



ØKOKRIM

< 106



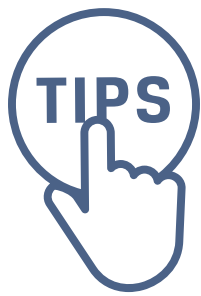
Tekstmelding
I dag 13:56

Det er problemer med bankkontoen din. Logg inn for å løse problemet. Hilsen banken din kor.tt/url

Temarapport

april 2023

Bedragere som utgir seg for å være politi- eller bankansatt



Tips oss om bedrageri
www.okokrim.no/tips

Innhold

Hovedpunkter.....	4
Eldre kvinner bedras	5
Hvordan går de kriminelle frem?.....	6
Norske kriminelle nettverk og aktører står bak bedrageriene	7
Rekruttering av pengemuldyr	8
Hvordan unngå å bli bedratt.....	9

Hovedpunkter

- Politiet registrerte i 2022 en økning i bedragerier hvor gjerningspersonene utgir seg for å være politi- bankansatt.
- Flere av de kriminelle aktørene som står bak denne typen bedrageri kan knyttes til annen alvorlig kriminalitet slik som grov vold, trusler, narkotika og hvitvasking.
- Gjerningspersonene bruker et stort antall pengemuldyr. Pengemuldyrene er ofte unge og/ eller sårbare mennesker som ikke forstår hva de bidrar til eller alvoret i handlingen. Det er rapportert at pengemuldyr har utført sin rolle under tvang, etter å ha blitt truet av bedragerne.
- I gjennomsnitt taper ofrene rundt 200 000 kroner, men det er rapportert om enkelttilfeller med tap på over 1 million kroner.
- Enkelte bedrageriofre har vært redde for å ha kontakt med politiet i etterforskningen av saker, av frykt for å bli bedratt på nytt. Det er en bekymring at enkeltpersoner kan få redusert tillit til politiet som følge av bedrageriene.



Eldre kvinner bedras

Politiet registrerte i 2022 en økning av bedragerier hvor gjerningspersonene utgir seg for å være politi- eller bankansatt.

Det er hovedsakelig kvinner i pensjonsalder som bedras og det gjennomsnittlige tapet i hvert bedrageri er på ca. 200 000 kroner. I noen tilfeller har offeret blitt bedratt for over 1 million kroner. Bedrageri der gjerningspersonen utgir seg for å være politi eller bank genererer et stort økonomisk utbytte til kriminelle aktører.

I september 2022 slo Høyesterett fast i dom at banker har ansvaret for å bære det økonomiske tapet fra BankID-bedragerier.¹ Økokrim sitt inntrykk er at bankene i de fleste tilfeller dekket tapet til den fornærmede.

Enkelte bedrageriofre har vært redde for å ha kontakt med politiet i etterforskningen av saker, av frykt for å bli bedratt på nytt. Bedragerne utnytter tilliten ofrene har til politiet og finansinstitusjoner, og det er en bekymring at enkeltpersoner kan få redusert tillit til politiet som følge av bedrageriene.

¹ Høyesteretts dom 13. september 2022, HR-2022-1752-A, (sak nr. 22-025299SIV-HRET).



Hvordan går de kriminelle frem?

Bedragerne ringer personer og utgir seg for å være ansatt i politiet eller banker. De snakker oftest godt norsk og oppgir en plausibel forklaring på hvorfor de ringer. Forklaringen kan være at noen har tatt opp et lån i navnet til den som blir oppringt og at det må ordnes opp i. Den kriminelle handlingen maskeres på denne måten som et tilbud om å hjelpe fornærmede.

Ofrene manipuleres i lange telefonsamtaler. Det finnes eksempler på samtaler som har pågått i mer enn fem timer og samtaler som har pågått over flere dager. De fornærmede blir i løpet av samtalene forledet til å gi fra seg personopplysninger, kortinformasjon og engangskoder. Informasjonen utnyttes av de kriminelle til å tilegne seg adgang til offerets bankkonto som oftest raskt blir tømt for midler.

Bedragerne benytter seg av spoofing, noe som i praksis betyr at bedragerene selv velger hvilket nummer det skal se ut som om de ringer fra. Samtalen kan derfor se ut som den kommer fra et pålitelig norsk nummer, noe som vekker mer tillit enn ukjente utenlandske nummer. Bedragerne benytter seg av programvare og tjenester hvor de selv oppgir hvilket nummer som skal vises på displayet til den som blir oppringt.

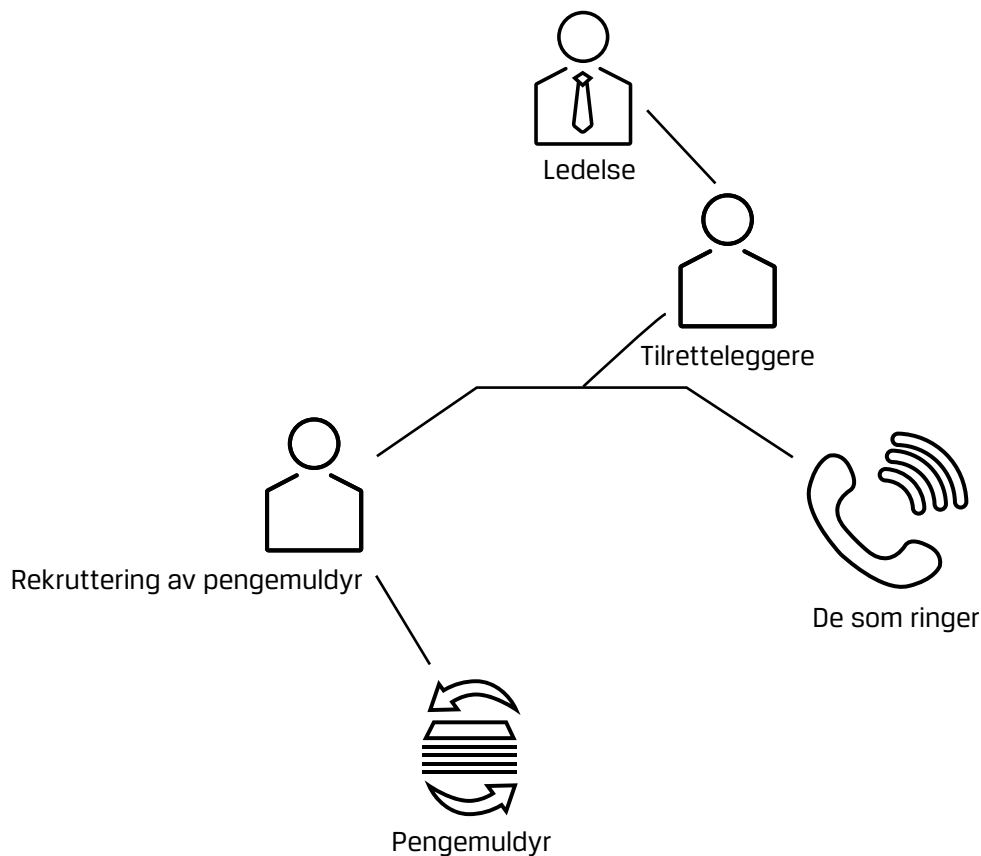
Norske kriminelle nettverk og aktører står bak bedrageriene

Flere nettverk og enkeltaktører kan knyttes til nettbankbedrageri der gjerningspersonen utgir seg for å være politi- eller bankansatt. Aktørene er hovedsakelig norske, men samarbeider også med aktører utenfor Norge.

Gjennomføringen av denne typen bedrageri krever mange personer, kommunikasjon, koordinering og logistikk. Gjennomføringen av bedrageriene er relativt lik uavhengig av hvilket nettverk som står bak.

Enkelte sentrale aktører er involvert i narkotikakriminalitet og andre typer bedrageri og voldskriminalitet.

Flere aktører opparbeider seg kapital og kompetanse som kan benyttes til videre kriminell virksomhet. Økonomisk utbytte fra bedrageri og narkotikakriminalitet fremstår å være aktørenes viktigste inntektskilder.



Rekruttering av pengemuldyr

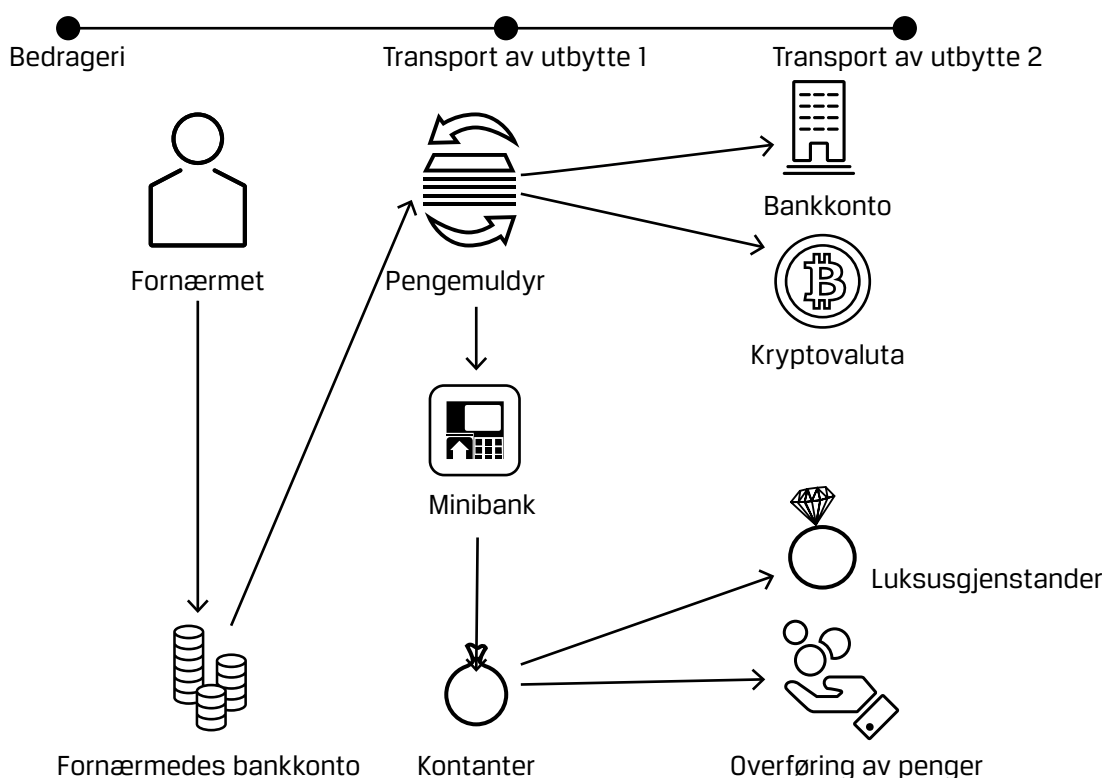
Pengemuldyr har en sentral rolle i flytting av utbytte fra bedrageriene, og bistår kriminelle ved at de mottar ulovlig ervervede penger på egne konti, for deretter å flytte disse videre. Pengene blir i mange tilfeller tatt ut i kontanter via minibanker eller overført til internasjonale digitale banktjenester. I mange saker blir deler av utbyttet overført videre til plattformer for kryptovaluta. Overføringer til utenlandske betalingstjenester og kryptovaluta vanskeliggjør sporingen av utbyttet. Det finnes også eksempler på at pengemuldyr blir instruert til å kjøpe gavekort, dyre klokker og andre luksusgjenstander, ofte med kontanter.

Pengemuldyrene rekrutteres til rollen av tilretteleggere på flere måter. I mange tilfeller opprettes det kontakt via sosiale medier. Ofte blir de tilbudt goder eller en annen form for betaling for å flytte penger. Pengemuldyrene fremstår selv i mange tilfeller å ikke ha en klar forståelse for egen deltakelse i kriminaliteten og hvitvaskingshandlingen de utfører.

Enkelte av de kriminelle bakmennene har rekruttert sårbare personer, og i flere tilfeller har personer også blitt truet og tvunget inn i rollen som pengemuldyr.

Pengemuldyrene blir også rekruttert gjennom bekjenskaper som har kontakt med kriminelle miljøer, mens andre muldyr fremstår som selv å være involvert i kriminell virksomhet.

Pengemuldyr benyttes ofte kun til ett bedrageri, noe som skyldes at pengemuldyrets bank etter kort eller lang tid ofte vil stille spørsmål ved den unormale aktiviteten på kontoen og sperre den for videre bruk. Slik blir pengemuldyr en forbruksvare for de kriminelle aktørene.



Hvordan unngå å bli bedratt

1. Ikke gi fra deg sensitiv informasjon til personer og firmaer som henvender seg til deg per telefon eller e-post. Eksempler på sensitiv informasjon kan være:
 - personopplysninger
 - konto- og kredittkortinformasjon
 - passord
 - pinkoder
2. Logg alltid på nettbank og offentlige sider ved å gå til deres hjemmeside, ikke følg lenker du får tilsendt.
3. Hvis noen prøver å stresse deg, slik at du må ta raske avgjørelser om avtaler og betalinger – avbryt kontakten.

Er du i tvil om du har mottatt melding fra politiet, banken eller en annen offentlig instans, kontakt den angivelige avsenderen direkte.

Ta kontakt med banken din eller ditt lokale politi dersom du er usikker på om du er utsatt for bedrageriforsøk.

