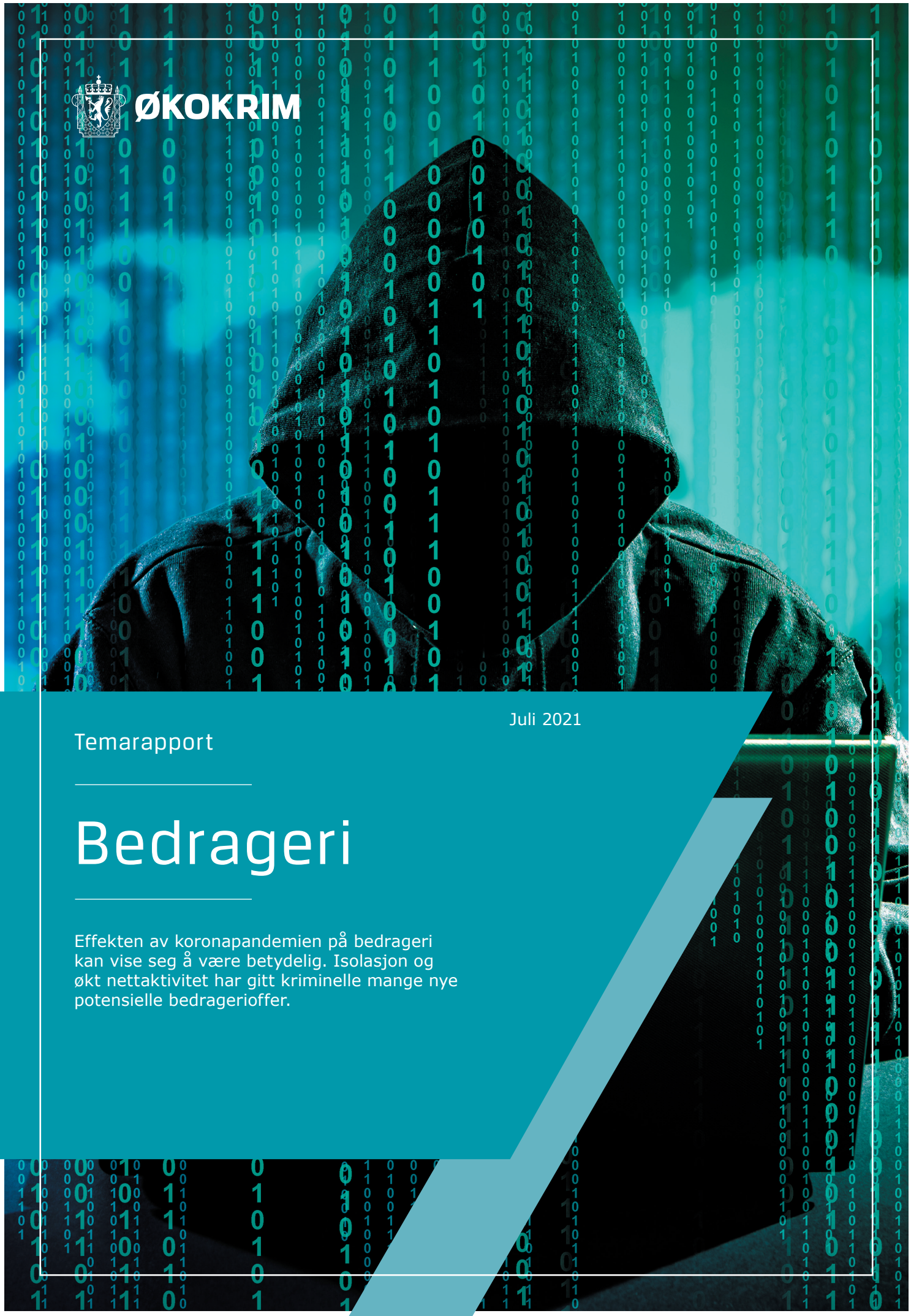


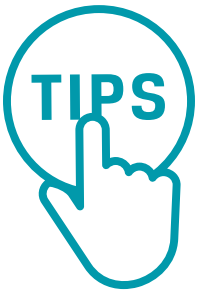
ØKOKRIM

Juli 2021

Temarapport

Bedrageri

Effekten av koronapandemien på bedrageri kan vise seg å være betydelig. Isolasjon og økt nettaktivitet har gitt kriminelle mange nye potensielle bedragerioffer.



Har du informasjon om noen som begår bedrageri? Varsle oss på www.okokrim.no/tips

Økokrim
Postboks 2096 Vika, 0125 Oslo
Telefon: 23 29 10 00
E-post: post.okokrim@politiet.no

Innhold

Innledning

Privatpersoner og bedrifter utsettes for en lang rekke bedragerier med ulike modus og grensesnitt. I denne rapporten forsøker vi å kartlegge omfanget for flere av disse og vurdere trusselen de utgjør fremover.

Vurderingene i rapporten er gjort av Økokrim basert på den tilgjengelige informasjonen og har som hensikt å gi beslutningstakere kunnskapsgrunnlag for å prioritere innsats mot ulike typer bedrageri-modus.

Sannsynlighetsord
Vurderinger vil alltid inneholde en grad av usikkerhet. For å håndtere dette på en standardisert og strukturert måte, er det benyttet sannsynlighetsord (se tabell). Sannsynlighetsordene står i kursiv.

Nasjonal standard	Beskrivelse	NATO standard
Meget sannsynlig	Det er meget god grunn til å forvente	Highly likely (〉90%)
Sannsynlig	Det er grunn til å forvente…	Likely (60-90%)
Mulig	Det er like sannsynlig som usannsynlig…	Even chance (40-60%)
Lite sannsynlig	Det er liten grunn til å forvente…	Unlikely (10-40%)
Svært lite sannsynlig	Det er svært liten grunn til å forvente…	Highly unlikely 〈10%

Hovedpunkter

- Sosial manipulering og identitetstyveri er en bakenforliggende faktor i flere av de ulike formene for bedrageri. Det menneskelige elementet er, og vil alltid være, sårbart for manipulering.
- Forebyggende arbeid og tekniske/fysiske sikkerhetstiltak anses å gi en betydelig gevinst i arbeidet med å hindre bedrageri av privatpersoner.
- Myndighetenes tiltak for å begrense smitten av koronaviruset har medført at mange har vært mer alene enn ellers. Dette antas å ha påvirket enkelte bedrageriformer, slik som investering- og kjærlighetsbedrageri, i negativ retning.
- Det er meget sannsynlig at bedrageri mot privatpersoner vil bli et større problem i årene fremover. Koronapandemien antas å ha fungert som en katalysator for dette da den har akselerert digitaliseringen av samfunnet. Investeringsbedrageri anses å være den mest alvorlige bedrageriformen mot privatpersoner.
- Direktør- og fakturabedrageri anses å være den mest alvorlige bedrageriformen mot næringslivet.
- Det varierer imellom de ulike bedrageriformene om bedragerne er norske eller utenlandske. Ved fakturabedrageri mot foretak er det nordmenn som står bak en del falske fakturaer som er tilpasset norske forhold, mens det er aktører i utlandet som ofte står bak massebedrageriene eller de svært sofistikerte modusene. Ved kreditt- og lånebedrageri samt forsikringsbedrageri virker de kriminelle å være utelukkende nordmenn eller personer som befinner seg i Norge.
- Ved bedrageri mot privatpersoner virker det i hovedsak å være organiserte kriminelle grupperinger i utlandet som står bak. De bruker gjerne ofrene som pengemuldyr i tillegg til å bedra dem. Dette er spesielt aktuelt innenfor kjærlighetsbedrageri. I den grad nordmenn står bak bedragerier mot privatpersoner så er det som oftest ved pyramidespill eller ved nettbankbedrageri hvor det at offeret snakker med noen som er norsktalende kan være overbevisende nok til at de gir fra seg bankopplysninger.
- Investeringsbedrageri vil trolig forbli den største trusselen i sommer. I mange tilfeller blir folk bedratt når de har fri.

Status bedrageri i Norge

Bedragerisaker utgjør en stor andel av den anmeldte kriminaliteten. DNB opplevde en økning i antall bedragerier på nesten 25 prosent i 2020, sammenlignet med 2019.[1] Telenor har på sin side uttalt at de stanser 200 000 bedrageriforsøk via telefon daglig.[2]

Sosial manipulering, herunder phishing (via e-post), vishing (via telefon oppringning), smishing (via SMS) og pharming (via falsk nettside), er ofte en sentral del av bedrageriet. Kort forklart handler dette om å utgi seg for å være noen andre enn den man egentlig er. I en undersøkelse utført av Næringslivets Sikkerhetsråd svarte 13 prosent av virksomhetene at de var utsatt for phishing eller andre former for sosial manipulering i 2019.[3] Målrettede angrep benytter i økende grad informasjon om offeret for å virke mer overbevisende.[4]

Finanstilsynets Risiko- og sårbarhetsanalyse for 2020 estimerer de totale tapene forbundet med sosial manipulering i Norge å være 295 millioner kroner. Dette er en betydelig nedgang fra 2019 hvor tallet var 500 millioner kroner. De faktiske tapene antas allikevel å være vesentlig større da ikke alle bedragerisaker blir meldt til banken.[5] Omfanget er også usikkert da mange aldri innser at de har blitt bedratt, eller at skamfølelsen over å ha latt seg utnytte er såpass stor at de ikke anmelder saken. Et bedragerioffer som er manipulert kan også utnyttes av de kriminelle til andre formål, eksempelvis som pengemuldyr.

DNB rapporter at de så en betydelig økning i målrettede angrep mot bedrifter som spesielt bruker phishing og smishing i angrepet i 2020. Totalt beløp forsøkt stjålet økte med 230 prosent, og antallet offer økte med 176 prosent til totalt 460 kunder som ble bedratt 651 ganger.[6] EUROPOL forventer at kriminelle vil øke bruken av kunstig intelligens og såkalt deepfakes i årene fremover. Ved å implementere kunstig intelligens i eksisterende modus kan angrepene mot næringslivet skaleres opp betraktelig.[7] Videre kan kunstig intelligens medføre at oversettelser blir bedre slik at svindel e-post virker mer overbevisende. NorSIS rapporter også at de kriminelle har begynt å dreie angrepene mot de ansatte fremfor IT-systemene.[8]

Effekten av koronapandemien på bedrageri kan vise seg å være betydelig. Isolasjon og økt nettaktivitet har gitt kriminelle mange nye potensielle bedragerioffer. Falske nettbutikker som lokker til seg offer med svært lave priser har vært en effektiv metode for kortbedrageri tidligere. Dette forventes å bli et økende problem fremover. En betydelig andel av registrerte kortbedrageri er relatert til misbruk av kortinformasjon via netthandel.

1 DNB v/FC3, «Annual Fraud Report 2020», 2021.
2 Aftenposten, «Telenor stopper 200.000 telefonsvindelforsøk daglig», 2020.
3 Næringslivets Sikkerhetsråd, «Mørketallsundersøkelsen 2020», 2020:18-19.
4 NorSIS, «Trusler og trender 2019-2020», 2020:19.
5 Finanstilsynet, «Risiko og sårbarhetsanalyse (ROS) 2020», 2021:36.
6 DNB v/FC3, «Annual Fraud Report 2020», 2021.
7 EUROPOL, «Serious and organised crime threat assessment», 2021:40.
8 NorSIS, «Trusler og trender 2021», 2021:25.

Bedrageri av næringslivet

Direktørbedrageri

Ved direktørbedrageri analyserer bedragere virksomhetens interne organisasjon og går direkte på medarbeidere for eksempelvis å få de til å overføre/godkjenne utbetalinger. Typisk utgir bedrageren seg ut for å være en leder og henvender seg til en økonomiarbeider for å få overført en større sum penger til utlandet.[9] Gjerningsmennenes oppfinnsomhet er stor og endringsviljen enda større.

I 2019 utgjorde kjente tap fra direktørbedrageri i Norge 188 millioner kroner.[10] DNB kunne også rapportere at antallet forsøk på direktørbedrageri mot deres kunder forble omtrent uendret i 2020 (146 mot 149 i 2019). Derimot økte tapet knyttet til direktørbedrageri med 15 prosent, til 129 millioner kroner.[11]

I følge Næringslivets sikkerhetsråd har 13 prosent av norske virksomheter i løpet av en ett-års periode blitt utsatt for forsøk og/eller suksessfulle direktørbedrageri. Her er det derimot stor forskjell avhengig av virksomhetens størrelse. Kun 6 prosent av mindre virksomheter har vært utsatt for dette, mens for virksomheter med mer enn 100 ansatte ble 27 prosent utsatt for direktørbedrageri. Ser man kun på privat sektor ble over halvparten av virksomhetene utsatt for direktørbedrageri.[12]

Det har også blitt observert en interessant modus hvor bedragerne går etter ledere og styremedlemmer i bedriften med antatt tilgang til bedriftskonto. Bedragerne utgir seg for å være fra BankID. Først mottar offeret en SMS fra «BankID». Kort tid etter mottar de en telefonsamtale hvor vedkommende snakker norsk. Dette skjer gjerne i sammenheng med en reell hendelse i selskapet, slik som en endring i Brønnøysundregisteret, og offeret får beskjed om at de må godkjenne endringen via BankID. I realiteten gir en slik godkjenning bedragerne tilgang til bedriftens bankkonto. Ifølge DNB virker svindlerne svært profesjonelle og godt forberedt.[13]

Direktør- og fakturabedrageri går ofte under fellesbetegnelsen «business email compromise» (BEC). EUROPOL rapporterer at BEC har økt blant EU-land det siste året, og at COVID-19 har fungert som en katalysator. Ifølge EUROPOL er de kriminelle mer sofistikerte og målrettede i sine angrep. Bakmennene identifiserer det optimale tidspunktet for angrepet, bruker korrekt språk, og benytter kunstig intelligens (KI/AI) effektivt. Hvitvasking av utbyttet bærer også preg av profesjonalitet. De kriminelle har også økt sine angrep mot mindre foretak.[14]

Vurdering

Det er *meget sannsynlig* at norske virksomheter vil fortsette å bli utsatt for direktørbedrageri. Trusselen er høyest for store virksomheter med over 100 ansatte og særlig stor for internasjonale virksomheter hvor ledelsen sitter i utlandet, og den norske virksomheten kun er et datterselskap. Dette gjør det mulig for de kriminelle å utgi seg for å være fra hovedkontoret i utlandet, noe som øker legitimiteten til forespørselen. Trusselen vurderes å være noe lavere for mindre virksomheter.

9 NTAES, «Bedrageri mot næringslivet», 2019:28.
10 Finanstilsynet, «Risiko og sårbarhetsanalyse (ROS) 2019,» 2020:48.
11 DNB v/FC3, «Annual Fraud Report 2020», 2021.
12 Næringslivets Sikkerhetsråd, «Kriminalitets- og sikkerhetsundersøkelsen (KRISINO)», 2019:24.
13 Dagens Næringsliv, «Ny svindelmetode lurer direktører og styreledere til å åpne bedriftskontoen: - Inter nasjonal organisert kriminalitet med norske medhjelpere på bakken», 2020.
14 EUROPOL, «Internet organised crime threat assessment (IOCTA) 2020», 2020:47.

Fakturabedrageri

Ved fakturabedrageri forledes mottakeren av fakturaen til å betale for en vare eller tjeneste som de ikke har bestilt. Alternativt betaler mottakeren en kapret faktura hvor betalingen går til svindlerne.[15] Svindlere kan for eksempel utgi seg for å være leverandører, og be bedrifter betale for varer og tjenester til en annen konto enn den egentlige leverandørens konto.

43 prosent av virksomheter har i løpet av ett år opplevd å få faktura for varer som ikke er bestilt. Virksomheter med 1-4 ansatte er noe mindre utsatt (av disse har 34 prosent opplevd å få fakturaer for varer som ikke er bestilt).[16]

Fakturabedrageri kan være svært profesjonelt gjennomført. Dette så man ved bedrageriet av Norfund, som skjedde i forbindelse med en låneavtale inngått med en mikrofinansinstitusjon i Kambodsja. Lånet på 10 millioner dollar ble i stedet utbetalt til bedragerne som har manipulert både Norfund og finansinstitusjonen i Kambodsja via epost over lang tid.[17]

Fakturabedrageri som rammer privatpersoner

Fakturabedrageri er best kjent som en modus som rammer virksomheter, men også privatpersoner rammes av denne modusen.

En modus som benyttes for å bedra privatpersoner er at de blir lovet noe gratis, men faktureres i etterkant. Høsten 2020 kontaktet flere personer politiet og advarte om en bedrageri-modus hvor de blir lurt til å tegne et abonnement som deretter fakturerer månedlig via en betalingsløsning.

Det finnes noen store kriminelle aktører som står bak en betydelig andel av fakturabedrageriene og flere av de kriminelle aktørene som benytter fakturabedrageri som modus er norske. Enkelte aktører har hold på i mange år.

Vurdering

Kriminelle aktører kan oppnå stort utbytte ved fakturabedrageri. Det er derfor *meget sannsynlig* at denne modusen fremdeles vil bli brukt mot norske virksomheter. Større foretak bør i tillegg til masseproduserte bedrageri, være på vakt for sofistikerte og tilpassede fakturabedrageri.

Kreditt- og lånebedrageri

Kreditt- og lånebedrageri utføres både av privatpersoner og bedrifter. Bedrageriformen innebærer kjøp av varer og tjenester på kreditt eller ved opptak av lån, uten noen plan om å betale tilbake beløpet. I enkelte tilfeller føres pengene ut av Norge kort tid etter at lånet er betalt inn på konto.[18]

I NTAES sin rapport om bedrageri mot næringslivet pekes det på hvordan utenlandske personer som har arbeidet i Norge, har fått innvilget billån og deretter tatt med kjøretøyet til hjemlandet.[19] Det siste

15 NTAES, «Bedrageri mot næringslivet», 2019:32.
16 Næringslivets Sikkerhetsråd, «Kriminalitets- og sikkerhetsundersøkelsen (KRISINO)», 2019:24.
17 E24, «Norfund ble svindlet for 100 millioner: - Det er dobbelt så stort som Nokas-ranet», 2020.
18 NTAES, «Bedrageri mot næringslivet», 2019:37.
19 Justis- og beredskapsdepartementet, «Nasjonal risikovurdering - Hvitvasking og terrorfinansiering i Norge 2018», 2018:20.

halvåret har vi også sett at utenlandske studenter har tatt opp lån før utreise av landet og at folk med gjeld gjør opp for seg ved å la egen identitet bli misbrukt til lånebedrageri. Vi har informasjon om at det foregår organisert produksjon av falske lønnsslipper som benyttes ved låneopptak slik at personer som egentlig ikke kan få lån, allikevel gjør det.

Våren 2019 ble flere øst-europeiske aktører anmeldt for bedragerier knyttet til kjøp av dyre biler. Bedrageriene fremstår som rene bestillingsverk. Det har også dukket opp tilfeller hvor personer utsatt for ID-misbruk blir truet av kriminelle aktører til å hente biler kjøpt i deres navn. Bilene blir fraktet ut av landet og solgt videre.

Vurdering
Kreditt- og lånebedrageri fremstår enkelt å gjennomføre. Særlig billån virker svært enkelt å få innvilget. Med misbruk av ID-er og forfalskede dokumenter blir det vanskeligere å oppdage. Det er derfor *meget sannsynlig* at kreditt- og lånebedrageri vil fortsette å være en trussel for norske finansinstitusjoner.

Forsikringsbedrageri

Hvert år svindles forsikringsnæringen for betydelige beløp. Bransjen selv antar at kun en liten del av forsikringsbedrageriene blir avdekket, og at det er store mørketall.

I 2020 avslo forsikringsbransjen totalt 1360 saker i henhold til forsikringsavtaleloven. Dette er en liten økning fra 2019 da totalt 1217 saker ble avslått. Blant avdekkede saker i 2020, gjaldt 76 prosent privat skadeforsikring, 21 prosent syke- og uføreprodukter og 3 prosent næringsskadeforsikring. Når det kommer til beløp er det derimot syke- og uføreprodukter som utgjør mest med 59 prosent av avdekket beløp i 2020, mens 33 prosent gjaldt privat skadeforsikring. Det totale kravet for de avslåtte søknadene var på 466 millioner kroner. Antallet avdekkede bedrageriforsøk har vært i en stigende trend siden 2015.[20]

Aktører begår både lånebedrageri og forsikringsbedrageri
Enkelte aktører kombinerer lånebedrageri og forsikringsbedrageri.

Økokrim har informasjon fra en sak hvor dette foregår ved at bakmannen finner folk som er villig til å kjøre biler ut av landet, hvorpå bil og reisegods blir meldt stjålet og forsikring innkrevet.

I tillegg hjelper bakmannen bilsjåførene med å ta opp forbrukslån før de reiser. Som betaling tar bakmannen 15-20 prosent av lånebeløpet.

I Norge er det blant unge større sosial aksept for forsikringsbedrageri enn andre typer kriminalitet. Den yngre delen av befolkningen er også mer tilbøyelig til å gjennomføre forsikringsbedrageri enn de som er eldre. Videre er menn mer tilbøyelige til å gjennomføre forsikringsbedrageri enn kvinner. [21]

Forsikringsbedrageri relatert til tyveri eller skade på bil fremstår ofte å være godt organisert, og gjennomføres gjerne i kombinasjon med at bilen fraktes ut av landet og selges videre.

20 Finans Norge, «Forsikringssvindel i Norge – Svikstatistikk for avdekkede saker i 2020», 2021:5-6.
21 Finans Norge, «Forsikringssvindel i Norge, Svikstatistikk 2019», 2020:16.

Vurdering
Forsikringsbransjen er en institusjonell og erfaren motpart for bedragerne. Dette gir bransjen en fordel ved at de i større grad kan agere raskere og mer koordinert, enn enkeltbedrifter som utsettes for direktør- eller fakturabedrageri. Forbedrede systemer for å avdekke falske forsikringskrav forventes også å gjøre det vanskeligere å bedrive denne typen bedragerier. Den sosiale aksepten for forsikringsbedrageri, særlig blant de unge, er derimot en utfordring. Det er derfor *mulig* at forsøk på forsikringsbedrageri vil øke i 2021.

Bedrageri av utenlandske sjømatimportører

Økokrim har mottatt flere tips om nettsvindel relatert til fiktive salg av sjømat til utenlandske importører. Dette er en modus aktører har brukt for å bedra utenlandske kjøpere av norsk sjømat i en årrekke.

Bedragerisakene har lik modus og viser at gjerningspersonen(e) har praktisk kjennskap til transaksjoner ved eksport av sjømat, samt oppdatert kunnskap om norske sjømateksportører. Fornærmede er utenlandske sjømatimportører som blir tilbudt å kjøpe ulike sjømatvarer fra gjerningspersonene. Gjerningspersonene fremstår som en tilsynelatende legitim norsk sjømateksportør. Ved et salg krever gjerningspersonene at fornærmede forhåndsbetaler for deler av leveransen.

Det benyttes som regel pengemuldyr med norsk bankkonto til å motta pengene fra bedrageriofferet, samt aktører godt omhandlet i politiets systemer til å hvitvaske disse. Flere kan knyttes til organisert kriminalitet i Norge.

Foruten å påføre fornærmede økonomiske tap, svekker bedrageriene norsk eksportnærings omdømme og den medfører en stor belastning for de som får sin identitet misbrukt.

Vurdering
Dette er en modus kriminelle aktører har brukt over en rekke år for å bedra utenlandske kjøpere av norsk sjømat. Modusen har vært omtalt i media, bransjen har økt fokus på problematikken og enkelte involverte har blitt siktet i straffesaker. Likevel ser vi at det dukker opp nye saker med samme modus. Det er derfor *meget sannsynlig* at denne typen bedrageri vil fortsette.

Bedrageri av privatpersoner

Over 100 000 nordmenn sier de har blitt utsatt for ID-tyveri de siste to årene. Kun 22 prosent av de som er rammet av ID-tyveri, anmelder dette til politiet.[22]

DNB opplevde en økning i antall bedragerier på nesten 25 prosent i 2020, sammenlignet med 2019.[23]

I sin årlige trusselvurdering advarer DNB om at kriminelle vil øke sin bruk av automatisering ved bedrageri. Dette innebærer blant annet at dialogen med potensielle bedragerioffer er automatisert.[24]
Dette gjør de kriminelle i stand til å nå ut til flere potensielle bedragerioffer på kortere tid.

Pyramidespill

Pyramidespill (Ponzi-bedrageri) er en form for investeringsbedrageri hvor man tiltrekker seg investorer med løfter om høy avkastning, mens verdiøkningen i virkeligheten kun er en illusjon. Eventuelle utbetalinger til investorer er overføring av midler fra nyere investorer, ikke avkastning.[25]

Pyramidespill omsettes sjeldent i et vanlig marked, noe som gjør de vanskeligere å avsløre. Pyramidespill skaper også grobunn for annen økonomisk kriminalitet, slik som brudd på reglene for hvitvasking, valutahandel, verdipapirhandel, bedrageri, regnskapsjuks, skatteunndragelse, lotteri- og pengespill, samt forbrukerrettslige regler for markedsføring og produktansvar.

Det er vanlig at pyramidespillene tilbyr investeringsmuligheter i flere ulike produkter. Bruken av kryptovaluta som investeringsobjekt har økt i den senere tid. Det at pyramidespillene ofte fremstår profesjonelle gir den ulovlige virksomheten legitimitet.

Pyramidespill er forbudt i flere land, men bakmennene finner stadig nye metoder for å omgå regelverket. Ofte forflytter de som står bak ulovlige pyramideselskap seg fra selskap til selskap. De oppretter nye selskap når de ikke lenger tjener penger i et selskap, eller når det har blitt avdekket at de driver et ulovlig pyramidespill. Mange pyramidespill driftes også av internasjonale selskap med utenlandske bankkontoer.

Vurdering
Det er *meget sannsynlig* at det pågår pyramidespill hvor norske borgere vil bli svindlet for store summer.

22 NorSIS, «Ny undersøkelse: Over 100 000 nordmenn har opplevd ID-tyveri de siste to årene»,2021.
23 DNB v/FC3, «Annual Fraud Report 2020», 2021.
24 DNB, «Årlig Trusselvurdering», 2021:18.
25 NTAES, «Bedrageri mot næringslivet», 2019:42.

Investeringsbedrageri

Investeringsbedrageri innebærer at man blir forledet til å investere i prosjekter eller produkter som er verdiløse eller ikke-eksisterende. Dette kan være investeringer i aksjer eller andre finansielle instrumenter, eiendom, råvarer, verdifulle gjenstander som kunst og antikviteter. Sosial manipulering er en sentral del av bedrageriprosessen.[26]

I forbindelse med koronapandemien spiller bedragerne på de store børssvingningene og at det nå er tiden for å investere i aksjer og kryptovaluta.[27] Spesielt via falske handelsplattformer har man sett en stor økning i bedrageriforsøk, og britiske myndigheter har fjernet over 300 000 nettsider i 2020, som knyttes til investeringsbedrager.[28] I flere land anses investeringsbedrageri over nett nå som den raskest voksende kriminalitetsutfordringen.[29] [30] Bedragerne har også blitt også mer målrettede i angrepene.[31]

Bankenes sikkerhetssenter avdekket 200 000 transaksjoner knyttet til investeringsbedrageri og avverget svindel for totalt 700 millioner kroner i 2020. Dette er en økning fra 100 000 avdekkede transaksjoner og 450 millioner kroner i avverget svindel i 2019. Det synes å være en overrepresentasjon av menn i alderen 30–50 år blant de som forledes.[32]

En vanlig modus

Et bedragerioffer trykker på en annonse i sosiale medier, gjerne en som fremhever hvordan en kjendis har tjent masse penger. Kort tid etter å ha fylt inn kontaktopplysninger blir han eller hun oppringt av noen som snakker godt engelsk, er overbevisende og bruker ord og begrep som gir inntrykk av kompetanse. Bedragerne vet at dette gjør fornærmet usikker samt overbevist om at de snakker med fagfolk. I realiteten blir bedragerioffer trolig oppringt fra et call-senter som kan ligge hvor som helst i verden.

Når fornærmede er overbevist og sier ja til å investere er neste fase og få offeret til å overføre pengene. Dette gjøres ofte ved at offeret overfører penger til en utenlandsk bankkonto, men offeret kan også bli bedt om å overføre pengene til en norsk bankkonto. I så fall bruker bedragerne pengemuldyr i Norge for å omgå bankenes sikkerhetssystemer.

Dette samsvarer med tall fra DNB som rapporterer om en 39 prosents økning i antall offer for investeringsbedrageri fra 2019 til 2020[33] og tall fra Danske bank som også rapporterer om en økning i investeringsbedrageri i 2020. De forklarer økningen med permitteringer, lave renter og at verdien på kryptovaluta har skutt i været. Sistnevnte brukes for å lure folk inn i investeringsbedrageri.[34]

26 NTAES, «Bedrageri mot næringslivet», 2019:41.
27 DNB, «Investeringssvindel har eksplodert», 2020.
28 NCSC, «Celebrity scam alert as criminals use rich and famous to lure online victims», 2020.
29 EUROPOL, «Internet organised crime threat assessment (IOCTA) 2020», 2020:50.
30 Uttalt av møteleder i AP APATE møte 26. oktober 2020.
31 TV2, «Stoppet svindelforsøk for 700 millioner kroner», 2021.
32 TV2, «Stoppet svindelforsøk for 700 millioner kroner», 2021.
33 DNB v/FC3, «Annual Fraud Report 2020», 2021.
34 Dagens Næringsliv, «DNB frykter ny helautomatisert form for svindel innen kort tid: - Det kan bli veldig omfattende», 2021.

Ifølge DNB tilhører bakmennene avanserte organiserte kriminelle grupperinger med koblinger til Øst-Europa og Israel. Disse bruker gjerne offer for kjærlighetsbedrageri som pengemuldyr.[35] INTERPOL advarer også om at investeringsbedragere rekrutterer offer via dating-apper.[36]

Økokrim mottar jevnlig tips om personer og foretak som er involvert i investeringsbedrageri. I 2021 har vi informasjon om investeringsbedrageri knyttet til virksomhet innen oljesektoren, Fintech, eiendom, kryptovaluta og vaksiner.

Modusene ved investeringsbedrageri knyttet til kryptovaluta er mange, og enkelte modus er de samme som for aksjeinvesteringer. Andre modus inkluderer opprettelse av falske handelsplattformer på nett, gjerne kombinert med en aggressiv markedsføring i sosiale medier som også misbruker kjente personer for å skaffe legitimitet.[37] [38] [39] Fornærmede kan også motta fiktive kvitteringer og dokumentasjon på investering og gevinst, som igjen brukes for å manipulere fornærmede til å gjøre ytterligere investeringer. Økokrim anslår at nordmenn årlig sender 50 millioner ut av landet i forbindelse med kryptobedrageri.[40]

Vurdering
Falske handelsplattformer markedsføres aggressivt og fremstår ved første øyekast som seriøse. Mediene skriver også fortsatt regelmessig om kryptovaluta, og folks frykt for å gå glipp av en «sikker gevinst» bør ikke undervurderes. Det er meget sannsynlig at omfanget av investeringsbedrageri med kryptovaluta og falske handelsplattformer vil øke, og at nordmenn vil bli bedratt for betydelige beløp.

Kortbedrageri

Ved kortbedrageri benytter gjerningspersonen en annen persons betalingskort eller kortopplysninger til å gjennomføre kjøp eller kontaktuttak. Kortbedrageriet foregår enten ved kjøp eller kontantuttak hvor kortet er fysisk tilstede (Card present), eller som en transaksjon hvor kortet ikke er tilstede (Card-not-present (CNP)).[41]

Fysiske sikkerhetsmekanismer
De fysiske sikkerhetsmekanismene er essensielle i stadig mer av egenbeskyttelsen på internett og i vår hverdag. Dette gjør tilgang til de mer attraktive for kriminelle da det åpner opp for ulike typer kriminalitet, slik som identitetstyveri, tømming av nettbank, og kortbedrageri.

For å få tak i kortopplysningene benytter kriminelle i hovedsak tre ulike metoder. Dette kan være skimming (kopiering av kortopplysninger via kortets magnetstripe), pharming/phishing (falsk nettside eller svindel e-post hvor du taster inn kortopplysninger) og datainnbrudd (hacking) av leverandører som lagrer kunders kortopplysninger.[42]

35 DNB, «Årlig Trusselvurdering», 2021:18.
36 INTERPOL, «Investment fraud via dating apps», 2021.
37 Dagens Næringsliv, «Fortviler over kryptosvindel – klager på henleggelse», 2019.
38 NTAES, «Bedrageri mot næringslivet», 2019:42.
39 Nettavisen, DNB advarer mot helt ny bedragerimetode – kundene svindles på finn.no», 2020.
40 E24, «Bitcoin-kursen snuser på rekord: Økokrim advarer mot bedrageri-bølge», 2021.
41 NTAES, «Bedrageri mot næringslivet», 2019:39.
42 NTAES, «Bedrageri mot næringslivet», 2019:40.

På grunn av innføringen av chip (EMV) på bankkortene, har skimming blitt et mindre problem i Europa, men det er fortsatt et omfattende problem i andre deler av verden. Falske nettsider eller e-poster som lurer deg til å gi fra deg kortopplysinger er effektive verktøy for kriminelle.[43] Enkelte nettsider utgir seg for å selge varer ekstremt billig, men i realiteten er det bare et skalkeskjul for å få tak i kortopplysninger.[44] Enkeltaktører eller organiserte kriminelle kan alene stå bak et betydelig antall bedragerier. Politiet mottok tidligere i år informasjon om en phishing kampanje hvor det ble avdekket databaser som inneholdt to milliarder linjer med personlig data, primært e-postadresser. Organisasjonen distribuerte phishing e-poster som var forkledd som offisielle betalingssider, gjerne tilknyttet oppdatering av betalingsinformasjon på strømmetjenester (eks. Netflix).

Et betydelig antall forsøk på kortbedrageri avverges av bankene. Tap ved kortbedrageri gikk ned med 22 prosent fra 2019 til 2020 til 148 millioner. Antallet svindeltransaksjoner falt med syv prosent, noe som viser at svindlerne i snitt får tak i et lavere beløp enn tidligere.[46]

Ifølge DNB økte netthandel blant eldre i perioden 1. november til 24 desember 2020 med 75 prosent sammenlignet med samme periode i 2019. Totalt steg netthandelen med 56 prosent, men fysisk handling utgjør fortsatt 85 prosent.[47]

Vurdering
På grunn av koronaviruset har flere norske borgere begynt med netthandel, mange for første gang. Det er forventet at pandemien vil fungere som en katalysator og at flere vil fortsette med netthandel også etter pandemien. Det er *meget sannsynlig* at flere norske borgere vil bli utsatt for phising, særlig via falske nettsider og e-poster. Det er *sannsynlig* at forsøk på kortbedrageri vil øke i Norge. Foreløpig ser det ut til at bankenes systemer for å stanse kortbedrageri fungerer godt nok til at dette ikke omsettes til tap for fornærmede.

Nettbankbedrageri

Det er i hovedsak to metoder som benyttes ved nettbankbedrageri. Den ene er at bankens infrastruktur angripes via kundens nettbank ved at offeret får sin datamaskin infisert med en trojansk hest (skjult dataprogram). De kriminelle tapper så kundens konto for penger.[48] Den andre metoden er tyveri av fysiske sikkerhetsmekanismer (eksempelvis BankID), eller falske BankID-brukersteder.[49] Det er store mørketall på dette området da få anmelder.

Det er internasjonalt en trend at falske nettsider blir konstruert for å ligne på for eksempel nettsiden til en nettbank. Offeret blir lurt inn på denne nettsiden og taster inn påloggingsinformasjonen, som så blir kopiert og lagret av de kriminelle, for deretter å benytte dette for å logge seg inn i offerets nettbank og tømme kontoen.[50]

43 ATT, «Protect yourself from phishing and false websites», ukjent.
44 Telenor, «Unngå kortsvindel i julestria», 2019.
46 Finanstilsynet, «Risiko og sårbarhetsanalyse (ROS) 2020», 2021:7.
47 Dagens Næringsliv, «Julehandelen trosset korona»,2020.
48 NTAES, «Bedrageri mot næringslivet», 2019:30.
49 Finanstilsynet, «Risiko og sårbarhetsanalyse (ROS) 2018», 2019:19.
50 EUROPOL, «Internet organised crime threat assessment (IOCTA) 2018», 2018:56.

Nettbankbedrageri har blitt mer profesjonalisert ved at en gjerne blir satt over fra en kundebehandler til den neste. I tillegg snakker «kundebehandlerne» i mange tilfeller godt norsk og benytter seg av spoofing, slik at det er bankens telefonnummer som vises for den som blir oppringt.[51]

I 2019 og 2020 var det bedragerikampanjer rettet mot eldre kvinner, ofte omtalt som Olga-bedrageri på grunn av at ofrenes navn i mange tilfeller kunne assosieres med høy alder. Bedrageriene ble utført systematisk og profesjonelt. Minst 57 eldre kvinner skal ha blitt svindlet for rundt 13,5 millioner kroner.[52]

Finanstilsynet rapporterer at tapstallene knyttet til bruk av nettbank utgjorde 355 millioner kroner i 2020. Antallet bedrageriforsøk økte i 2020, men gjennomsnittlig tap ble redusert, slik at de totale tapstallene er ble lavere i 2020 enn 2019.[53]

Person(er) som utgir seg for å være fra politiet
Våren 2021 har en eller flere kriminelle aktører kontaktet privatpersoner på telefon og utgitt seg for å være fra politiet. Telefonnummeret fornærmet ser på sin telefon tilhører politiet, men dette er manipulert av bedrageren(e).

Troverdigheten dette gir har kriminelle brukt for å få folk til å oppgi sensitive bank-, kort- og personopplysninger. Dette brukes deretter for å tømme fornærmedes bankkonto og bankkort samt ta opp lån som umiddelbart overføres til de kriminelle.

Det har våren 2021 foregått flere omfattende bedragerikampanjer som misbruker ulike virksomheter for å få tilgang til privatpersoners kort-/ og/eller bankopplysninger. I noen av de retter bedragerne angrepet mot eldre personer, og modus kan minne om de tidligere Olga-bedrageriene. Det er trolig utenlandske bakmenn involvert i alle fall i en av bedragerikampanjene.

I løpet av de siste månedene har også flere personer som er i en jobbsøkeprosess blitt utsatt for bedrageri, eller forsøk på dette. I mange av sakene har offeret blitt kontaktet av noen som utgir seg for å være en arbeidsgiver de har søkt jobb hos, og som kontakter de via SMS eller e-post som fremstår å være fra en jobbsøkerportal de har benyttet.

Vurdering
Nettbankbedrageri ved hjelp av falske nettsider er ikke en stor trussel i Norge, da man som regel krever to-nivå autentisering (slik som SMS eller BankID). Ettersom de «enkle» mulighetene til å gjennomføre kortbedrageri blir færre, er det *meget sannsynlig* at tyveri av fysiske sikkerhetsmekanismer blir mer attraktive for kriminelle, og vil øke. Det er *meget sannsynlig* at både nettbankbedrageri og andre typer kriminalitet som kan gjennomføres ved hjelp av stjålne fysiske sikkerhetsmekanismer vil øke som en konsekvens.

Kjærlighetsbedrageri

Ved denne typen bedrageri etablerer kriminelle en relasjon til sitt offer over lengre tid før svindelen gjennomføres. Ved å bruke god tid i å bygge relasjonen opparbeides større tillit, noe som igjen reflekteres i totalbeløpet offeret bedras for. Ved hjelp av sosiale medier og regelmessig tett kontakt i private kanaler bygges det opp en historie som legger opp til at offeret skal sende penger, gjerne i små beløp i

51 NRK, «'Olga-svindelen' er tilbake: Ti personer svindlet for 1,5 millioner kroner», 2020.
52 NRK, «Fra dette hotellrommet i Oslo skal mennene ha svindlet eldre kvinner for 13 millioner», 2020.
53 Finanstilsynet, «Risiko og sårbarhetsanalyse (ROS) 2020», 2021:7.

begynnelsen, men som etter hvert vil øke ettersom offeret betaler. Ofrene er gjerne godt voksne med profiler i sosiale medier eller på dating-sider.[54]

I de tilfellene hvor banken mistenker bedrageri, tar de kontakt med offeret, men det er ofte vanskelig å overbevise offeret om at de har blitt manipulert da de fanges i en følelsesmessig relasjon det er vanskelig å bryte ut av.[55] I en sak fra 2017 klaget et bedragerioffer inn DNB til Finansklagenemnda etter at banken nektet henne å overføre penger til «forloveden».[56]

Finanstilsynet estimerer at tapene forbundet med kjærlighetsbedrageri utgjorde ca. 43 millioner kroner i 2019.[57]

Hos DNB var det 254 kunder som ble utsatt for kjærlighetsbedrageri i 2020. Ofrene tapte gjennomsnittlig 48 500 kroner, totalt over 12 millioner kroner.[58] Ifølge banken er antallet saker relativt stabilt. De påpeker derimot at i mange tilfeller er ikke formålet primært bedrageri, men å skaffe seg pengemuldyr.[59] Danske Bank rapporter om en økning i kjærlighetsbedrageri under koronapandemien.[60]

Politiet har opplysninger om at ofre for kjærlighetsbedragerier kjøper dyre elektronikkvarer (eks. iPhone, iPad, Mac) og gavekort som de deretter sender til bakmennene. Dette er trolig for å omgå bankenes mulighet til å stanse utenlandstransaksjoner.

En «romantisk» historie

Bedragerne vil ofte bygge en relasjon med fornærmede over lang tid. Dette gjør manipulasjonen mer overbevisende. Etter en stund vil de spørre om en tjeneste. Ofte påstår bedragerne at de har en jobb som innebærer mye reising. Dette gjør mange av unnskyldningene for hvorfor de trenger økonomisk hjelp mer troverdig. De kan for eksempel være strandet på en flyplass, trenge hjelp med en tollavgift eller penger til en flybillett slik at de kan komme på besøk.

Bedragerne forsøker i mange tilfeller også å bruke fornærmet som pengemuldyr. Her igjen hjelper det på troverdigheten at de arbeider internasjonalt da pengene ofte vil komme fra utlandet, samt at det skal overføreres videre til et tredje land.

Dette kan foregå over flere år, noe som igjen forsterker troverdigheten og den følelsesmessige relasjon fornærmede får til bedragerne.

Politiet har også informasjon som om foretak som er involvert i kjærlighetsbedrageri ved at de stiller bankkonto til disposisjon for bedragere.

54 NorSIS, «Trusler og trender 2018 – 19», 2018:18.
55 Finanstilsynet, «Risiko og sårbarhetsanalyse (ROS) 2018», 2019:73.
56 Dagens Næringsliv, «Overførte 745.000kr til kriminelle – klager på DNB fordi hun ikke får sende mer penger», 2018.
57 Finanstilsynet, «Risiko og sårbarhetsanalyse (ROS) 2019», 2020:48.
58 DNB v/FC3, «Annual fraud report 2020», 2021.
59 DNB, «Årlig Trusselvurdering», 2021:18.
60 Dagens Næringsliv, «DNB frykter ny helautomatisert form for svindel innen kort tid: - Det kan bli veldig omfattende», 2021.

Vurdering
Koronapandemien og påfølgende ensomhet antas å gjøre flere norske borgere sårbare for kjærlighetsbedrageri. For bedragerne er dette en kriminalitetsform som har lav risiko for å bli tatt og dømt, samtidig som utbyttet er stort. Det er derfor *sannsynlig* at kjærlighetsbedrageri vil øke i omfang.

Gebyrbedrageri[61]

Ved denne modusen lures offeret til å betale det de tror er en avgift. Som regel påstår bedragerne at avgiften er for levering av en postpakke, eller lignende varelevering. Det finnes også eksempler på at «avgiften» er for å kunne utbetale gevinst fra et utenlandsk lotteri (som offeret ikke har deltatt i), eller en tollavgift på dyrebare verdier, for eksempel gull, som påstås å være på vei til offeret, men som har blitt stanset av toll.

DNB rapporterte at gebyrbedrageri økte med 55 prosent i 2020, til totalt 579 saker. I snitt taper offeret 20 300 kroner per sak.[62] Ifølge banken var økningen nesten utelukkende mot kunder som forsøkte å ta opp lån hos det de trodde var utenlandske finansinstitusjoner. DNB mener dette har vært drevet av anstrengt økonomisk situasjon for enkelte under koronapandemien, samt at opprettelsen av gjeldsregisteret har tvunget mange som ikke lenger får lån i Norge til å lete etter utenlandske aktører på nett.[63]

To nettsider som tilbyr lån uten kredittsjekk har blitt benyttet til å bedra flere personer den siste tiden. Det gjøres ved å kreve innbetaling av et «gebyr» før utbetaling av lån. I begge tilfellene ser det ut til at pengemuldyr benyttes.

Det har også vært flere offer knyttet til salg av bil på finn.no. Offeret er bilselger, mens «kunde» utgir seg for å bo i utlandet, i mange tilfeller Danmark. På grunn av dette ønsker de at selger skal betale ulike avgifter for at bilen skal kunne fraktes og importeres til Danmark. I minst en sak betalte også offeret i håp om å få tilbake pengene.

Politiet mottar jevnlig informasjon fra folk som har blitt utsatt for bedrageriforsøk ved at bedragerne forsøker å kreve inn et «gebyr» for en postpakke som angivelig er fra Posten, Digipost, eller mer ukjente logistikkselskap. Hvis offeret betaler «porto» gir de i realiteten bedragerne kortopplysninger som så brukes for å tømme bankkortet for penger.

Vurdering
Trusselen knyttet til gebyrbedrageri vil *meget sannsynlig* forbli uendret.

61 Advanced fee fraud.
62 DNB v/FC3, «Annual Fraud Report 2020», 2021.
63 DNB, «Årlig Trusselvurdering», 2021:17.

Annonsebedrageri

Dette foregår ved at offeret betaler for en vare de aldri mottar. Dette skiller seg fra fakturabedrageri ved at de ikke mottar en faktura uten at offeret selv aktivt har forsøkt å bestille en vare. Dette skiller seg også fra avgiftsbedrageri da offeret betaler full pris, og ikke kun en avgift.

Det er en utfordring at bedragere av mindre beløp ikke blir stoppet. Det er flere personer og foretak som tar betalt for varer som aldri leveres. Ofte via finn.no, men også andre plattformer. Mange har blitt rapportert av opptil flere bedragerioffer, men bedragerne får tilsynelatende fortsette med bedrageriene.[64]

Politiet har kjennskap til flere nettvirksomheter som utgir seg for å selge mobiltelefoner, men i realiteten leveres aldri varen. De annonserer via Facebook, og virker å ha rekruttert pengemuldyr som tar imot betalingene fra ofrene. Bedrageriet virker profesjonelt og systematisk gjennomført. Det benyttes bilder fra reelle firma, og pengemuldyr rekrutteres ved at de tror de er ansatt. En del av innbetalingene er overført videre til utlandet.

Politiet har også informasjon om at en falsk nettside tar betalt for varer som aldri leveres. Nettsiden drives formentlig av en norsk borger som er godt omhandlet i politiets systemer. Foreløpig er det ikke snakk om mange saker, men det finnes også tilfeller hvor offeret har blitt bedratt til å gi fra seg virtuelle spillgjenstander. Disse kan ha en verdi på over 100 000 kroner.[65]

Vurdering

Det er *meget sannsynlig* at utfordringene knyttet til annonsebedrageri vil vedvare. Det er videre *meget sannsynlig* at bedragerne rekrutterer stråpersoner på sosiale medier som benyttes i betalingsformidlingen for å tilsløre midlenes opphav og mottaker av pengene.

Utpressing

Trusler om å publisere video av potensielle bedragerioffer som onanerer (sextortion) er ofte benyttet modus. Et slikt opptak eksisterer selvfølgelig ikke, men mange lar seg skremme til å betale bedragerne.

Denne kriminalitetsformen virker å ha økt i løpet av 2020. Spesielt i løpet av høsten 2020 mottok politiet henvendelser fra flere bekymrede personer. De fornærmede er som regel menn. Gjerningspersonen vil ha betalt i Bitcoin (BTC) sendt til wallet (lommebok). Videre skriver bedragerne godt norsk og det virker ikke å benyttes oversettingsverktøy.

Det er forventet at bruken av deepfake vil bli mer utbredt innenfor sextortion.[66]

Vurdering

Økt bruk av deepfake vil gjøre forsøk på sextortion mere troverdig. Det er *sannsynlig* at flere vil bli offer for denne typen utpressing.

64 Bergens Avis, «Advarer mot sofaselger på finn: - Vi ble lurt av samme mann», 2020.
65 NRK, «Vart svindla for 140 000 kroner på spel plattform», 2020.
66 Trend Micro, «Trading in the dark», 2020.