Der kan være tilfælde, hvor et almindeligt hemmeligt nummer ikke er 'nok', f.eks. i tilfælde af social kontrol og stalking. Sådanne legitime formål skal stadig beskyttes i en implementering af anbefalingen. Taletidskort bør kunne registreres med hemmeligt nummer, hvor det alene er myndigheder, som har adgang til oplysninger om identitet.

Anbefalingen vil mindske misbrugen af anonym kommunikation baseret på taletidskort og dermed styrke bekæmpelsen af svindel og andre former for kriminalitet.

[6] Jf. www.traficom.fi/en/news/obligations-regulation-come-effect-200000-scam-calls-are-prevented-day, Traficom, Finland 2024 og Telephone scams (spoofing), Sverige 2024
[7] www.gasa.org/post/finnish-move-blocks-over-200-000-scam-calls-a-day, Global Anti-Scam Alliance, 2020
[8] www.dr.dk/nyheder/udland/svenskerne-vil-forbyde-uregistrerede-taletidskort. DR 2018

5. Nordic Finansiel CERT som "Trusted Flagger"

Svindelsituation

Mange ofre for svindel - især investeringssvindel - er blevet udsat for falske reklamer på sociale medier. Reklamerne har til formål at få offeret til at overføre penge eller personlige oplysninger. De sociale medier har hidtil enten slet ikke eller med meget stor forsinkelse reageret på anmeldelser af svindel fra brugerne.

Anbefaling

Svindel Task Forcen anbefaler, at der oprettes en "trusted flagger" funktion for bankerne på svindelområdet i forhold til relevante sociale medier – f.eks. Facebook, Instagram og TikTok. Task Forcen anbefaler, at Nordic Financial CERT bliver trusted flagger for de nordiske banker.

Trusted flagger ordningen er en mulighed som følger af EU-forordningen om digitale tjenester. Det er en ny fast track-ordning, som har til formål at få platformene til at reagere hurtigere på indrapporteringer af falskt indhold. Ordningen er allerede taget i brug på ophavsretsområdet. Det vil give mulighed for en hurtigere nedtagning af falske reklamer og svindelrelateret indhold på sociale medier, da indberetningerne kommer fra en legitim og troværdig kilde. Derfor kan platformen reagere hurtigt på det.

At blive trusted flagger kræver en myndighedsgodkendelse. Trusted flagger funktionen skal finansieres af Nordic Financial CERT's medlemmer (nordiske banker og forsikringsselskaber).

Nordic Financial CERT som trusted flagger vil give mulighed for, at bankerne får en direkte og hurtig kanal til indrapportering af svindel til de sociale medier. Trusted flagger funktionen vil minde om den opgave, som Nordic Financial CERT i dag varetager for de nordiske banker i form af nedtagning af falske hjemmesider. Nordic Financial CERT nedtager årligt omkring 10.000 falske hjemmesider.

Anbefalingen vil reducere risikoen for at blive udsat for falske reklamer på sociale medier.

6. Krav om to-trins godkendelse på sociale medier

Svindelsituation

Ofre for digital svindel bliver ofte udsat for svindel fra hackede profiler på sociale medier. Svindlere overtager legitime profiler og stjæler brugeres identitet, hvilket skaber et troværdigt dække for yderligere svindelforsøg. Dette skyldes især, at ikke alle sociale medier er lige gode til at udbrede muligheden for at sikre profiler med to-trins godkendelse.

Anbefaling

Svindel Task Forcen foreslår, at det bliver obligatorisk for sociale medier at implementere to-trins godkendelse for deres brugere.

Dette kan ske enten gennem dansk særlovgivning eller en revideret udgave af EU-forordningen om digitale tjenester. I dag er det op til

brugerne selv at vælge, om de vil aktivere to-trins godkendelse. Hvis man opsætter to-trins godkendelse, bliver man som bruger bedt om at bekræfte et loginforsøg, hver gang der benyttes en ukendt browser eller mobilenhed.

To-trins godkendelse vil gøre det væsentligt sværere for svindlere at overtage konti og anvende dem til svindel eller anden kriminalitet. Den endelige løsning bør tage hensyn til behovet for brugervenlighed på de berørte platforme.

Anbefalingen vil kunne begrænse hackede profiler på sociale medier.

7. Digital svindel på skoleskemaet

Svindelsituation

Unge bliver – som alle andre – udsat for forskellige typer af digital svindel. Men særligt svindel i forbindelse med køb og salg mellem private på handelsplatforme, f.eks. ikke eksisterende studieboliger eller via applikationer på deres telefoner, fylder for de unge. Udover risikoen for at blive udsat for svindel er de unge også i risiko for at medvirke til svindel, f.eks. ved at de uvidende/vidende fungerer som muldyr, hvor de lægger bankkonto eller telefonnummer til svindlernes aktiviteter.

Anbefaling

Svindel Task Forcen anbefaler, at faget teknologiforståelse bliver indført som et obligatorisk fag for 7.-9. klasse.

Det er allerede politisk besluttet, at faget teknologiforståelse skal indføres i folkeskolen som valgfag. Samtidig skal eksisterende fag i folkeskolen præges, så undervisningen forholder sig til nye teknologier og digitale faldgruber.

Svindel Task Forcen anbefaler, at læseplanen kommer til at indeholde undervisning i sund digital adfærd og kildekritik, så eleverne får kendskab til de mest relevante svindeltyper og behovet for at være på vagt på sociale medier. Dette skal også indarbejdes i de eksisterende fag i folkeskolen. Det vil både skærpe unges kendskab til og modstandsdygtighed mod de svindeltyper, som er de mest sandsynlige, de vil blive udsat for.

Anbefalingen vil give kommende generationer en bedre forståelse af digital svindel og kompetencer til håndtering af det digitale univers og de farer, der er ved det.

8. Oplysningsindsats fra bankerne om svindel

Svindelsituation

Svindelmetoder udvikler sig med stor hastighed og er teknisk avancerede. Det gør det meget svært for borgerne at følge med og være på vagt over for nye trusler. Det er vigtigt, at borgerne har kendskab til, hvordan man kan opdage svindel.

Anbefaling

Svindel Task Forcen anbefaler, at bankerne løbende gennemfører oplysningskampagner rettet mod relevante kundesegmenter, samt oplyser om digital svindel i den løbende dialog med alle kunder. Det vil øge bevidstheden om digitale trusler. Kampagner kan også blive gennemført som fælles sektorinitiativer, f.eks. som i "Sikker bank – sammen"-kampagnen.

Svindel Task Forcen lægger vægt på, at bankerne løbende skal give klare oplysninger til kunderne om, hvordan de kan identificere svindel og advare dem om de nødvendige foranstaltninger og forholdsregler, der kan træffes for at undgå, at kunderne bliver ofre for svindel.

Svindel Task Forcen anbefaler, at bankerne forsætter deres "Sikker bank – sammen"-kampagne i 2025. Samtidig skal kommunikationsindsatsen på tværs af sektorer og det offentlige koordineres stærkere, så den samlede indsats styrkes. Koordineringen kan blive forankret i Sikkerdigital.dk under Ministeriet for Samfundssikkerhed og Beredskab som et offentlig/privat samarbejde.

Samlet set vil en målrettet kommunikationsindsats og øget bevidsthed hos medarbejderne i bankerne bidrage til en bedre forebyggelse af svindel.

Under-fasen: Anbefaling 9-13

I de tilfælde, hvor svindleren har held til at skabe en troværdig kontakt til offeret og overtale offeret til at overføre sine penge eller oplysninger til svindleren, er der brug for stærke tekniske løsninger, som kan bremse svindlen.

I Danmark er det ofte nemt at bruge samfundets digitale løsninger, hvad enten man skal flytte penge, skifte forsikring eller begynde på en uddannelse. De stærke og brugervenlige digitale løsninger gør hverdagen lettere for de fleste danskere, men de skaber også et attraktivt grundlag for svindlerne. For med få klik kan vi i dag overføre penge eller gennemføre betalinger, og det kan svindlerne udnytte. Det er vigtigt, at det i fremtiden fortsat er nemt og enkelt at udføre sine betalinger og andre digitale ærinder.

Bekæmpelsen af svindlen kan medføre lidt flere forsinkelser, og lidt flere kontroller for kunden, og det kan opleves som irriterende. Men de kan være nødvendige for at styrke sikkerheden og forhindre svindlere i at slippe afsted med ofrenes penge. Med anbefalingerne i "Under-fasen" sigter Svindel Task Forcen især på de løsninger, som bankerne driver, da betalingerne går igennem bankens løsninger.

9. Fastfrysningsordning ved svindelmistanke

Svindelsituation

Svindel med bankoverførsler er et stigende problem og rammer alle typer af borgere gennem en bred vifte af svindelmetoder. De kriminelle anvender især straksbetalinger, da det gør det muligt for den kriminelle hurtigt at flytte det svindlede beløb mellem flere konti i forskellige banker. Det gør det vanskeligt at stoppe svindlen og tilbagebetale pengene til offeret.

Anbefaling

Svindel Task Forcen anbefaler, at danske banker etablerer en it-understøttet fastfrysningsordning af de overførte penge ved mistanke om svindel. Det kan f.eks. være i de tilfælde, hvor der bliver foretaget en for kunden usædvanlig transaktion, f.eks. en overførsel af et større beløb, som kunden ikke plejer at gøre.

Med ordningen kan den bank, der sender en betaling, iværksætte en fastfrysning af beløbet på kontoen i den bank, der modtager betalingen. Afsenderbanken kan bruge ordningen, hvis en kunde henvender sig om en konkret svindelmistanke, eller når afsenderbanken selv har en mistanke om, at der er tale om svindel. Ordningen medfører en kortvarig suspendering af adgang til pengene hos modtageren. Formålet er at begrænse tiden og muligheden for, at svindlede beløb kan blive ført videre til andre konti. Dette vil samtidig øge sandsynligheden for, at svindlede beløb kommer tilbage til offeret.

Svindel Task Forcen anbefaler, at en dansk ordning bliver implementeret snarest muligt. Implementeringen bør ikke afvente den EU-regulering, der er på vej. Anbefalingen kræver derfor,

at der bliver etableret en særskilt dansk regulering, indtil EU-reguleringen er på plads, samt at alle danske banker dernæst implementerer fastfrysningsordningen.

Svindel Task Forcen anbefaler, at en fastfrysningsordning på sigt udvides til også at omfatte banker uden for Danmark.

Anbefalingen vil betyde, at fastfrosne svindlede beløb ikke uden videre kan blive videreført til andre konti. Det vil begrænse kundernes tab, gøre det vanskeligere for de kriminelle og begrænse de kriminelles fortjeneste.

10. Otte sikkerhedstiltag i bankerne

Svindelsituation

De kriminelle udnytter, at danske bankkunder i høj grad benytter sig af selvbetjening. De mange muligheder giver de kriminelle let adgang til at svindle, hvis de kan overtale bankkunderne og lokke dem til på egen hånd at overføre penge, ændre beløbsgrænser, optage lån mv.

Anbefaling

Svindel Task Forcen anbefaler, at bankerne styrker sikkerheden i bankernes kundevendte systemer. Konkret anbefaler Task Forcen at fokusere på otte tiltag:

1. Yderligere styrkelse af bankernes tekniske anti-svindel systemer
2. Tilpasning af onlinekanaler med henblik på bekæmpelse af svindel
3. Karenstid og tidsbegrænsning
4. Forstærket godkendelse
5. Kundetilpasset funktionalitet på betalingskort, f.eks. blokering af betalinger i specifikke geografiske områder
6. Implementering af beskyttelse af opkald og sms'er
7. Advarsler til kunden ved mistænkelige aktiviteter
8. Tydelig og relevant information til kunden ifm. alle transaktioner.

De enkelte bankers løsninger til bekæmpelse af svindel er forskellige, og flere af bankerne har allerede taget hul på flere af tiltagene.

Anbefalingen bør blive implementeret med mindst mulig brug af kundedata for at beskytte kundens privatliv. Af sikkerhedsmæssige årsager har Svindel Task Forcen valgt ikke at offentliggøre tiltagene detaljeret.

Anbefalingen vil medføre en bedre beskyttelse af kunderne og vil kunne stoppe flere svindelforsøg.

11. Bekræftelse af modtager ved kontooverførsler

Svindelsituation

De kriminelle bilder ofrene ind, at de trygt kan overføre penge til en sikker konto hos f.eks. politiet. Det er i dag ikke muligt for en bankkunde at vide, at den, der modtager pengene, også er den, man ønsker at sende pengene til. Det er alene navnet på den modtagende bank, der fremgår ved konto til konto overførsler.

Anbefaling

Svindel Task Forcen anbefaler, at bankerne tilbyder deres kunder at få tjekket, om der er overensstemmelse mellem navn på den forventede modtager og kontonummerets ejer. Konkret betyder det, at når bankkunder opretter en betaling, så får kunden at vide, om der er et match mellem det navn og kontonummer, som kunden oplyser, og de oplysninger, som den modtagende bank har registeret om modtageren.

Kunden vil kun få at vide, om der enten er et match, ikke er et match eller der er et "måske match". Et eksempel på "måske match" kunne være en stavefejl i modtagernavnet.

Løsningen skal overholde gældende databeskyttelsesregler og minimere omfanget af data, der bliver delt.

Ordningen kræver, at der bliver etableret en lovhjemmel til at foretage det tjek, der kan afgøre, om der er et match. EU-lovgivning, som skal etablere en hjemmel, er i øjeblikket i gang med at blive forhandlet.

Svindel Task Forcen anbefaler, at ordningen på sigt udvides med, at kunder generelt - automatisk og uden navnetjek - kan få oplyst navnet på den virksomhed, som kunden ønsker at overføre penge til. Altså på samme måde, som det i dag gælder, når man betaler regninger på baggrund af et indbetalingskort.

Anbefalingen vil give kunderne bedre mulighed for at tjekke, hvem de sender penge til.

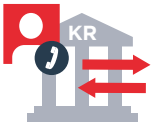
12. Deling af data til brug for bankernes risikovurderinger af svindel

Svindelsituation

Ofre bliver ringet op af svindlere, som forsøger at overtale dem til at overføre penge eller udlevere personlige oplysninger. Teleselskaberne har data som f.eks. abonnementsdata og opkaldsdata, som bankerne – hvis de havde adgang til dem - vil kunne nyttiggøre til at opdage og forhindre svindlernes aktiviteter.

Anbefaling

Svindel Task Forcen anbefaler, at det bliver muligt at dele data fra teleselskaberne til bankerne, som kan gøre brug af data til at øge sikkerheden ved pengeoverførsler og betalingstransaktioner. Konkret drejer det sig om teledata, bankerne kan bruge til at identificere og vurdere risiko for svindel, så svindelforsøg kan blive stoppet i tide.



Det kan være data om, hvorvidt en kunde er i et aktivt opkald. I mange svindelsager fastholder den kriminelle offeret i en længerevarende

telefonsamtale, samtidig med at transaktioner bliver foretaget.

Et andet eksempel kunne være data om, hvorvidt der for nylig er foretaget en omskiftning af kundens simkort (sim-swap). Dette kan være en indikator på, at en svindler har overtaget ofrets identitet og har fået teleudbyderen til at overføre offerets nummer til svindleren.

Potentielt kan disse data anvendes af bankerne i forbindelse med en samlet risikovurdering ved en pengeoverførsel og kan f.eks. udløse, at betalingen bliver stoppet af banken.

Anbefalingen indebærer, at teleselskaberne og bankerne skal etablere løsninger, som kan udveksle og behandle data, så de kan anvendes til svindelbekæmpelse.

Kan løsningen ikke etableres inden for den eksisterende lovgivning, er det Task Forcens anbefaling, at der bliver etableret en særskilt hjemmel.

Anbefalingen vil gøre det muligt at stoppe flere svindelforsøg.

13. Bedre phishing beskyttelse i MitID

Svindelsituation

Ofre for digital svindel bliver fortsat ofte udsat for phishing, hvor svindlere forsøger at snyde sig til oplysninger. Det kan f.eks. være via et link, hvor der bliver bedt om et kodeord, betalingskortoplysninger eller oplysninger om MitID. Med MitID-phishing forsøger svindlerne at få offeret til at godkende en MitID-transaktion, der er igangsat af svindleren.

Anbefaling

Svindel Task Forcen anbefaler, at man i MitID går videre med udviklingen af den såkaldte FIDO-teknologi (Fast Identity Online), som kan give en mere effektiv beskyttelse mod den type af svindel, hvor ofre godkender MitID-transaktioner, som svindleren har startet.

Når brugeren gennemfører en transaktion, tjekker MitID for, om MitID-transaktionen er startet af den samme bruger, som nu godkender transaktionen. Det kan forhindre, at man ikke kommer til at godkende en MitID-transaktion, som er igangsat af en svindler.

Anbefalingen kræver etablering af en ny FIDO-funktionalitet i MitID. Løsningen kan dog også give udfordringer for brugeren, da den nye funktionalitet kan kræve en mere besværlig MitID-godkendelsesproces for brugeren end den nuværende løsning.

Svindel Task Forcen anbefaler desuden, at de tekster, som MitID-brugere bliver præsenteret for, når de godkender en MitID-transaktion, bliver forbedret, så de giver en klar beskrivelse af, hvad der er ved at blive godkendt. Det er afgørende, at brugerne er vant til at se præcise beskrivelser, da dette skaber tillid, og gør det lettere at spotte mistænkelige transaktioner.

Etablering af FIDO-funktionalitet i MitID vil give en bedre beskyttelse mod MitID-phishing.

Efter-fasen: Anbefaling 14-18

Når svindleren har haft held til at overtale offeret til at overføre oplysninger eller penge, er der flere hensyn at tage. I denne fase skal der tages hånd om ofrene, hvor svindlen kan have store økonomiske og personlige konsekvenser. De kriminelle skal retsforfølges. Og vi skal alle lære af erfaringerne.

I dag bliver en del af de anmeldelser, som politiet modtager om digital svindel, henlagt. Det øger risikoen for, at visse svindlere kan fortsætte deres aktiviteter, og det gør det mere attraktivt for nye svindlere at gå i gang. Derfor ønsker Svindel Task Forcen at styrke efterforskning og samarbejde mellem alle parter på området.

14. Flere ressourcer til politiets efterforskning af digital svindel

Svindelsituation

Ofre for digital svindel oplever ofte, at de kriminelle ikke bliver stillet til ansvar. Der er ikke tilstrækkeligt med ressourcer til at gennemføre efterforskningen i alle tilfælde. Det kan betyde, at de ansvarlige for økonomisk kriminalitet ustraffet kan fortsætte deres aktiviteter. Alene fra 2022 til 2023 oplevede politiet en stigning på 30 procent i antallet af anmeldelser om svindel.

Anbefaling

Svindel Task Forcen anbefaler, at politiets indsats mod it-relateret økonomisk kriminalitet bliver politisk styrket og tildelt flere midler end i dag. Man bør i bevillingen til politiet tage udgangspunkt i stigningen af antal anmeldelser til politiet og lade den udvikling afspejle sig i bevillingen. Flere ressourcer hos politiet vil forventeligt styrke efterforskningskompetencerne og muligheden for at forfølge flere sager, hvilket vil føre til færre henlæggelser og flere retsforfølgelser.

Det har været en succes, at den indledende efterforskning er blevet samlet hos National Center for it-kriminalitet, hvorefter sagerne bliver videreformidlet til de enkelte politikredse. Derfor skal der ses på, hvordan der kan blive bygget videre på dette, så hele efterforskningskæden for svindel bliver styrket, og sagerne bliver håndteret af specialister med den nødvendige ekspertise.

En styrket efterforskning vil øge sandsynligheden for at fange flere kriminelle, reducere antallet af henlagte sager og øge retsbevidstheden.

15. Styrket samarbejde og udveksling af data mellem banker og politi

Svindelsituation

Samarbejdet mellem banker og politi er afgørende for at fange de kriminelle. De eksisterende processer, herunder udveksling af data, skal derfor styrkes. Det er afgørende med en effektiv efterforskning for at øge sandsynligheden for at stoppe de kriminelle.

Anbefaling

Svindel Task Forcen anbefaler, at der bliver nedsat en arbejdsgruppe med deltagelse af banker og politi, der sammen skal udvikle en mere effektiv og systematisk proces for dataudveksling. Arbejdsgruppen skal fokusere på følgende problemstillinger:

- Bankernes rolle i anmeldelsen af digital svindel.
- Udvekslingen af data fra banker til politi ved anmeldelse og efterforskning af sager.

- Sikring og udveksling af videomateriale til brug for efterforskning, f.eks. fra hæveautomater, hvor svindlere anvender ofres betalingskort. I dag risikerer videomaterialet at blive slettet, inden efterforskningens opstart.
- Beredskab hos bankerne ved hastende efterforskningsaktiviteter.

Alt efter arbejdsgruppens konklusioner kan der være brug for at foretage investeringer i dataudvekslingen, evt. et nyt it-system for udveksling og behandling af data i politiet og bankerne.

En bedre anmeldelsesproces og udveksling af data vil kunne forbedre politiets muligheder for at efterforske svindel og bankernes mulighed for at bidrage til det.

16. Støtte og vejledning til ofre og pårørende

Svindelsituation

Digital svindel har store omkostninger, og de er ikke kun økonomiske. Ofre for digital svindel er tvunget til at håndtere konsekvenser af den kriminalitet, de har været udsat for. For nogle er konsekvenserne meget alvorlige, og det kan være en stor psykisk belastning. Det kan være svært at finde rundt i de tilbud om hjælp, der er. Pårørende kan også have svært ved at hjælpe i de situationer, som ofrene ofte oplever som skamfulde. Desuden kan det være svært for bankrådgivere at tale med manipulerede ofre, som befinder sig i vildfarelse og måske ikke kan eller vil indse, at de er udsat for svindel.

Anbefaling

Svindel Task Forcen anbefaler, at bankerne i deres hjælp til kunder, som udsættes for digital svindel, systematisk henviser til to specialiserede tjenester, der rådgiver ofre – den statslige Cyberhotline for digital sikkerhed og den uafhængige Offerrådgivning.

Det samlede samarbejde mellem tilbuddene kan blive styrket gennem bedre oplysning mellem parterne, så det bliver lettere at finde

rundt i tilbuddene. Banker, borgerservice mv. skal være tydelige med henvisning. Det er væsentligt, at rådgivningens tilbud bliver synlige og kendte af alle de involverede parter på området.

Der findes også andre initiativer på området, og de kan med fordel også bistå ofrene med rådgivning, f.eks. i samarbejde med de to tjenester – Cyberhotline og Offerrådgivningen.

Svindel Task Forcen anbefaler samtidig, at det sikres, at Offerrådgivningen har de nødvendige driftsmidler til at styrke offerrådgivningen.

Svindel Task Forcen anbefaler endeligt, at bankerne sikrer, at de bankansatte er rustet til de svære samtaler med de svindelramte kunder. Bankerne skal sørge for at øge medarbejderes bevidsthed og kompetencer vedrørende digitale trusler og have uddannelsesprogrammer om risici og tendenser i forbindelse med svindel for deres ansatte.

Anbefalingen vil kunne give en mere fokuseret rådgivning af ofre og pårørende.

Offerrådgivningen

Offerrådgivningen er en uafhængig organisation, der har afdelinger i alle politikredse. De tilbyder anonym og gratis støtte til ofre, vidner og pårørende til kriminalitet og ulykker. De arbejder tæt sammen med politiet, som henviser ofre til dem. Offerrådgivningen giver ofre rådgivning på tværs af forbrydelseskategorier, f.eks. som et ekstra tilbud, hvis ofre fortsat er meget utrygge og har brug for yderligere hjælp.

Cyberhotline

Cyberhotline er en offentlig hotline, som er udviklet under den nationale strategi for cyber- og informationssikkerhed. Cyberhotline hjælper borgere og virksomheder med at blive mere digitalt sikre samt håndtere og forebygge digital svindel.

De tilbyder vejledning om beskyttelse mod cyberkriminalitet og hjælp ved identitetstyveri.

17. Bedre deling af data mellem aktører ved svindelbekæmpelse

Svindelsituation

De kriminelle kan i dag gennemføre deres svindel med udgangspunkt i én bank, uden at denne bank kan dele sin viden med andre banker. Det skyldes, at bankerne lovgivningsmæssigt er underlagt strenge begrænsninger for, hvad man må dele mellem banker. Det betyder f.eks. også, at en svindler kan skifte fra en bank til en anden, uden at den nye bank bliver informeret af den tidligere bank om svindelmistanken.

Anbefaling

Svindel Task Forcen anbefaler at styrke og forbedre videndelingen, så der er mulighed for hurtigere og bedre spredning af viden om igangværende svindeltyper, kriminelle mv. Når data i dag ikke bliver delt, er det til de kriminelles fordel. Svindel Task Forcen anbefaler:

- at der bliver etableret en hjemmel til banker om deling af indikatorer for svindel mellem banker. Konkret drejer det sig særligt om at dele mere data om svindlen og svindleren – f.eks. identitet, dato om hændelsen samt oplysninger om browser, terminal, geolokation mm. Det er vigtigt, at der bliver taget højde for, at indikatorer kan ændre sig over tid på grund af nye metoder og teknologi. Det er væsentligt ikke at dele "falske positiver", så en kunde ikke uretmæssigt "stemples" som svindler.
- at der bliver etableret yderligere online deling via Nordic Financial CERT til teleselskaber. Det kan f.eks. være deling af telefonnumre eller profiler, som bliver brugt til svindel (f.eks. "fake support"-numre osv. fra smishing), at der bliver delt kendte phishing-URL'er, så teleselskaberne kan blokere dem m.m. Delingen bør ske via maskine til maskine kommunikation, så informationen flyder hurtigt.

Videndelingen skal ske via Nordic Financial CERT, der har etableret en sikker platform til deling af viden. Her kan man dele informationer online i et lukket system, så alle aktører har kendskab til aktuelle svindeltyper og kriminelle metoder.

Det er en anbefaling, at kun nødvendige data bliver delt, og at der bliver implementeret sikkerhedsforanstaltninger for at forhindre misbrug af personfølsom data.

Med bedre videndeling vil de kriminelle kunne stoppes tidligere. Anbefalingen vil desuden have en positiv effekt på bekæmpelsen af muldyr, da viden om deres ageren fremover vil kunne deles i større grad, end hvad tilfældet er i dag.

18. Strategisk, operationelt og teknisk forum for svindelforebyggelse

Svindelsituation

Svindlen udvikler sig konstant, og derfor er bekæmpelse af svindel en meget dynamisk opgave, som kræver, at der løbende bliver udviklet nye tiltag til at forebygge svindel. FIT, ODIN[9] og NFCERT er eksempler på velfungerende etablerede samarbejdsfora, men der ses fortsat et behov for yderligere at styrke samarbejdet på hhv. det strategiske, operationelle og tekniske niveau.

Anbefaling

Svindel Task Forcen anbefaler, at der bliver etableret en stærkere samarbejdsstruktur, hvor der løbende kan blive udviklet nye redskaber i svindelbekæmpelsen, delt aktuelle trusler og trends for svindel m.m. Task Forcen anbefaler, at der bliver etableret en struktur på området for svindelbekæmpelse, som baserer sig på følgende tre niveauer og i videst muligt omfang tager hensyn til eksisterende fora og forsøger at indplacere disse på de forskellige niveauer:

1. Strategisk forum

Svindel Task Forcen anbefaler et nyt strategisk stående offentlig/privat samarbejdsforum, hvor de vigtigste dagsordener og aktuelle svindeltendenser bliver drøftet. Sekretariatsfunktionen kan med fordel varetages af relevante myndigheder. Det er vigtigt at sikre en forankring øverst i de berørte organisationer og myndigheder, hvor udfordringer og potentielle løsninger kan eskaleres til. Det kan være på samme strategiske niveau som det offentlig-private samarbejdsforum FSOR, som arbejder med at styrke operationel robusthed i finanssektoren, og hvor samarbejdet er frivilligt, men forpligtende. Deltagerkredsen kan være myndigheder, politi, banker, Teleindustrien og andre relevante aktører.

2. Operationelt forum

Profiler med ansvar for svindelbekæmpelsen i de berørte organisationer deltager og drøfter aktuelle svindel trends, kriminalitetsmønstre, modreaktioner og koordination af aktiviteter. Den deling foregår i dag mellem de nordiske banker på ugentlig basis i regi af Nordic Financial CERT, ligesom der hver anden uge er et dansk møde, hvor politiet også deltager. Dette behov for et operationelt forum kan fortsat være løftet ind i Nordic Financial CERT-regi. Svindel Task Forcen anbefaler, at politiet og telesektoren også er tilknyttet møderne.

3. Teknisk-forum

Efterforskere og fagspecialister fra de berørte organisationer udveksler aktuelle efterforskninger, mistanker, dag-til-dag udviklinger i den digitale svindel mv. Sagsfokuserede og efterforskningsdrevne drøftelser, som ligner det eksisterende ODIN-samarbejde, der er etableret på hvidvask-området. Behovet for et teknisk forum kan blive løftet ind i ODIN-samarbejdet, hvor digital svindel – evt. med en nærmere afgrænsning – fremover kan indgå. Det kan kræve, at området tilføres yderligere ressourcer.

[9] www.politi.dk/om-politiet/samarbejde/odin

Det anbefales, at kun nødvendige data deles, og at der bliver implementeret passende sikkerhedsforanstaltninger for at forhindre misbrug af personfølsom data.

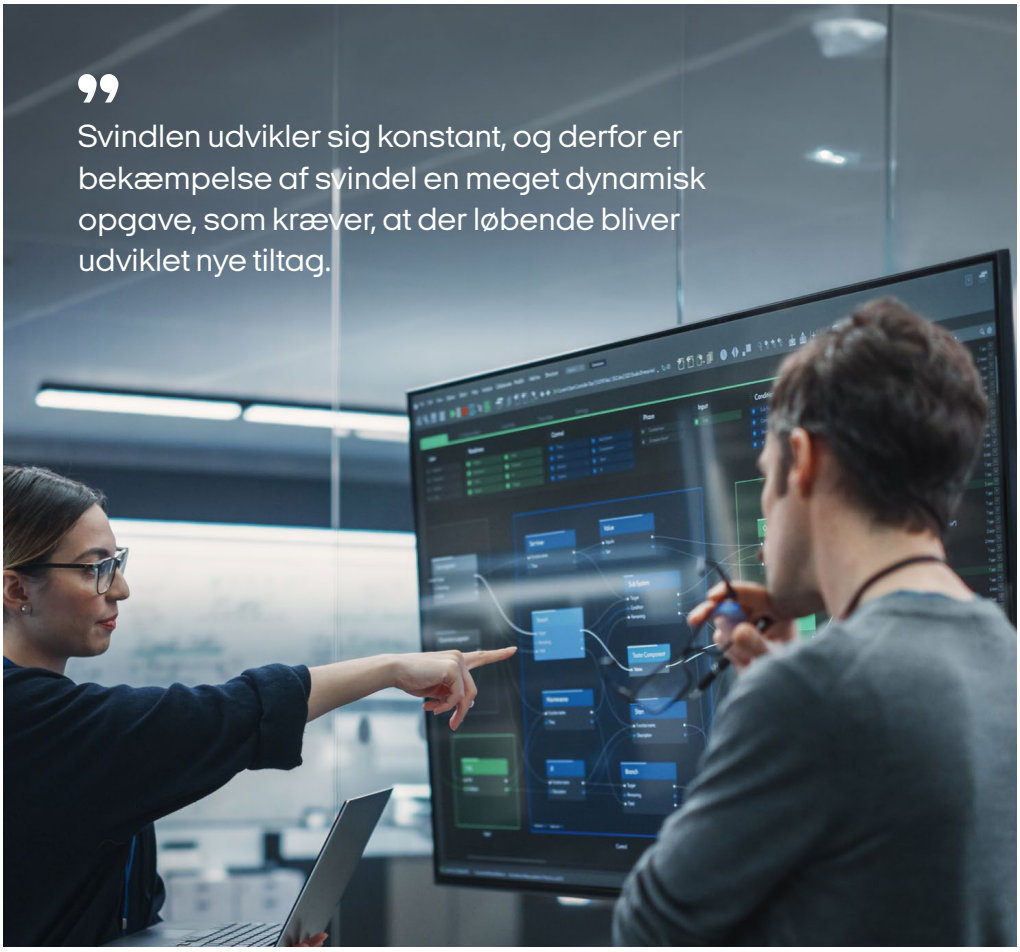
Med anbefalingen bliver der etableret et nyt strategisk forum for svindelbekæmpelse, som f.eks. kan komme i stand i forbindelse med en kommende ny national strategi for cyber- og informationssikkerhed. For de to øvrige niveauer af samarbejde kan man med fordel tilpasse eksisterende fora.

Der skal være en tæt sammenhæng imellem de tre fora, så det sikres, at udfordringer, problemstillinger og løsninger kan blive adresseret fra taktisk til strategisk niveau.

Etablering eller udbygning af samarbejder eller fora skal ske med fokus på optimal ressourceanvendelse og i koordinering med eksisterende tiltag på området for hvidvask, terrorfinansiering og anden økonomisk kriminalitet.

I forbindelse med det strategiske arbejde på området bør der også være fokus på at sikre ny forskning på området.

Særligt etablering af et formelt strategisk forum vil sikre en bedre koordinering og vil kunne styrke svindelforebyggelsen betydeligt.



Oversigt over alle 18 anbefalinger

Før-fasen

1. Bedre blokering af svindelhjemmesider
2. Sms-spamfilter mod svindel sms'er
3. Bedre beskyttelse af fastnet- og mobilnumre mod spoofing
4. Obligatorisk registrering af taletidskort
5. Nordic Financial CERT som "Trusted Flagger"
6. Krav om to-trins godkendelse på sociale medier
7. Digital svindel på skoleskemaet
8. Oplysningsindsats fra bankerne om svindel

Under-fasen

9. Fastfrysningsordning ved svindelmistanke
10. Otte sikkerhedstiltag i bankerne
11. Bekræftelse af modtager ved kontooverførsler
12. Deling af data til brug for bankernes risikovurderinger af svindel
13. Bedre phishing beskyttelse i MitID

Efter-fasen

14. Flere ressourcer til politiets efterforskning af digital svindel
15. Styrket samarbejde og udveksling af data mellem banker og politi
16. Støtte og vejledning til ofre og pårørende
17. Bedre deling af data mellem aktører ved svindelbekæmpelse
18. Strategisk, operationelt og teknisk forum for svindelforebyggelse

FAKTAARK

Svindel Task Forcens 18 anbefalinger

Før-fasen: Anbefaling 1-8

1. Bedre blokering af svindelhjemmesider

Svindel Task Forcen anbefaler, at der hos alle teleselskaber bliver etableret en supplerende beskyttelse af kunderne baseret på DNS-blokering af skadelige hjemmesider.

2. Sms-spamfilter mod svindel sms'er

Svindel Task Forcen anbefaler, at der bliver etableret et sms-spamfilter hos mobilselskaberne. En sms-spamfilter fungerer omtrent som et e-mail spam filter.

3. Bedre beskyttelse af fastnet- og mobilnumre mod spoofing

Svindel Task Forcen anbefaler at udvide den eksisterende spoofingbeskyttelse til at omfatte fastnet- og mobilnumre. Anbefalingen vil forhindre flere fupopkald.

4. Obligatorisk registrering af taletidskort

Svindel Task Forcen anbefaler, at der bliver indført obligatorisk registrering af navn og CPR-nummer ved køb af taletidskort. Anbefalingen vil gøre det sværere for kriminelle at bruge uregistrerede taletidskort.

5. Nordic Financial CERT som "Trusted Flagger"

Svindel Task Forcen anbefaler, at der bliver oprettet en "trusted flagger"-funktion på svindelområdet i forhold til relevante sociale medier. Med anbefalingen får bankerne en direkte kanal til indrapportering af skadeligt indhold og skadelige profiler hos sociale medieplatforme. Det vil hurtigere fjerne skadeligt indhold.

6. Krav om to-trins godkendelse på sociale medier

Svindel Task Forcen anbefaler, at det bliver obligatorisk for sociale medier at implementere to-trins godkendelse for deres brugere. Anbefalingen vil gøre det sværere at misbruge en andens profil på de sociale medier.

7. Digital svindel på skoleskemaet

Svindel Task Forcen anbefaler, at folkeskolens nye fag, teknologiforståelse, skal være obligatorisk. Det vil både skærpe unges kendskab og modstandsdygtighed overfor digital svindel.

8. Oplysningsindsats fra bankerne om svindel

Svindel Task Forcen anbefaler, at bankerne løbende gennemfører oplysningskampagner om svindel. En målrettet oplysningskommunikationsindsats vil kunne bidrage til en bedre forebyggelse af svindel.

Under-fasen: Anbefaling 9-13

9. Fastfrysningsordning ved svindelmistanke

Svindel Task Forcen anbefaler, at bankerne etablerer en fastfrysningsordning ved mistanke om digital svindel ved overførte penge. Anbefalingen vil sikre, at flere mistænkelige transaktioner bliver stoppet.

10. Otte sikkerhedstiltag i bankerne

Svindel Task Forcen anbefaler, at bankerne styrker sikkerheden i bankernes kundevendte systemer. Konkret anbefales otte tiltag:

1. Yderligere styrkelse af bankernes tekniske anti-svindel systemer
2. Tilpasning af onlinekanaler med henblik på bekæmpelse af svindel
3. Karenstid og tidsbegrænsning
4. Forstærket godkendelse
5. Kundetilpasset funktionalitet på betalingskort, f.eks. blokering af betalinger i specifikke geografiske områder
6. Implementering af beskyttelse af opkald og sms'er
7. Advarsler til kunden ved mistænkelige aktiviteter
8. Tydelig og relevant information til kunden ifm. alle transaktioner.

Af sikkerhedsmæssige årsager bliver anbefalingerne ikke offentliggjort detaljeret. Anbefalingerne vil styrke sikkerheden i bankernes systemer yderligere.

11. Bekræftelse af modtager ved kontooverførsler

Svindel Task Forcen anbefaler, at bankerne tilbyder kunderne at få tjekket, om der er overensstemmelse mellem navn på den forventede modtager og kontonummerets ejer. Forslaget vil reducere risikoen for at overføre penge til svindlere og reducere risikoen for fejlagtige betalinger generelt.

12. Deling af data til brug for bankernes risikovurderinger af svindel

Svindel Task Forcen anbefaler, at det bliver muligt at dele data mellem teleselskaberne og bankerne, som kan gøre brug af disse data til at øge sikkerheden ved pengeoverførsler og betalingstransaktioner.

13. Bedre phishing beskyttelse i MitID

Svindel Task Forcen anbefaler, at man i MitID går videre med udviklingen af den såkaldte FIDO-teknologi (Fast Identity Online), som kan give en mere effektiv beskyttelse mod den type af svindel, hvor ofre godkender MitID-transaktioner. Anbefalingen vil give bedre beskyttelse mod MitID phishing.

Efter-fasen: Anbefaling 14-18

14. Flere ressourcer til politiets efterforskning af digital svindel

Svindel Task Forcen anbefaler, at politiets indsats mod it-relateret økonomisk kriminalitet bliver styrket og tildelt flere midler end i dag.

15. Styrket samarbejde og udveksling af data mellem banker og politi

Svindel Task Forcen anbefaler, at der bliver nedsat en arbejdsgruppe med deltagelse af banker og politi, der sammen skal udvikle en mere effektiv og systematisk proces for dataudveksling.

16. Støtte og vejledning til ofre og pårørende

Svindel Task Forcen anbefaler, at bankerne systematisk henviser til to specialiserede tjenester, der rådgiver ofre – den statslige Cyberhotline og den uafhængige Offerrådgivning. Svindel Task Forcen anbefaler samtidig, at det sikres, at de to tjenester har de nødvendige ressourcer til at kunne varetage opgaven.

17. Bedre deling af data mellem aktører ved svindelbekæmpelse

Svindel Task Forcen anbefaler at styrke og forbedre videndelingen, så der er mulighed for hurtigere og bedre spredning af viden om igangværende svindeltyper, kriminelle mv. mellem alle aktører. Det skal ske ved, at der etableres en hjemmel til banker om deling af informationer om konkrete svindelsager, herunder oplysninger om svindleren, samt at datadelingen styrkes via Nordic Financial CERT.

18. Strategisk, operationelt og teknisk forum for svindelforebyggelse

Svindel Task Forcen anbefaler, at der bliver etableret en styrket samarbejdsstruktur på området for svindelbekæmpelse, som baserer sig på tre niveauer: Strategisk forum, Operationelt forum og Teknisk forum. Det vil sikre en bedre koordinering og kunne styrke svindelforebyggelsen betydeligt.

FINANS
DANMARK

Finans Danmark
Amaliegade 7 · 1256 København K
Tlf. 33 70 10 00 · www.finansdanmark.dk