Bedrageri

– et samfunnsproblem

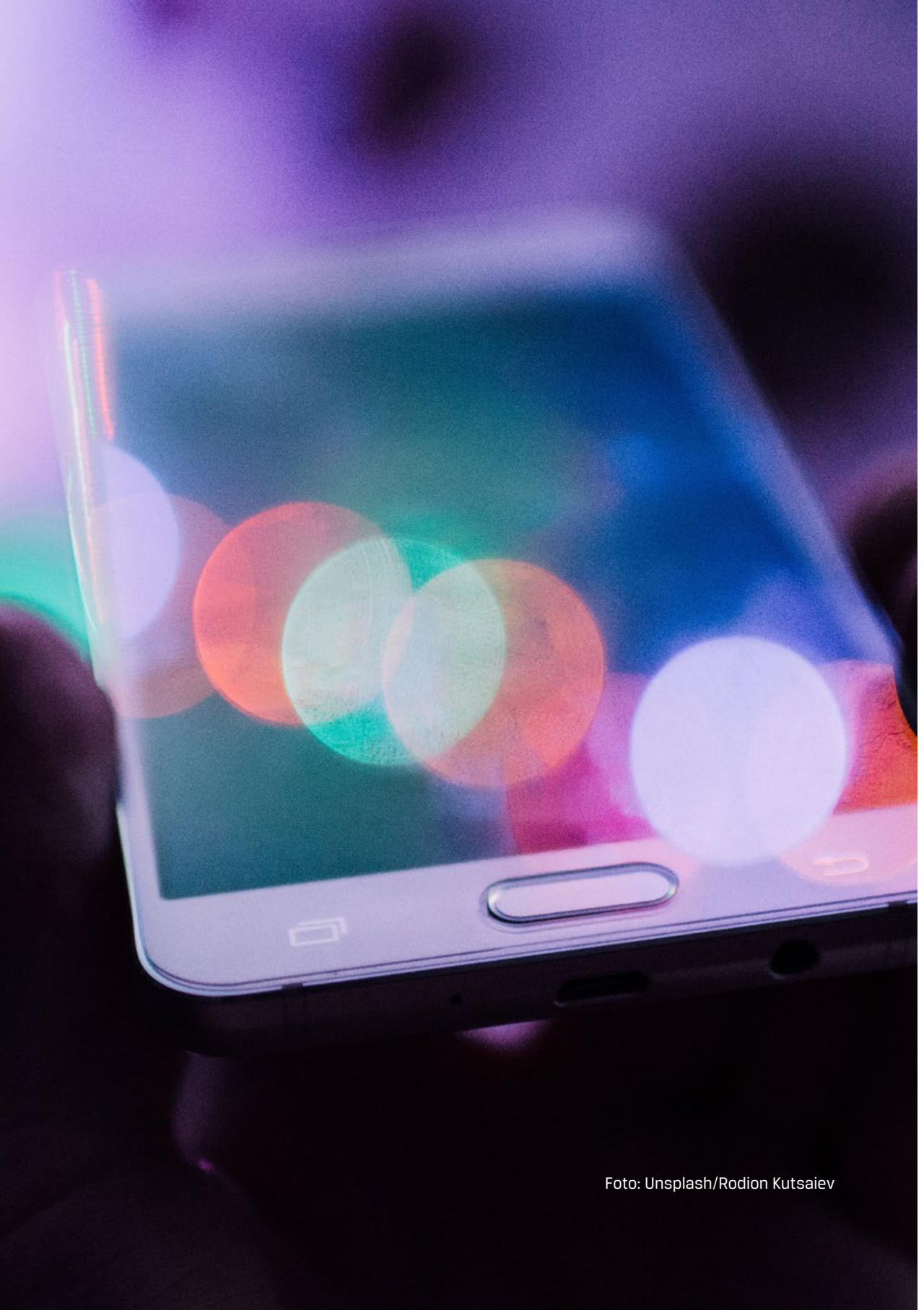


Foto: Unsplash/Rodion Kutsaiev

Forord

Både politiet og bankene registrerer en voldsom økning i antall bedrageri, og omfanget er nå så stort at det er et samfunnsproblem. For første gang kommer Økokrim med en kunnskapsoppsummering med konkrete anbefalinger til tiltak. Kriminelle nettverk står bak massebedrageri, og den teknologiske utviklingen gjør at kriminelle får stadig flere virkemidler.

Vi som samfunn må ta tak i dette og endre kurs. Vi ser allerede at folk er skeptiske til informasjon fra det offentlige, fordi de er engstelig for at det er bedrageri. Ifølge politiets innbyggerundersøkelse fra 2021 er identitetstyveri og bedrageri på internett blant de hendelsene som norske borgere er mest bekymret for å bli rammet av. Bedrageri på nett er samtidig blant hendelsene som innbyggerne har minst tillit til at politiet evner å håndtere. Vi kan ikke komme dit at tillitssamfunnet vårt brytes ned.

Kriminelle tar raskt i bruk ny teknologi og opparbeider seg betydelige økonomiske midler som benyttes til å finansiere ny kriminalitet. Både privatpersoner, organisasjoner og bedrifter lider store økonomiske tap, og politiet, banker og IKT- og sikkerhetsavdelinger må bruke betydelige ressurser på å avdekke bedrageri.

For å møte dette problemet vil Økokrim i 2023 opprette en nasjonal bedragerienhet. Formålet med enheten er å identifisere bedragerilovbrudd som rammer innbyggere på tvers av politidistrikt, og/eller som har internasjonale forgreninger, og få i stand en mer effektiv og strukturert bedrageribekjempelse blant annet ved å iverksette forebyggende tiltak i samarbeid med banker og andre i næringslivet. Dette skal også styrke etterforskingen av bedrageri som er organisert og systematisk utført.

Men dette er ikke nok. Vi som samfunn må se helhetlig på dette problemet, og gå sammen for å stoppe det. Derfor kommer vi med anbefalinger til tiltak, som vi også jobber videre med i Økokrim.

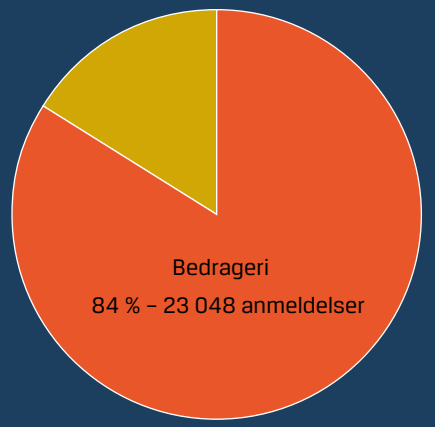
Pål K. Lønseth
Sjef for Økokrim

Antall bedrageri øker

Fra 2013 til 2022 har antall anmeldelser av bedrageri økt med nesten 60 prosent. Tall fra banksektoren indikerer at økningen er større og mørketallene antas å være betydelige.

Antall bedrageriforsøk er langt høyere enn antall anmeldelser. Hver måned stanses det, ifølge Nasjonal kommunikasjonsmyndighet (Nkom), over én million bedrageriforsøk via telefon.

Anmeldt økonomisk kriminalitet 2022



Kilde: SSB

Alle kan bli offer for bedrageri

Bedragerier kan ramme alle, uavhengig av alder og sosial status. Tradisjonelt har personer i pensjonsalder vært ansett som mest sårbare for bedrageri.[1] I Storbritannia observeres det nå at flere av ofrene for bedrageri er personer mellom 25 og 54 år med høy utdanning og inntekt.[2]

Det kan være svært belastende å bli offer for bedrageri, både økonomisk og følelsesmessig. Bedrageriofre rapporterer ofte om sterk skamfølelse og depresjon. Internasjonalt har det også vært hendelser hvor mennesker har tatt sitt eget liv som en direkte konsekvens av å ha blitt bedratt.

1 Europol, Internet organised crime threat assessment (IOCTA), 2021.
2 RUSI, The Silent Threat: The impact of fraud on UK National Security, 2021.

Organiserte kriminelle nettverk begår bedrageri

Flere siktede i norske bedragerisaker kan knyttes til organiserte kriminelle nettverk. Aktørene kan også knyttes til alvorlig kriminalitet som narkotikakriminalitet og besittelse av våpen. Flere av de norske bedrageriaktørene er unge menn som i tidlig alder har startet med kriminalitet og blitt en del av kriminelle miljø. Det er også mange bedragere med tilhold i utlandet.

Kriminelle aktører i Norden samarbeider også tett ved bedrageri og hvitvasking av utbytte.

Aktørene kan være svært kyniske og bedrar blant annet målrettet eldre mennesker som kan ha lav teknologisk kompetanse og rekrutterer unge personer til å være pengemuldyr.

Bedrageri genererer store summer til kriminelle

Tapene i Norge relatert til bedrageri var totalt på over en halv milliard kroner i 2022.[3]

Majoriteten av bedrageri resulterer i forholdsvis små beløp tapt per person. Ved investeringsbedrageri og kjærlighetsbedrageri kan imidlertid de økonomiske tapene for ofrene være betydelige. Det er ikke uvanlig at ofre taper flere hundre tusen kroner, og i noen tilfeller millionbeløp.

De kriminelle reinvesterer ofte inntektene fra bedrageri i annen kriminell virksomhet.[4] Eksempler fra utlandet viser at i Sverige finansierer bedrageri grov voldskriminalitet og annen organisert kriminalitet.[5] I Storbritannia har det blitt avdekket at inntekter fra bedrageri har gått til å finansiere terrorisme, blant annet IS.[6]

3 Finanstilsynet, Risiko- og sårbarhetsanalyse (ROS), 2023.
4 Europol, Serious and organised crime threat assessment (SOCTA), 2021.
5 Nationellt Bedrägericentrum, De dödliga bedrägerierna, 2022.
6 HM Government, Fraud Strategy: Stopping scams and protecting the public, 2023.

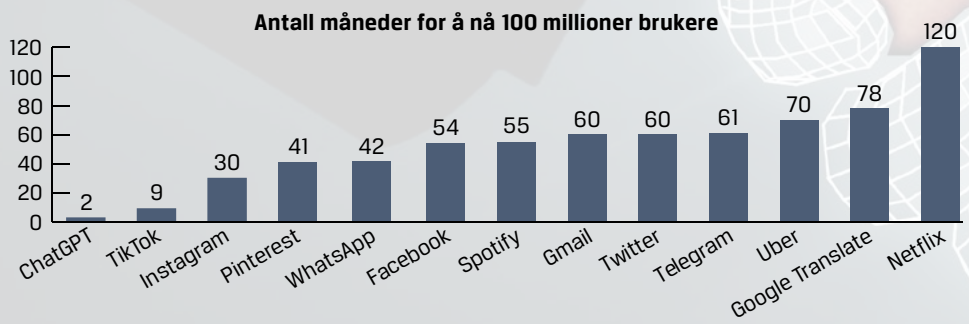
Et digitalisert samfunn i en polarisert verden

Et digitalisert samfunn
Virtualisering og digitalisering skyter fart innen forbrukersfæren og kritisk infrastruktur, samt offentlige og private tjenester. Dette gjør at vi kan samhandle både sosialt og økonomisk på tvers av landegrenser i sanntid.

I 2021 hadde 96 prosent av den norske befolkningen tilgang på smarttelefon og i 2022 brukte ni av ti nordmenn sosiale medier. Med det er vi også svært tilgjengelige for bedragere.

Adopsjonen av ny teknologi, som kunstig intelligens (KI), går stadig raskere. Det tok bare to måneder før KI-tjenesten ChatGPT hadde 100 millioner brukere. Til sammenligning brukte Facebook 54 måneder på å oppnå det samme. Kunstig intelligens er dermed tilgjengeliggjort for allmennheten, inkludert for aktører med ønske om økonomisk vinning.

Bedragere har fått tilgang til tjenester som kan skape overbevisende tekster som er egnet til å forlede et stort antall offer.



En polarisert verden
Krigen i Ukraina og økt polarisering mellom øst og vest preger i dag utviklingen i verden. Bruken av sammensatte trusler[7] er aktualisert, og ulike virkemidler, blant annet i det digitale rom, benyttes for å true Norges verdier og interesser.[8]

PST har sett flere eksempler på at kriminelle aktører drives av samme intensjon eller målsetting som statlige aktører. Hacktivist-gruppen Killnet, som identifiserer seg med Russland, har gjennomført tjenestenektangrep[9] mot flere statlige institusjoner og virksomheter i Europa. Det er også tilfeller hvor utenlandske etterretningstjenester og kriminelle aktører samarbeider om løsepengevirus, og tilfeller hvor etterretningstjenesters egne digitale trusselaktører har vinningskriminalitet som mål.[10]

Den sikkerhetspolitiske situasjonen og de flytende grensene mellom bedrageri og sammensatte trusler utfordrer derfor sektoransvar og beredskap, både nasjonalt og lokalt.

---

7 I følge FFI er sammensatte trusler en betegnelse på strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt som kan kombinere diplomatiske, informasjonsmessige, militære, økonomiske og finansielle, etterretningsmessige og juridiske virkemidler for å nå strategiske målsettinger.

8 Forsvaret, Fokus, 2023.

9 Tjenestenektangrep er et digitalt skadeverk med formål å forhindre eller forringe tilgangen til en tjener, tjeneste eller et nettverk. Et tjenestenektangrep kan ramme en hel virksomhet, men også privatpersoner. (Kripos, Cyberkriminalitet 2023, 2023.)

10 PST, Nasjonal trusselvurdering, 2023.

Foto: Shutterstock

Kriminelle tar i bruk ny teknologi

Teknologiske nyvinninger har blitt rimeligere, tilgjengelig for folk flest og gir muligheter for effektivisering og utvikling av samfunnet. Teknologien benyttes også av de kriminelle til å effektivt oppdatere og målrette deres angrep der de kan oppnå profitt.

De skreddersydde bedrageriene bruker ofte avanserte tekniske løsninger. Økokrim erfarer at kriminelle bistår hverandre med kompetanse inkludert salg av programvare.

Etter hvert som samfunnet blir bedre på å beskytte seg mot de enkleste formene for bedrageri, forventer vi at de kriminelle vil ta i bruk mer avanserte metoder og teknologi. Ny teknologi skaper nye samhandlingsmønstre og nye muligheter, men den skaper også nye sårbarheter. Vi må ta dette på alvor og forberede næringslivet, befolkningen og offentlig sektor på at dette vil medføre store endringer i samfunnet generelt og kriminaliteten spesielt.

Kunstig intelligens og automatisering

Økokrim er bekymret for hvordan kriminelle vil øke bruken av kunstig intelligens i årene fremover. Flere avanserte maskinlæringsteknologier er lansert. De kan blant annet trenes til å imitere en persons uttrykksform og tilpasse skriftlige svar.

I en nær fremtid vil bedragere nyttiggjøre seg av KI med syntetiske stemmer og talegjenkjenning i sanntid. Systemet er selvlærende og trener seg opp til å lykkes i sine bedrageri ved å analysere data fra egne mislykkede forsøk samt suksesser. Systemet vil i tillegg kunne innhente data om fornærmede fra internett og tilgjengelige kilder i sanntid, og tilpasse kommunikasjon med offeret deretter.

Derfor genererer den svært troverdige samtaler med et menneske, også på andre språk. ChatGPT er ett slikt verktøy. Det er rapportert at bedragere har begynt å bruke dette, og at interessen blant kriminelle er økende.

Kunstig intelligens benyttes også i deepfaketeknologi. Dette gjør at bedragere kan forfalske video og stemme slik at de kan fremstå som en annen person. Bedragerne kan også ta i bruk automatisering i bedrageriforsøk, eksempelvis for å generere enkle svar på en melding.

I tillegg til at denne typen verktøy vil gjøre bedrageri mer troverdige, forventer vi en betydelig økning i antall bedrageriforsøk. Det teknologiske kappløpet mellom kriminelle aktører på den ene siden og politi og næringslivet på den andre vil være avgjørende for hvordan vi vil kunne håndtere denne utviklingen.

Grensekryssende betalingsløsninger

Det forventes at bruken av digitale tjenester vil øke i en digital økonomi.[11] Dette legger til rette for blant annet raske, grensekryssende og anonyme transaksjoner. Kriminelle aktører tar i bruk de nye tjenestene til å overføre utbytte fra bedrageri til utlandet.

Flere nye produkter og tjenester tar ikke i tilstrekkelig grad hensyn til krav om kundetiltak og transaksjonsovervåkning. Dette utfordrer banker og anti-hvitvaskingssystemet da de mister oversikt over hvilke personer som er del av transaksjonskjeden.[12]

11 European Commission, Supra-National Risk Assessment (SNRA), 2019.
12 DNB v/FC3, Annual Fraud Report 2022, 2023.

Mennesker er en sårbarhet

Bedrageri er en spesiell form for kriminalitet fordi det krever at offeret aktivt deltar i handlingen for at det skal lykkes. Manipulering av mennesker er nødvendig for å gjennomføre bedrageri og mennesker utgjør ofte den største sårbarheten i møte med bedragere. Den teknologiske sikkerheten forbedres stadig, noe som antas å være en av årsakene til at NorSIS rapporterer at de kriminelle har begynt å dreie angrepene mot ansatte fremfor IT-systemer.[13]

Sosial manipulering

Bedragere benytter ofte sosial manipulering. Det vil si at de utgir seg for å være noen andre enn den de egentlig er. De påvirker ofrene til å utføre en handling, gjerne ved bruk av virkemidler som spiller på følelser. Reelle hendelser i samfunnet blir ofte benyttet som agn for å skape troverdighet. Formålet kan være å få offeret til å gi fra seg sensitiv informasjon slik som digital identifikasjon. Dette kan i neste omgang benyttes for å få tilgang til en persons bankkontoer.

Sosial manipulasjon kan også være innledning til annen kriminalitet, som datakriminalitet, eller inngå i påvirkningsoperasjoner fra andre lands myndigheter. Informasjon stjålet for å utføre bedrageri kan også ha etterretningsverdi for statlige aktører.

Falske lenker, nettsider og oppringninger

For at mottakeren skal gi fra seg sensitive personopplysninger eller kortinformasjon sender bedragere ut falske lenker på SMS, e-post og i sosiale medier. Mange nye nettsider er falske og de opprettes raskere enn tjenesteleverandører klarer å ta de ned. De svært troverdige nettsidene kan eksempelvis gi inntrykk av å være en nettbutikk eller en handelsplattform for aksjer eller kryptovaluta. I realiteten er alt man ser fiksjon, og de kriminelle benytter de falske nettsidene til å tilegne seg personopplysninger og kortinformasjon for å bedra ofret.

Telefonoppringninger og datingapper er andre kanaler hvor bedragere bygger tillit hos sine ofre, gjerne over lengre tid.

Bedragere kartlegger mennesker digitalt

Alle mennesker og foretak i Norge legger igjen informasjon om seg selv på ulike digitale plattformer. Bedragere kartlegger enkeltpersoner eller virksomheter digitalt ved å samle inn data som deles i ulike sosiale medier, nettsider og offentlige registre. Økokrim forventer at bedragere vil automatisere innhenting og systematisering ved hjelp av KI og at informasjonen vil bli benyttet til å skreddersy bedrageri.

Eksempel på falsk melding på WhatsApp.

13 NorSIS, Trusler og trender, 2021.

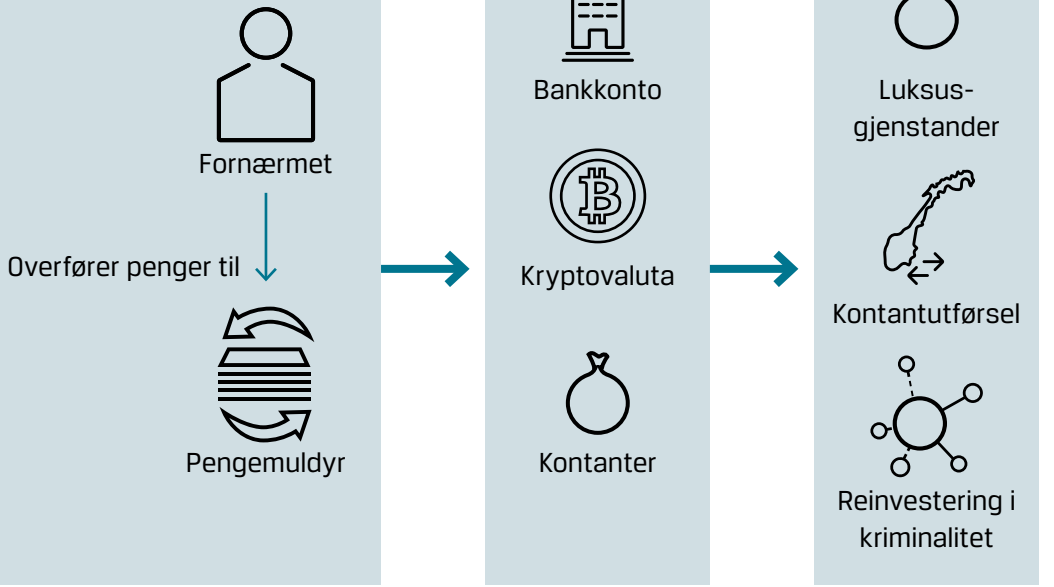
Foto: Maskot/NTB

Rekruttering av pengemuldyr

Bedragere ønsker å skjule sin tilknytning til utbytte fra bedrageri. Derfor rekrutterer de ofte personer som kan flytte penger for seg, også kalt pengemuldyr. Noen tilbys goder eller en annen form for betaling for dette.

I mange tilfeller fungerer bedrageriofrene også som pengemuldyr. Økokrim registrer videre at unge personer blir rekruttert, blant annet via jobbannonser. De blir «ansatt» i det som fremstår som en reell jobb og får deretter instrukser om å stille sin bankkonto til disposisjon. Ungdom helt ned i 13-14 års alderen rekrutteres også via vennegjenger på skole eller i idretten. I tillegg til å stille bankkontoen sin til disposisjon blir de ofte bedt om å ta ut penger fra bedrageri kontant, eller til å overføre penger raskt videre via ulike tjenester for straksbetaling.

Ungdommene virker i liten grad å forstå alvoret i handlingen, at de faktisk bistår kriminelle med å tilegne seg penger, og at de begår en kriminell handling med høy strafferamme.[14] Økokrim ser svært alvorlig på at kriminelle rekrutterer unge og sårbare mennesker til kriminalitet på denne måten.



Eksempler på konvertering av utbytte fra bedrageri

14 DNB, Trusler, trender og utviklingstrekk 2022 – Hvitvasking og terrorfinansiering, 2023.

Bedrageri utfordrer tilliten og sikkerheten i samfunnet

Tillit er fundamentalt for at et samfunn skal fungere. Generelt er tilliten høy i Norge.

Økningen i bedrageri utfordrer denne tilliten – både til teknologiske løsninger, i mellommenneskelige relasjoner og til myndigheter og viktige samfunnsinstitusjoner. Lav oppklaringsprosent kan allerede ha redusert privatpersoner og næringslivets tillit til politiets håndtering av bedrageri.[15]

Den eksplosive teknologiske utviklingen forventes å akselerere ytterligere i årene fremover. Det kan gi vedvarende utfordringer med å skille fakta fra fiksjon. Dette vil kriminelle utnytte, noe som kan svekke friksjonsfri samhandling mellom borgere, næringsliv og myndigheter. I ytterste konsekvens kan dette påvirke tilliten til demokratiet og demokratiske prosesser.

Digital identifisering

Sikker verifisering av brukeridentitet er en grunnleggende forutsetning for tillit i et digitalt samfunn. Per i dag benyttes samme digitale identifiseringsløsning for å få tilgang til en rekke digitale tjenester, både private og offentlige. For den enkelte er dette praktisk, men det medfører også en sårbarhet.

Kriminelle utfører phishing-angrep som ofte har som formål å få tilgang til en persons digitale identifikasjon. Økokrim registrerer at kriminelle utnytter dette til raskt å kartlegge ofrenes økonomi før de logger inn på deres nettbank og stjeler pengene.

Personopplysninger om nordmenn har også en kommersiell verdi, og er til salgs på ulike nettsider. Det er derfor viktig at alle tar digital sikkerhet på alvor fordi informasjonen kan bli benyttet som inngang til både alvorlig kriminalitet og påvirkningsoperasjoner fra andre stater uten sikkerhetssamarbeid med Norge.

15 POD, Politiets innbyggerundersøkelse 2022, 2023.

Foto: iStock

Kriminelle utnytter norsk åpenhetskultur

Økokrim erfarer at kriminelle benytter informasjon fra private og offentlige instanser til kriminelle formål. Dette gjør de kriminelle ved å observere endringer i eksempelvis offentlige registre.

Publisering av data, ofte i sanntid, gir bedragere mulighet til å bruke virkelige hendelser som en troverdig inngang til bedrageri. Det kan være selskapsendringer, kjøp og salg på digitale markedsplasser og informasjon om ofres økonomi.

Opplysninger i offentlige registre blir manipulert

Kriminelle utfordrer også det tillitsbaserte samfunnet ved å manipulere offentlige registre. Eksempelvis benyttes fiktivt ansatte i foretak for å få offentlige ytelser og uriktige inntektsdata i skattemeldingen for å muliggjøre lån på feilaktig grunnlag.

Det er vanskelig å skille bedragere fra statlige aktører

Grensene for hva som er kriminalitet og statlige aktørers virkemiddelbruk er uklare. I begge tilfellene utnyttes sårbarheter og mulighetsrommet i et tillitsbasert samfunn, og sosial manipulasjon benyttes som virkemiddel. Målet kan i begge tilfeller være økonomisk vinning.

Ondsinnede aktører kan ønske å skape mistillit og splittelse i samfunnet[16] og det som tilsynelatende er bedragerikampanjer kan være del av en sammensatt trussel. Det er eksempelvis observert flere phishing-kampanjer det siste året som bruker russisk infrastruktur/IP-adresser.

16 NSM, Risiko 2023, 2023.

Situasjonsforståelse og responsevne

For at politiet, andre offentlige og private aktører skal kunne forebygge bedrageri må det foreligge en omforent og tidsriktig situasjonsforståelse, som er basert på et godt kunnskapsgrunnlag.

For lite kunnskapsbygging og informasjonsdeling

Det er i dag få som anmelder bedrageri. Enkelte private foretak har god oversikt over bedrageri som rammer egne kunder. Politiet har frem til nå hatt lite fokus på kunnskapsbygging og har ikke en god nok innsikt i reelt omfang, hvilke fremgangsmåter som benyttes og hvor store økonomiske tap bedrageri medfører.

Det er videre lite samarbeid og informasjonsutveksling mellom offentlige etater og private aktører. Regelverket setter begrensninger for effektiv utnyttelse av digitale løsninger som kunne ha understøttet kriminalitetsbekjempelsen. Manglende muligheter for å dele informasjon mellom ulike sektorer i samfunnet utfordrer vår evne til å forebygge, avverge og etterforske bedrageri.

Internasjonale etterforskninger blir enda mer krevende

Det er ressurskrevende å etterforske digital grensekryssende kriminalitet. Regelverket for internasjonalt politisamarbeidet er i stor grad blitt til i en analog tid, myntet på analog kriminalitet. Kriminalitet i det digitale rom med tilpasningsdyktige internasjonale kriminelle blir derfor utfordrende. Økt konfliktnivå og polarisering kan også gjøre internasjonalt politisamarbeid vanskeligere.

Anbefalinger

Handlingsplan mot digitale bedrageri

Bedrageri utgjør allerede en betydelig samfunnstrussel og det forventes at antall bedrageriforsøk fremover vil øke. Politiets evne til å forebygge og bekjempe denne type kriminalitet alene er begrenset.

Myndighetene bør derfor i samarbeid med privat og offentlig sektor utvikle en handlingsplan som ser på bekjempelse av digitale bedrageri i Norge i en bred kontekst. Handlingsplanen bør definere tydelige tiltak som setter privatpersoner og privat- og offentlig sektor i stand til å forebygge bedrageri og straffeforfølge bedragere. Tiltakene bør fokusere på teknologiutvikling, legge til rette juridisk for informasjonsdeling og bygge kapasitet og kompetanse til å håndtere den økende mengden digitale bedrageri.

Regelverk må oppdateres

En forutsetning for å kunne bekjempe digital kriminalitet er at lover og regelverk blir oppdatert i takt med teknologi- og kriminalitetsutviklingen. Myndighetene bør derfor legge til rette for en kontinuerlig utvikling av regelverket.

Regelverket i dag muliggjør eksemelvis ikke deling av informasjon i sanntid på tvers av sektorer og analyse av stordata. Det er også behov for å effektivisere internasjonalt politisamarbeid, da mange bedragere befinner seg i utlandet.

Fokus på teknologi- og fremtidig utvikling

De kriminelle tar raskt i bruk ny teknologi – det må også politiet og andre offentlige og private aktører gjøre.

Det er viktig at myndighetene og næringslivet investerer i teknologiske løsninger som understøtter offentlig-privat samhandling og deling av informasjon. Utvikling og utnytting av teknologi for å monitorere og analysere store datamengder er en forutsetning for å raskt kunne varsle og respondere på nye modus.

Det bør benyttes ulike flerfaktor-autentiseringsmetoder[17] for å gjøre det vanskeligere for kriminelle å både identifisere seg som en annen person og å få tilgang til ulike tjenester slik som bank, skatt- og avgiftsregister.

Autentiseringen må også skje på en måte som reduserer risikoen for at uvedkommende kan plassere seg mellom bruker og tjeneste. Det hjelper lite med flerfaktor-autentisering dersom en bedrager kan spørre en bruker om passord og kode fra kodebrikken og misbruke dette umiddelbart.

Det er også behov for å utdanne fagpersonell med høy kompetanse innenfor IT-sikkerhet, teknologi og nye betalingsformer. Disse bør utdannes til bruk av datastyrte algoritmer, kunstig intelligens og andre tekniske verktøy slik at de kan utvikle sikkerhetssystemer som kan beskytte mot ulike former for bedrageri.

Politiet må prioritere bedrageri høyere

Antall bedrageri er høyt og forventes å øke. Politiet bør evne å se saker i sammenheng, øke oppklaringsprosenten og ivareta ofre for bedrageri på en bedre måte.

Bedrageri bør kunne anmeldes digitalt. Politiet bør også utvikle rutiner som legger til rette for en styrket samhandling med privatpersoner og næringslivet. Politiet må prioritere å behandle og analysere informasjonen de mottar for å etablere et bedre kunnskapsgrunnlag.

Arbeidet med forebygging må styrkes

Det er viktig å utvikle robusthet og motstandskraft i samfunnets digitale infrastruktur, virksomheter og befolkningen for øvrig for å beskytte befolkningen mot bedrageri.

Bedrageri kan bekjempes ved å tette sårbarheter i eksisterende infrastruktur. Flere bedragere utnytter svakheter i telenettet, benytter offentlig tilgjengelig informasjon, raske grensekryssende pengeoverføringer og annen teknologi. Det er mulig å stoppe spoofede telefonsamtaler og mistenkelige transaksjoner, ta ned falske internettsider og forsinke offentliggjøring av informasjon.

Det er også viktig at befolkningen gis kunnskap og verktøy til å beskytte seg selv mot bedragere, for eksempel gjennom utdanning, kommunikasjon og veiledning.

17 Metode for brukerautentisering hvor en bruker kun gis adgang etter å ha presentert to eller flere separate bevis for sin brukeridentitet. Det det er vanlig å kreve at disse bevisene kommer fra forskjellige grupper av de tre følgende: noe en vet (kunnskap), noe en besitter (nøkkel av noe slag) eller noe en er (fingeravtrykkleser, ansikt, netthinnen eller stemmegjenkjenning osv.).

ØKOKRIM

Postadresse: Pb. 2096 Vika, NO-0125 Oslo
Besøksadresse: C.J. Hambros plass 2 C, NO-0164 Oslo
Kontakt: 23 29 10 00 / post.okokrim@politiet.no

www.okokrim.no

Foto fremside: Unsplash/Yngve Windsland og Shutterstock