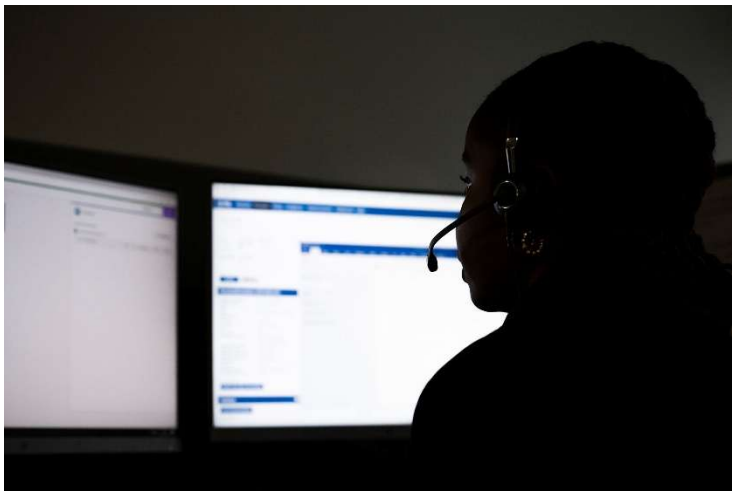
A791.657/2025

Analys av befogenhets-bedrägerier

Ärenden som inkommit till polisområde Östergötland
år 2024 från1 januari till sista veckan i april

Utkast, ver 2.0



Stefan Holgersson

BF-samordnare

Polisområde Östergötland

Innehållsförteckning

1. Analys av befogenhetsbedrägerier

1.1 Felkodning och försöksbrott

Brottsförebyggande rådet definierar befogenhetsbedrägerier i sin skrift om klassificering av brott som:

> *”Gärningspersonen kontaktar en person/organisation/ett företag och utger sig för att ha befogenheter, t.ex. utger sig för att vara ekonomichef på det utsatta företaget, eller banktjänsteman på den utsattes bank, och därigenom förmår den kontaktade till handling som ger ekonomisk vinning till gärningspersonen. Exempelvis s.k. VD-bedrägeri och vishing.”*[1]

Av 100 slumpmässigt utvalda ärenden som brottskodats som befogenhetsbedrägeri var det 16 procent (16 fall) som skulle ha kodats som en annan typ av bedrägeribrott. Exempelvis skulle två ärenden ha kodats som kortbedrägerier då målsäganden klickat på en länk och fyllt i kortuppgifter, ett skulle ha kodats som identitetsbedrägeri (så kallat kreditbedrägeri) där ett företag lurats att skickade 11 pallar med sockor, två fall rörde sig om social manipulation av annan typ (än bl.a. befogenhetsbedrägerier) där målsäganden fått ett sms om att deras barn bytt telefon och lurats att Swishat pengar och ett skulle ha kodats som annonsbedrägeri då en person sett en annons på Facebook om försäljning av en bil och sedan blev lurad att betala förskott på bilen. Dessutom är det i 17 procent av ärendena (17 fall) där det inte är uppenbart att det rör sig om en felkodning, men att det går att ifrågasätta om det är var rätt att koda brottet som ett befogenhetsbedrägeri. Att dessa tveksamheter uppstår är kopplat till att det finns en överlappning i definitionerna av flera av brottskoderna för bedrägeribrott i kombination med att försöksbrott och fullbordade brott inte särskiljs i brottskodningen.

Ett exempel på denna problematik är att det finns en brottskod för kortbedrägeri som definieras som att någon olovligen använt annans bankkort, betalkort eller kreditkort. I denna brottskod ingår brott där någon gärningsperson kommit över kortuppgifter där kortdata använts eller försökt användas i den olovliga transaktionen. Om de kortuppgifter som använts har kommits över genom social manipulation ska då brottet kodas som social manipulation (såsom befogenhetsbedrägeri) eller som ett kortbedrägeri? Ett annat exempel är att det i definitionen för annonsbedrägeri anges att ett sådan brott även kan ske genom att gärningspersonen agerar som en intresserad köpare till det som erbjuds via en annons i syfte att komma över pengar från säljaren. Vad går gränsen för att ett sådant brott ska kodas som social manipulation eller ett annonsbedrägeri? Likaså när någon ger sken av att vara någon annan person än den egentligen är och lyckas eller försöker lura till sig pengar ska det kodas som ett identitetsbedrägeri eller social manipulation?

Sammanfattningsvis har 33 procent av de anmälda befogenhetsbedrägerierna en felaktig brottskod eller en brottskod som det går att ifrågasätta om den är korrekt.

Att ange korrekta brottskoder blir särskilt utmanande när anmälan innehåller sparsamt med information och när det rör sig om ett försöksbrott där modus för det kontaktsökande som sker kan vara liknande för olika typer av brottskoder. I och med att processen avbrutits kan

[1] https://bra.se/download/18.73ed0f241939545744f1974e/1734442788353/2024_Klassificering%20av%20brott%20v%2013_0.pdf sidan 74.

det därmed vara svårt att veta vad gärningsmannen hade tänkt sig för tillvägagångssätt. Om det hade anmälts enstaka försöksbrott hade det varit ett mindre problem, men av diagram 3 framgår at drygt 4 av 5 anmälda befogenhetsbrott handlar om ett försökbrott och inte ett fullbordat brott. Vidare går det att utgå från att en försvinnande liten andel av försöksbrotten anmäls. Av samtal och egna iakttagelser framgår att både företag och privatpersoner överöses av kontaktförsök som utgör olika former av försök till bedrägerier som inte anmäls.

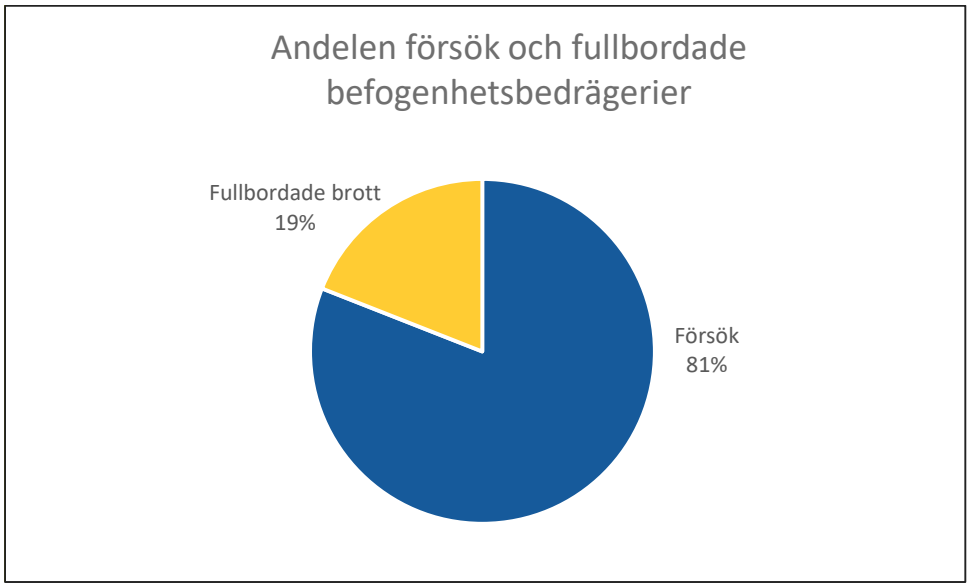


Diagram 1. Hur stor andel av de anmälda befogenhetsbedrägerierna som var försöksbrott respektive fullbordade brott (n=84)[2]

Av Brå:s statistik framgår att under år 2023 anmäldes 12 312 befogenhetsbedrägerier[3]. Om vi antar att 81 procent av dessa var försöksbrott och 6 procent av de fullbordade brotten var felkodade[4] så betyder det att det under år 2023 anmälts 1 600 brott som rör sig om befogenhetsbedrägerier där en målsägande förlorat pengar.

I stort sett alla fullbordade befogenhetsbedrägerier som analyserades handlade om så kallad vishing, ”*där brottsoffren kontaktas via telefon och blev lurade att göra en transaktion eller lämnade ifrån sig uppgifter som möjliggjorde för bedragarna att göra en transaktion*”. Denna definition på vishing är hämtad från Brå[5] som skiljer sig från Polismyndighetens definition som används i rapporten om brottsvinster av bedrägeribrottslighet. Där definieras vishing som att de uppringda personerna: ”*manipuleras att lämna ifrån sig sina inloggningsuppgifter eller uppmanats att använda sitt Bank–ID och därefter föra över pengarna till ett annat konto*.”[6]. Definitionen är mer detaljrik och smalare än Brå:s definition. Som det utrycks är det tveksamt om utlämningen i av kontouppgifter ingår i definitionen – liksom Swishöverföringar. I en annan definition på vishing som Polismyndigheten presenterar på sin hemsida inkluderas

[2] De ärenden som är felkodade exkluderas i redovisningen (11 fall), men de ärende där det inte är klart om fel brottskod angivits inkluderas.

[3] https://bra.se/amnen/bedrageri [2025-02-02]

[4] Som var fallet vid den analys som gjordes inom ramen för denna rapport.

[5] https://bra.se/download/18.3808406a192bd2f0b727c8f/1730736409029/2023_11_Bedragerier-mot-privatpersoner.pdf

[6] https://polisen.se/siteassets/dokument/ovriga_rapporter/brottsvinsterna-for-bedrageribrottsligheten-2023.pdf, sidan 13

dock utlämnade av kontouppgifter i vishing[7]. Problematiken att det finns skillnaden vad som ingår i olika begrepp kan kopplas till ett tidigare påpekat behov avseende en förändrad klassificering av bedrägeribrott.

1.2 Den ekonomiska omfattningen av befogenhetsbedrägerier

Intervallet på belopp i ärendena om befogenhetsbedrägerier som inkommit till polisområde Östergötland i början av år 2024 låg mellan 6200 kronor och 300 000 kronor. Medelvärdet var 44 000 kronor och medianvärdet 15 000 kronor. I rapporten om uppskattade brottsvinster vid bedrägeribrottslighet som Polismyndigheten publicerat anges inte uppskattade brottsvinster för brottstypen befogenhetsbedrägerier. Det finns en redovisning av Vishingbedrägerier som delvis ingår i befogenhetshetsbedrägerierna, men som även inkluderar fysisk Vishing som innebär att en gärningsperson uppmanar ett brottsoffer att ta fram alla sina smycken, kontanter och bankkort och sedan besöker offrets bostad och tar med sig godset. Polismyndigheten anger att Vishing–bedrägerier är den näst största inkomstkällan för kriminella aktörer och brottsvinsten var 708 miljoner kronor år 2023[8] och 425 miljoner kronor år 2024[9]. Högsta fullbordade summan för vishingbedrägerier år 2023 var 16 miljoner kronor och det fanns 83 ärenden där brottsvinsten översteg 1 miljon kronor och för år 2024 var det 35 ärenden som översteg 1 miljon kronor.

I Brå:s definition av befogenhetsbedrägerier ingår även bland annat så kallade VD-bedrägerier. Polismyndigheten redovisar VD-bedrägerier separat (BEC) i sin rapport om brottsvinster av bedrägerier, där VD-bedrägerierna enligt den definition som anges begränsar sig till då konversationen skett genom e-post. Brottsvinsten för BEC-bedrägerier år 2023 var 329 miljoner kronor[10] och 242 miljoner kronor år 2024[11]. En anmälan år 2023 omfattande en brottsvinst på 80 miljoner kronor och en annan på 57 miljoner kronor. Det var 29 andra anmälningar i intervallet mellan 1 och 10 miljoner kronor. Mellan år 2023 och år 2024 blev fler företag utsatta för bedrägerier där de betalade mer än en miljon kronor (13 företag 2024 och 4 företag 2024)[12].

Sammanfattningsvis är befogenhetsbedrägerier en av de bedrägerityper som genererar störst brottsvinster.

1.3 Befogenhetsbedrägerier klaras sällan upp men penningtvättare lagförs

Ingen av de befogenhetsbedrägerier som inkom till polisområde Östergötland har lett till att någon lagförts för denna brottstyp utan för penningtvättbrott. Av diagram 4 framgår att av de anmälda befogenhetsbedrägerier som inkom till polisområde Östergötland har cirka 6

[7] https://polisen.se/utsatt-for-brott/polisanmalan/bedrageri/bedragerier/telefonbedrageri/

[8] https://polisen.se/siteassets/dokument/ovriga_rapporter/brottsvinsterna-for-bedrageribrottslighet-2023.pdf

[9] Polismyndigheten (2024). *Brottsvinsterna för bedrägeribrottslighet 2024*.

[10] https://polisen.se/siteassets/dokument/ovriga_rapporter/brottsvinsterna-for-bedrageribrottslighet-2023.pdf

[11] Polismyndigheten (2024). *Brottsvinsterna för bedrägeribrottslighet 2024*.

[12] Polismyndigheten (2024). *Brottsvinsterna för bedrägeribrottslighet 2024*. Om man jämför siffrorna gällande år 2023 i rapporten från år 2023 och år 2024 ger dessa intrycket av att vara olika då det i rapporten för år 2023 år verkar vara fler företag som blivit lurade.

procent (5 fall) redovisats till åklagare. 4 procent (3 fall) är fortfarande öppna och 90 procent av ärendena har lagts ned.

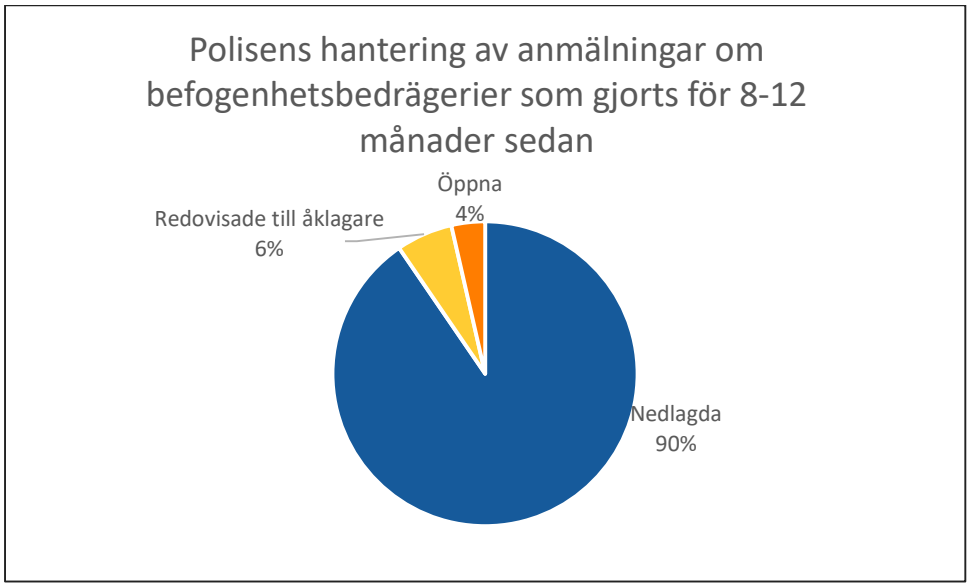


Diagram 2. Polisområde Östergötlands hantering av anmälningar om befogenhetsbedrägerier som gjorts för 8-12 månader sedan (n=84)

Om man bara ser till de fullbordade befogenhetsbedrägerierna har en tredjedel av dem redovisats till åklagare. I samtliga fall handlade det om penningtvättbrott med en annan brottskod än befogenhetsbedrägeri, men i statistiken kommer ärendet redovisas som ett uppklarat befogenhetsbedrägeri. Tre ärenden är fortfarande öppna där utredningarna är inriktade på att lagföra personer för penningtvättbrott. Prognosen är god för att dessa ärenden ska kunna redovisas till åklagare. Om antagandena är riktiga betyder att drygt femtio procent av de fullbordade befogenhetsbedrägerier som anmäldes till Polisområde Östergötland i början av 2024 redovisa till åklagare – då i form av penningtvättbrott.

I 84 procent av de ärenden som lades ned angavs som skäl att ”*Uppenbart att brott ej går att utreda*”. Åtta procent av ärendena (sju fall) som hade ett liknande underlag lades ned av andra skäl och sex procent lades ned för att misstänkt hade blivit dömd för eller skulle åtalas för annan brottslighet som gjorde att det fanns skäl för åtalsunderlåtelse. I fyra av dessa fem fall förelåg tydligt dessa förutsättningar, men nedläggningen av ett av fallen går att ifrågasätta eftersom det enbart handlade om ett penningtvättbrott – samma brott som personen var misstänkt för i det fall som lades ned.

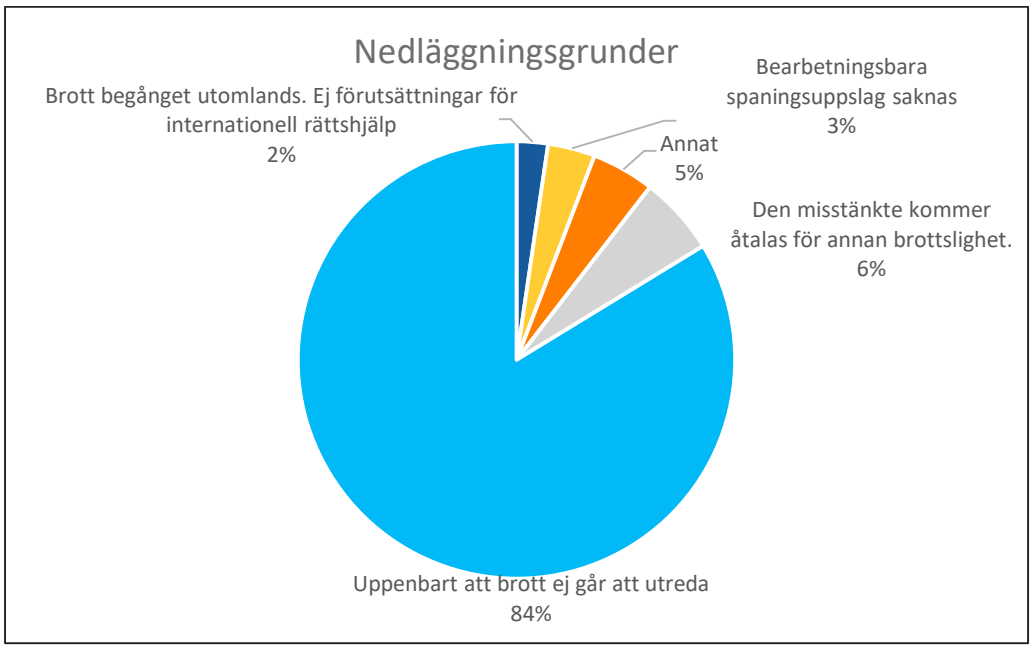


Diagram 3. Nedläggningsgrunder när det gäller befogenhetsbedrägeri i polisområde Östergötland av de ärenden som kom in de första fyra månaderna år 2024 (n=76).

Samtliga försöksbrott har lagts ned och det verkar göras per automatik eftersom förutsättningarna bedöms som små för att kunna lagföra någon för dessa brott. I och med att det inte skett någon förmögenhetsöverföring saknas möjligheten att lagföra någon för penningtvättbrott. När det gäller att hushålla med polisens utredningsresurser är det rationellt att lägga ned dessa brott omgående utan att vidta några utredningsåtgärder, men inte ur en brottsförebyggande aspekt. Som tidigare påpekas har den brottsförebyggande verksamheten ett litet utrymme i polisområde Östergötland och det gäller inte minst inom utredningsverksamheten, vilket kan kopplas till vad som mäts. Polisområde Östergötland är inte unika i det sammanhanget[13].

De som lägger ner tid på att göra anmälningar om försöksbrott kan tänkas göra detta på grund av att det finns en förhoppning om att polisen ska dra nytta av denna information för att kunna förhindra och försvåra situationen för de gärningsmän som försökt lura målsägandena. En sådan förväntan kan ses som rimlig, men polisen drar inte nytta av dessa möjligheter. För att angripa befogenhetsbedrägerierna finns ett behov av att polisen anammar ett annat förhållningssätt.

Vid en genomgång av anmälningarna framgår att det finns svenska telefonnummer som börjar på 031, 08 och 040 som är återkommande telefonnummer i befogenhetsbedrägerierna som innefattar vishing. En sökning på telefonnummer som figurerar i anmälningarna visar att det skett många sökningar på dessa och att det har skrivits varningar om att det är telefonnummer kopplade till bedrägeri. Ett telefonnummer har det exempelvis gjorts sökningar på 1147 gånger. Ett annat 296 gånger. Sökningarna fortgår på vissa telefonnummer som anges i de analyserade ärendena. När detta kapitel skrevs i januari 2025 hade det exempelvis gjorts 46 sökningar på ett telefonnummer de senaste tre månaderna som förekom i bedrägeriärendena som anmälts för ett år sedan.

[13] Framkommit vid samtal med personal från andra regioner och polisområden.

Flera, sannolikt fiktiva namn, återkommer i ärendena om befogenhetsbedrägerier i form av vishing. Ett sådant namn är exempelvis ”*Erik Nilsson*” som uppger sig arbeta på Inkasso Göteborg. En sökning med orden ”*Erik Nilsson inkasso*” ger en träff på en artikel i tidningen Smålänningen[14] som publicerades 30 augusti 2023. Det vill säga ett halvår innan detta namn figurerar i de anmälningar som analyseras i denna rapport. I mediaartikeln i Smålänningen framgår att flera äldre personer under samma dag fick ett samtal som inleddes med: ”*Jag heter Erik Nilsson och ringer från ett inkassobolag i Västerås.*”. Sökningen med orden ”*Erik Nilsson inkasso*” gav också en träff på ett telefonnummer (031-7859472) på Hitta.se som det gjorts 166 sökningar på och med 44 rapporter om bedrägeri. Sökningar på numret är gjorda framförallt i Stockholm, Göteborg och Malmö. Operatören för detta telefonnummer är Tele2. Den första användarkommentaren på telefonnumret på hitta.se gjordes i början av januari 2024 och det står att: ”*Presenterade sig som Erik Nilsson från Inkasso i Göteborg*”. Just detta telefonnummer verkar inte för närvarande vara aktivt i bedrägeriärenden och den sista sökningen på detta telefonnummer gjordes i juli 2024.

För en utredare kan det i efterhand vara hopplöst att med de uppgifter som finns i ett ärende försöka komma fram till vilka som är gärningsmän bakom befogenhetsbedrägerier och exempelvis använder sig av namnet ”*Erik Nilsson*”. Det är med nuvarande inriktning naturligt att ärendena läggs ned, men med en brottsförebyggande strävan ska det inte vara ett ensidigt fokus på att lösa inkomna ärenden utan att förhindra nya bedrägerier.

Av anmälningar framgår att det anges nummer som gärningsmännen vill att de presumtiva offren ska ringa på. Dessa nummer går att nyttja för att komma i kontakt med gärningsmännen. Vid kontakt med gärningsmännen går det genom tekniska och fysiska åtgärder identifiera vilka gärningsmännen är, lokalisera var de befinner sig och därefter genomföra tvångsåtgärder mot dem där telefoner och datorer tas i beslag och analyseras. Det krävs en nationell koordinering för detta arbetssätt så att inte olika polisområden arbetar mot samma telefonnummer och gärningsmän. Förutom att det sker aktiviteter för att om möjligt slå ut dessa individers möjlighet att ägna sig åt befogenhetsbedrägeri går det också att iscensätta aktiviteter för att försvåra befogenhetbedrägerierna genom bland annat ta kontakt med telefonoperatör gällande telefonnummer som upprepade gånger figurerar i anmälningar.

Ett proaktivt agerande där inkomna anmälningar omedelbart används för ett kartläggningsarbete och förebyggande åtgärder bedöms ha en stor potential att hindra och försvåra befogenhetsbedrägerier genom så kallad vishing. I drygt en tredjedel av ärendena fanns det telefonnummer som använts av bedragarna. Som tidigare påpekats går det att säkerställa att kvaliteten på de inkomna anmälningarna ökade som skulle innebära att det inte behövdes vidtas några utredningsåtgärder för att få tillgång till fler telefonnummer som skulle underlätta ett brottsförebyggande arbete.

1.4 Gärningsmän och modus

Avsaknad av utredningsåtgärder och information begränsade möjligheten att inom ramen för denna rapport analysera gärningsmännen som ägnar sig åt befogenhetsbedrägerier, men det finns uppgifter om 13 personer i de ärenden som ingått i analysen som genom penningtvätt möjliggjort befogenhetsbedrägerier i form av vishing. Median och medelåldern på dessa personer var 38 år. Den yngsta personen var 17 år och den äldste 72 år.

[14] https://www.smalanningen.se/artikel/bedragare-i-farten-polisen-varnar-sa-ledsamt/

Ungefär hälften (53 %) av personerna hade utländsk bakgrund[15] och nästan alla var män (11 av 13). Samtliga förekom i misstanke och/eller brottsregistret för andra brott än de ärenden som analyserades:

- Fem av dem förekom bara i misstankeregistret och då för andra penningtvättbrott (eller grovt penningtvättbrott). De hade tidigare inte blivit dömda för några brott – inte ens ett trafikbrott.
- Tre förekom både i misstanke och brottsregistret. En av dessa går att beteckna som en missbrukare och har blivit dömd för upprepade narkotikabrott, men även grov misshandel. En annan ägnade sig åt grov kriminalitet och var misstänkt för eller hade blivit dömd för rån, utpressning, övergrepp i rättssak, grovt rattfylleri, vållande till kroppsskada m.m. En person var misstänkt för annan grov brottslighet kopplad till penningtvätt.
- Fem förekom inte i misstankeregistret (utöver de brott som ingick i analysen) utan enbart i brottsregistret. Förutom att en av dessa personer hade blivit dömd för grov misshandel var det mestadels brott med ett lågt straffvärde såsom skadegörelse, penningtvättbrott, stöld och ordningsföreläggande för trafikbrott.

Befogenhetsbedrägerier genom vishing skulle kunna försvåras om man agerar snabbt mot de som är penningtvättare och även försökte frysa/säkra pengar som målsäganden blivit av med. Det finns lovande initiativ som genomförts i landet som inneburit att åtgärder vidtagits omgående i ärenden istället för att dessa blev liggande utan åtgärd[16]. I analysen av annonsbedrägerier som presenteras i en särskild rapport beskrevs att om transaktionen skett via Swish skulle ett effektivt, men begränsat ingrepp vara att ta bort deras möjlighet att ta emot Swishbetalningar. Precis som vid annonsbedrägerier kunde det i ett senare skede vara aktuellt att ta bort deras BankID. Av vad som framgår av ärendena är det troligt att vissa av penningtvättarna är de som även lurat målsäganden, men att det är svårt att styrka i efterhand.

Befogenhetsbedrägerier genom vishing skiljer sig mycket från befogenhetsbedrägerier genom så kallade VD-bedrägerier – ändå har de samma brottskod. Det var bara ett fåtal av de anmälda befogenhetsbedrägerierna som inte skett genom vishing så en statistisk redovisning av VD-bedrägerierna är därför inte meningsfullt att göra inom ramen för denna rapport[17]. Det finns dock innan den statistiska analysen av befogenhetsbedrägerier genom vishing presenteras att beskriva VD-bedrägerier som inhämtas genom samtal med personer med en kunskap om denna typ av bedrägerier.

Vid VD-bedrägerier som även kallas BEC (Business email compromise) handlar det ofta om att en bedragare skickar ett mejl i syfte att lura en anställd på ett företag att överföra pengar. Bedragarna kan ha kartlagt företaget via social manipulation och identifierat vem som är chef och när denna är på semester eller tjänsteresa, vilka som är ansvariga för utbetalningar och rutiner i företaget. Vid ett genomtänkt tillfälle skickas ett kortfattat mail till utvald person och ber denna genomföra en viktig och brådskande utlandsutbetalning. Mailet ser ut att komma från vd, med korrekt eller liknande e-postadress (om man svarar på mejl går det

[15] Utifrån bland annat namn.

[16] Bland annat vid ett pilotprojekt som genomfördes på PKC i region Väst de sista månaderna under år 2024 där drygt 600 000 kr kunde återföras/frysas/spärras/tas i beslag.

[17] För att få ett större underlag vad gäller VD-bedrägerier studerades de befogenhetsbedrägerier som inkom under juli-september år 2024 (22 st) eftersom det antogs att förekomsten av VD-bedrägerier kunde skilja sig åt under denna period jämfört med andra perioder. Under denna period inkom dock inget sådant ärende.

dock att se att adressen är felaktig). Det behöver inte vara chefen som tar kontakt utan det kan vara en samarbetspartner som bygger upp en konversation och begär en överföring som sker till ett ändrat konto. Bedragaren kan även genom att planterat in skadlig kod skicka ett mejl i någon leverantör eller samarbetspartners namn med information om att kontouppgifter för kommande transaktioner ska ändras.

VD-bedrägerierna kan också genomföras genom djupa kartläggningar av företag, dess samarbetspartner, bankkontakter etc. Kontakt via telefon kan ske för att stressa på och påskynda överföringarna, där bedragarna i vissa fall kan ha kunskaper om äkta utbetalningar, men att den påstådda chefen ger instruktioner om ett nytt mottagarkonto.

Det går att förutspå att möjligheten att använda AI vid VD-bedrägerier kommer användas i ökad utsträckning för att den som luras ska få intrycket av att de pratar med en viss person. Det här kräver redan nu att det utarbetas strategier för hur detta hot ska hanteras i företag. Det går också att tänka sig att det går att dra nytta av AI genom att företag använder sig av sådan teknik för att lokalisera potentiella VD-bedrägerier och varna medarbetare för detta.

Vid VD-bedrägerierna är email vanligt förekommande, vilket skiljer sig från befogenhetsbedrägerierna genom vishing. Dessa ärenden initierade i drygt hälften av fallens genom att gärningsmannen ringde upp den person som denne tänkt att lura. I 45 procent av fallen så skickades ett sms där det fanns ett telefonnummer och en text som syftade till att få det presumtiva brottsoffret att ringa angivet telefonnummer. Texterna i sms:n kunde handla om information om att en ansökan om kreditkort inkommit eller att det tackades för en beställning av en vara från exempelvis Biltema.

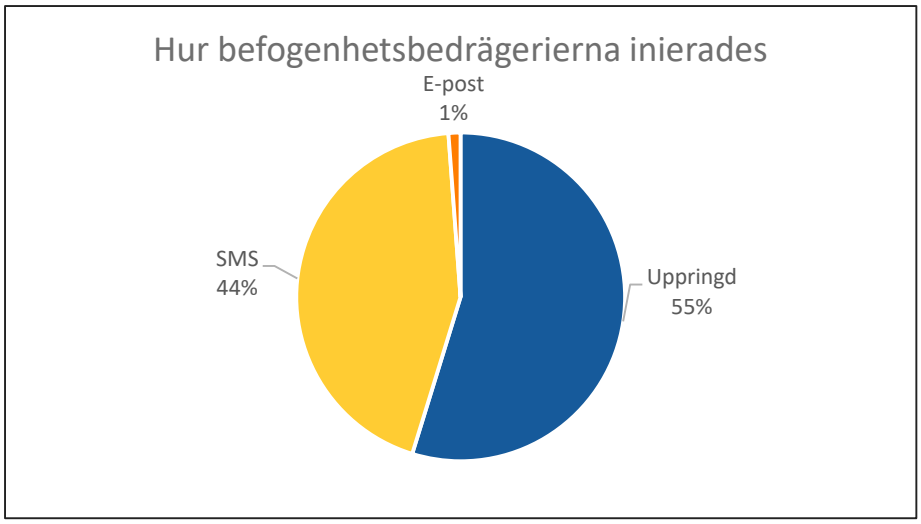


Diagram 4. Hur befogenhetsbedrägerierna initierades (n=84)

I diagram 5 framgår att i de fullbordade befogenhetsbedrägerierna (vishing) användes BankID i drygt hälften av fallen för att föra över pengar. Swish användes vid 39 procent av dessa fall.

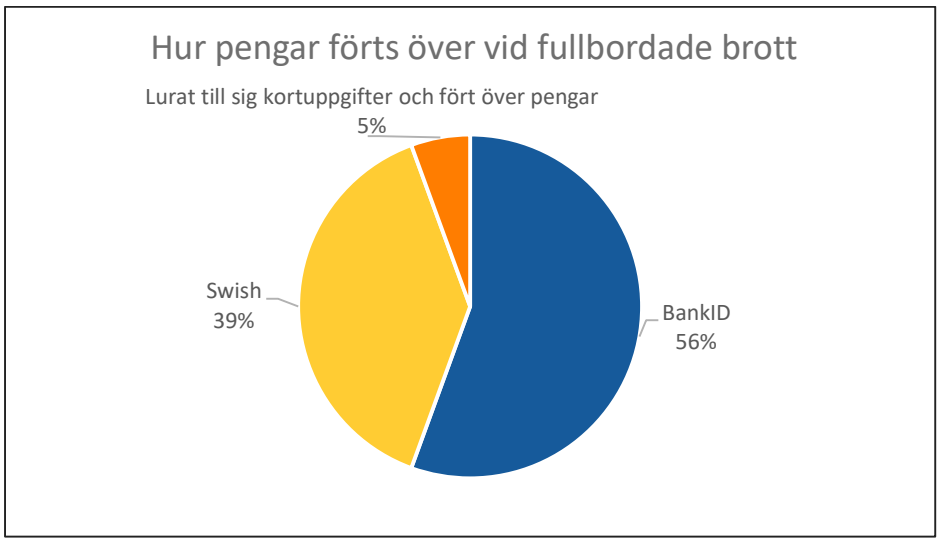


Diagram 5. Hur pengar förts över vid fullbordat befogenhetsbedrägeri (vishing) (n=18)[18]

När det gäller nyttjandet av BankID för att lura brottsoffren går det att vara kritisk till att någon med BankID och kund på en bank tidigare behövde vara rädd för att själv logga in på BankID eftersom någon annan person därigenom kunde sitta på en annan plats och logga in på kundens bank utan att kunden kände till detta. Det har riktats kritik mot BankID för en bristande säkerhet[19] och en förändring skedde i maj år 2024 där en QR-kod ska skannas in vid inloggning som försvårar att man kan sitta på en annan plats och logga in på ett konto med hjälp av BankID.

Analysen av befogenhetsbedrägerierna genom vishing indikerar dock att en stor andel (4 av 10 i det material som undersöktes) av överföringar av pengar sker med hjälp av swish och det förekommer även att brottsoffer blir lurade att lämna ut sina kontouppgifter (5% i det material som undersöktes), där ovanstående förändring av BankId saknar betydelse. Likaså förekommer det att brottsoffer blir lurade att släppa in andra att fjärrstyra deras datorer, vilket möjliggör att genomföra befogenhetsbedrägerierna på distans. Det förekommer också att de får QR-koder skickade till sig från bedragarna.

I planen för att genomföra befogenhetsbedrägerier ingår att utföra ett stort antal försök innan ett bedrägeri lyckas. En bedragare som intervjuas i SVT berättar: *”Om du skickar 100 sms, kanske tio personer ringer tillbaka och de har redan gått på första steget”*[20]. I vissa fall omfattar ett befogenhetsbedrägeri ett så stort belopp att det kan motivera att lägga ned månader och till och med år på misslyckade försök. Om man utgår från ett lågt brottsutbyte av befogenhetsbedrägerier genom vishing i form av det framräknande medianvärdet på 15 000 kronor innebär det att om en gärningsman lyckas med två befogenhetsbedrägerier i månaden motsvarar det en månadslön innan skatt på 40 000 kronor. Av anmälningarna går det att utläsa att många försök inte tar någon tid alls genom att det rör sig om sms-utskick eller att det tar kort tid innan ett presumtivt brottsoffer anar oråd och avslutar samtalet.

[18] Att n=18 och inte 16 beror på att både BankId och Swish användes i två ärenden.

[19] Se bland annat https://news55.se/ekonomi/sverige-och-bank-id-tredje-samsta-landet-mot-natbedragerier/ och https://www.di.se/debatt/debatt-bank-id-s-nya-krav-okar-utanforskapet-men-problemen-kunde-losts-enklare-for-lange-sedan/

[20] https://www.svt.se/nyheter/granskning/ug/granskning-se-bedragarnas-metoder-fran-insidan-har-toms-margaretas-konto

Det gör att det går att hinna med många försök under kort tid och att det kan räcka med att några tiondels promille av försöken lyckas för att nå upp till en månadslön på 40 000 kr/månad.

Även om en liten andel av försöken till befogensbedrägerier anmäls möjliggör det stora antalet försök att få ett underlag för att kunna genomföra proaktiva aktiviteter mot dessa gärningsmän.

1.5 Ålder, kön och riskmedvetenhet hos målsäganden

Målsäganden i fullbordade befogenhetsbedrägeri genom vishing var mellan 57 och 86 år. Genomsnittsåldern var 77 år. 52 procent var män. Om man inkluderar även de som var målsäganden i försöksärenden var deras ålder mellan 26 och 88, där genomsnittsåldern var 69 år. 51 procent var män.

Av ärenden framgår att målsäganden har skämts över att blivit lurade och vid samtal med polispersonal har det getts exempel på att personer som fått information om befogenhetsbedrägerier ändå blivit lurade och av ärenden som analyserats framgår att vissa målsäganden varit utsatt för fullbordade befogenhetsbedrägeri flera gånger. Det är inte så att dessa personer inte känner till riskerna. De vill undvika att bli lurade, men bedragarna lyckas lura dem ändå. Forskare som utvärderade polisens informationskampanj där 1,2 miljoner vykort skickades ut för att öka medvetenheten om bland annat befogenhetsbedrägerier visade sig ha en mycket liten effekt[21]. Däremot har informationskampanjer som polisen i Danmark och Island gjort för att förebygga VD-bedrägerier visat sig få en effekt. I Danmark genomfördes informationskampanjerna i samverkan med branschorganisationerna där det togs fram olika former av guider[22].

Det har framförts förslag på att man som bankkund frivilligt skulle kunna välja att vissa utbetalningar skulle kräva dubbelsignering av exempelvis ett barn eller partner. Det har också framförts förslag på att bankerna skulle sätta en 24 timmars överföringspaus på överföringar till nya konton och att man måste signera vid starten och efter 24 timmar igen. Dubbelsignering och väntetider är väl kända och etablerade tekniker som förhindrar bedrägerier[23].

[21] Niklas Jakobsson & Manne Gerell (2023) “Evaluating the impact of an informational postcard campaign on telephone scams targeting the elderly“, *Nordic Journal of Criminology*, Volume 25, no.1-2024, pp.1-6

[22] https://polisen.se/siteassets/dokument/ovriga_rapporter/nordic-threat-assessment-on-online-fraud-2024-web.pdf/download/?v=46fb9ca8b5e21460a8a232a324b64254

[23] https://www.di.se/debatt/debatt-bank-id-s-nya-krav-okar-utanforskapet-men-problemen-kunde-losts-enklare-for-lange-sedan/

2. Åtgärder

2.1 Verka för att initialt erhålla på vissa uppgifter i ärenden

Utarbeta rutin och dokument som används i samband med anmälningsupptagning eller som skickas ut digitalt strax därefter för att få in information som många gånger i dagsläget saknas i ärendena. Denna information skulle öka förutsättningarna att kunna hushålla med polisens resurser på ett effektivt sätt genom att tid inte läggs ned på fall som är utsiktslösa att klara upp, öka kvaliteten på underlagen för nedläggning och samtidigt ge användbar information i det kartläggningsarbete som krävs för att kunna rikta in insatser för att klara upp, hindra och försvåra befogenhetsbedrägerier. Det vore bra om målsäganden skulle kunna få återkoppling gällande betydelsen av att de anmält brott och att ha lämnat ytterligare information – även om det inte leder till att just deras brott klaras upp kan de uppmuntras av att det bidrar det till arbetet mot investeringsbedrägerier.

2.2 Verka för att möjliggöra webbanmälan för denna typ av bedrägerier

Möjligheterna att kunna göra en webbanmälan gällande vissa typer av befogenhetsbedrägerier skulle underlägga för företag att göra anmälningar som de i dagsläget avstår ifrån att göra på grund av att det tar för lång tid samt att det skulle finnas möjligheter att säkra viss information som i dagsläget ofta saknas (se punkt 2.1)

2.3 Bevaka inkomna anmälningar om befogenhetsbedrägerier

Ha en kontinuerlig bevakning av inkomna anmälningar om befogenhetsbedrägerier där information omgående används för proaktiva och brottsförebyggande aktiviteter (se punkt, 2.4, 2.5 och 2.6).

2.4 Proaktivt och brottsförebyggande arbete i utredningsverksamheten

För att angripa befogenhetsbedrägerierna som skett genom vishing finns ett behov av att i utredningsverksamheten frångå en inriktning där man inväntar att anmälningar inkommer och därefter vidtar utredningsåtgärder. Ett sådant tillvägagångssätt gör att utsikterna är små för att klara upp de flesta av befogenhetsbedrägerierna och att kunna förebygga befogenhetsbedrägerier på ett framgångsrikt sätt. I en rapport om narkotikabrott som publicerades för 14 år sedan beskrivs hur polisen byggde upp virtuella agenter på nätet för att arbeta mot narkotikabrott[24]. **Systematiken och processerna vad gäller befogenhetsbedrägerierna genom vishing öppnar upp möjligheter för att använda sig av virtuella agenter som ett sätt att angripa denna typ av brottslighet**. Genom att ringa upp telefonnummer som anges i sms finns möjlighet att få kontakt med personer som ägnar sig åt systematiska bedrägerier. Med hjälp av teknik och spaning går det att lokalisera bedragarna som kan leda till tvångsåtgärder där bland annat datorer och telefoner beslagtas. Samtal med bedragare kan spelas in som kan användas i de utredningar där målsäganden blivit lurade. En internationell samverkan i de ärenden som de virtuella agenterna är inblandade i kan göra det möjligt att spåra bedragare och säkra bevis som inte är möjligt att göra då anmälningar kommer in efter att samtal och transaktioner skett.

[24] https://polisforskning.se/ws/media-library/a34e5cb2fd3a475c95fed15f185a540a/pol_arb_m_narkotika-rapport_inl110825w.pdf , sidan 83-86.

Det går också att bygga upp samarbetet med telefonbolagen och omgående ge dem information när det finns misstanke om att vissa telefonnummer används vid bedrägerier (se punkt 2.3).

Inom ramen för polisområde Östergötlands verksamhet bör det användas virtuella agenter och bedriva ett proaktivt arbetssätt. Eftersom befogenhetsbedrägerier genom vishing är välplanerad och strategiskt upplagda är en viktig förutsättning för ett lyckat resultat att polisens arbete också är välplanerat och bedrivs på ett strategiskt sätt. På nationell nivå finns därför ett behov av att koordinera arbetet så att det sker mot olika brottsstrukturer och genomförs på ett systematiskt och effektivt sätt ur ett nationellt perspektiv, men också att en samverkan bland annat sker med de nordiska länderna eftersom vi ur flera aspekter delar samma problematik[25].

När det gäller fysisk vishing finns ett behov att bygga upp rutiner för att snabbt kunna agera och få tag i bedragarna. Nuvarande organisering av polisens ledningscentraler utgör ett hinder för en effektiv brottsförebyggande och repressiv verksamhet, vilket också gäller denna typ av brott. Det finns möjlighet med hjälp av virtuell teknik utveckla ledningscentralernas verksamhet[26].

När det gäller VD-bedrägerier var det för få fall för att det inom ramen för denna analys ska gå att dra slutsatser om lämpliga tillvägagångssätt för att angripa denna brottstyp, men det finns sannolikt goda möjligheter till att arbeta proaktivt och brottsförebyggande även mot dessa brott, men det kräver sannolikt i högre grad av internationell samverkan jämfört med vishing ärendena.

2.5 Samverkan för att förbättra företags och andra organisationers rutiner

Polisområde Östergötland kan inom ramen för Östergötland tillsammans mot brott (ÖTMB) involvera branschorganisationer i en informationskampanj för att förebygga VD-bedrägerier genom att verka för att företag och andra typer av organisationer i Östergötland utvecklar sina rutiner för att förebygga denna typ av bedrägerier. Förutom en informationskampanj där olika former av guider utformas går det att tänka sig att företag och andra typer av organisationer erbjuds att det med jämna mellanrum görs fiktiva VD-bedrägeriförsök för att öka motståndskraften om det sker riktiga försök. Det går också tänka sig att företag och organisationer löpande får information om tillvägagångssätt i de anmälningar som inkommer till polisen som rör försök eller fullbordade VD-bedrägerier.

2.6 En påverkan att externa aktörer försvårar bedrägerier

Vid vishingbedrägerierna är det vanligt förekommande att samma telefonnummer används. Genom att verka för att telefonnummer som används vid bedrägerier eller bedrägeriförsök snabbt stängs av kan försvåra arbetet för bedragarna.

För polisen på nationell nivå är det viktigt att medverka till att bland annat telefonoperatörer och banker försvårar befogenhetsbedrägerier genom olika former av åtgärder. I detta arbete går det exempelvis att hänvisa till vad våra nordiska grannar gjort. I Finland har teleoperatörerna via filter gjort det svårare för telefonbedragare och på Island har banker infört

[25] https://polisen.se/siteassets/dokument/ovriga_rapporter/nordic-threat-assessment-on-online-fraud-2024-web.pdf/download/?v=46fb9ca8b5e21460a8a232a324b64254

[26] Se bl.a. http://www.diva-portal.org/smash/get/diva2:1143487/FULLTEXT01.pdf

olika spärrar, exempelvis stoppat Google Pay-installationer på mobiler i utlandet för att försvåra för bedragarna[27]. Det vidtas också åtgärder i Sverige och bland annat Nordea har under 2024 startat upp en ny typ av sparkonto med fördröjda transaktioner och ett tillval som utsatta grupper kan använda för att försvåra och begränsa bedrägerier.

Vissa av förändringarna kan kopplas till att ett program i SVT:s uppdrag granskning[28] fick stor uppmärksamhet som visade hur en svensk liga med telefonbedragare i Marbella agerade för att lura pensionärer på deras besparingar. Detta ledde till att regeringen kallade bankerna till ett möte. Tillvägagångssättet vid dessa befogenhetsbedrägerier var på intet sätt nytt, men den mediala uppmärksamheten skapade en press på politiker att visa handlingskraft som i sin tur satte press på bankerna. Det finns ett behov av att se till att telefonbolag, banker och andra aktörer får ett tryck på sig att vidta åtgärder för att försvåra befogenhetsbedrägerierna och ge dem information så det har möjligheter att lyckas med sådana ambitioner.

Polisområde Östergötland kan förutom att peppa befattningshavare på nationellt bedrägericentrum att fortsätta arbetet med att i samverkan med externa aktörer försöka försvåra befogenhetsbedrägerier även bidra med information till externa aktörer. Vid samtal har det framkommit att nationellt bedrägericentrum (NBC) är måna om att ha goda relationer med sina samverkanspartner, vilket är naturligt. Polisområde Östergötland har inte samma behov av att ha goda relationer med externa samverkanspartner på nationell nivå och kan därför göra uttalanden som är mer kritiska, vilket kan vara viktigt för att skapa en press som kan motivera de externa aktörer att vidta åtgärder som kostar pengar. Det är betydelsefullt att det förändringstryck som uppkom i samband med SVT:s reportage om bedrägerier i Uppdrag granskning bibehålls och det krävs en medveten strategi för detta. Med tanke på signaler som fångats upp kring NBC förhållningssätt är det något som polisområde Östergötland tillsammans med andra polisområden bör se som angeläget att driva.

2.7 Verka för att Brå ökar kvaliteten på brottskodningen

Polisområde Östergötland bör när tillfälle ges och i olika sammanhang göra yttranden som kan påverka Brå att försöksbrott och fullbordade bedrägeribrott får olika brottskoder. Det är särskilt viktigt vad gäller befogenhetsbedrägerier där en stor andel av de anmälda brotten utgöras av försöksbrott. När det gäller brottskategorin befogenhetsbedrägerier bör Polisområde Östergötland också i den mån det finns möjlighet att verka för att denna övergripande kategori tas bort och istället delas upp i två andra kategorier: ”*Vishing*” och ”*BEC-bedrägerier*”. Det är uppenbart att dessa två tillvägagångssätt skiljer sig så mycket åt att de inte borde ligga under samma brottskategori.

I denna rapport är det med tanke på det behov som uppstår att skilja dessa brott åt tydligt att nuvarande klassificering behöver ändras. Att så är fallet blir också klart med tanke på att det både i Polismyndighetens rapport om brottsvinster vid bedrägeribrottslighet[29] och i den rapport som tagits fram i samarbete mellan polisen i de nordiska länderna görs en sådan

[27] Se https://polisen.se/siteassets/dokument/ovriga_rapporter/nordic-threat-assessment-on-online-fraud-2024-web.pdf/download/?v=46fb9ca8b5e21460a8a232a324b64254

[28] https://www.svt.se/nyheter/granskning/ug/granskning-se-bedragarnas-metoder-fran-insidan-har-toms-margaretas-konto

[29] https://polisen.se/siteassets/dokument/ovriga_rapporter/brottsvinsterna-for-bedrageribrottsligheten-2023.pdf

uppdelning[30]. Det kan också nämnas att när Brå själva gör en uppställning av tillvägagångssätt vid bedrägerier mot privatpersoner anges bland annat romansbedrägerier, investeringsbedrägerier som brottstyp, men inte befogenhetsbedrägerier[31]. Det om något borde visa att det finns ett behov av att ta bort brottstypen befogenhetsbedrägeri i statistiken.

En invändning mot att ta bort klassen kan vara att det då inte går att följa upp brottsutvecklingen över tid. Med tanke på vad som framkommer i denna analys har ett sådant argument liten bäring på ett verkligt förhållande med tanke på en omfattande felkodning och den stora andelen försöksbrott som anmäls. Om klassificeringen görs om går det dessutom att vidta åtgärder för att möjliggöra en jämförelse bakåt i tiden genom att med hjälpa av AI och fritexten i anmälningar genomföra en klassificering av anmälningar bakåt i tiden med de nya brottskoderna.

[30] https://polisen.se/siteassets/dokument/ovriga_rapporter/nordic-threat-assessment-on-online-fraud-2024-web.pdf/download/?v=46fb9ca8b5e21460a8a232a324b64254

[31] https://bra.se/download/18.3808406a192bd2f0b727c8f/1730736409029/2023_11_Bedragerier-mot-privatpersoner.pdf, sidan 37