Rapport 2023:11

Bedrägerier mot privatpersoner

De förebyggande åtgärdernas träffsäkerhet

Brå – kunskapscentrum för rättsväsendet
Myndigheten Brå verkar för att brottsligheten minskar och tryggheten ökar i samhället. Det gör vi genom att ta fram fakta och sprida kunskap om brottslighet, brottsbekämpning och brottsförebyggande arbete, till i första hand regeringen och myndigheter inom rättsväsendet.

Publikationen finns som pdf på www.bra.se. På begäran kan Brå ta fram ett alternativt format. Frågor om alternativa format skickas till tillgangligt@bra.se

Författare: Lina Fjelkegård och Anna Horgby

urn:nbn:se:bra-1137
ISSN 1100-6676

Brottsförebyggande rådet, Box 1386, 111 93 Stockholm
Telefon 08–527 58 400, e-post info@bra.se, www.bra.se

Bedrägerier mot privatpersoner

De förebyggande åtgärdernas träffsäkerhet

Rapport 2023:11

Förord

Bedrägeri är ett av de vanligaste brotten. Under 2022 anmäldes närmare 200 000 bedrägeribrott. Bedrägerierna medför stora brottsvinster som många gånger går till organiserad brottslighet. I media rapporteras om hur brottsoffer – särskilt äldre – luras på stora summor. Samtidigt är andelen anmälda brott som klaras upp mycket låg, vilket sätter ljuset på det brottsförebyggande arbetet. Hittills har det dock inte funnits någon sammanställning av det brottsförebyggande arbetet eller av vilka bedrägerier och sårbarheter åtgärderna riktar sig mot.

Hösten 2022 initierade Brå därför en studie om bedrägerier mot privatpersoner, vilka omständigheter och situationer som möjliggör brott och vilka åtgärder som görs för att förebygga bedrägerier. Brå gör även en analys av hur träffsäkra de förebyggande åtgärderna är och presenterar utvecklingsområden och rekommendationer till olika brottsförebyggande aktörer. Rapporten vänder sig till regeringen liksom till olika aktörer som arbetar förebyggande mot bedrägerier mot privatpersoner, såsom Polismyndigheten, andra myndigheter, intresseorganisationer och företag.

Rapporten är skriven av Lina Fjelkegård (projektledare) och Anna Horgby, båda utredare på Brå. Brå vill särskilt tacka professor emeritus Sven-Åke Lindgren och docent Oskar Engdahl, båda vid Göteborgs universitet, som har vetenskapligt granskat ett utkast till rapporten och lämnat värdefulla synpunkter. Det är dock Brå som i alla avseenden ansvarar för innehållet i rapporten. Avslutningsvis vill Brå rikta ett varmt tack till de intervjupersoner som deltagit i studien och bidragit med sin tid, erfarenhet och kunskap.

Stockholm i september 2023

Mattias Larsson
Generaldirektör

Anna Hansson
Enhetschef

Innehållsförteckning

Sammanfattning

Bedrägeri är ett brott som drabbar många och som över tid ökat i omfattning. Under 2022 anmäldes drygt 180 000 bedrägerier, vilket kan jämföras med 50 000 år 2000. Dessutom rapporterar Polismyndigheten om stora brottsvinster för bedrägerier som ökat över tid och som många gånger går till organiserad brottslighet. Den omfattande brottsligheten i kombination med att brotten i regel är svåra att utreda kräver att det brottsförebyggande arbetet prioriteras. Brå initierade därför en studie om bedrägerier mot privatpersoner i syfte att undersöka hur träffsäkra de brottsförebyggande åtgärderna är. Träffsäkerheten i det förebyggande arbetet studeras genom en analys av hur omständigheter och situationer som möjliggör bedrägerier träffas av de bedrägeriförebyggande åtgärderna. Rapporten innehåller även rekommendationer till olika brottsförebyggande aktörer.

Studien bygger i första hand på intervjuer med yrkespersoner från Polismyndigheten, andra myndigheter, intresseorganisationer och företag. Intervjuerna kompletteras med skriftligt material samt viss beskrivande statistik.

Telefonbedrägerier beskrivs som det allvarligaste problemet

Olika källor ger olika bilder av bedrägeribrottslighetens omfattning och struktur. Exempelvis stod *kortbedrägerierna* för 40 procent av alla anmälda brott under 2022, men enbart för 5 procent av den uppskattade brottsvinsten. Samma år stod de anmälda *bedrägerierna genom social manipulation* – när bedragaren genom att skapa ett förtroende lurar brottsoffret på pengar eller personuppgifter – för 19 procent av alla anmälda brott och för 46 procent av brottsvinsterna.

Telefonbedrägerierna, där brottsoffer kontaktas via telefon, är den typ av bedrägeri som är mest oroande enligt de flesta intervjupersonerna. Vanligtvis har bedragaren inför samtalet gjort en kartläggning för att välja ut lämpliga brottsoffer och för att verka trovärdig i sin kontakt. Ofta sker en del av vilseledandet genom att bedragaren manipulerat det telefonnummer som visas hos mottagaren. I samtalet påstår bedragaren exempelvis att hen ringer från polisen, banken eller ett inkassobolag och stressar och skrämmer upp brottsoffret med en påhittad historia. Bedragaren är vänlig

och hjälpsam och erbjuder en lösning på situationen. Pengarna förs i regel över till ett målvaktskonto – många gånger en ungdom – för att i slutändan hamna hos ett kriminellt nätverk. Manipulering av avsändaren används även för att skapa trovärdighet vid *social manipulation via sms, e-post eller sociala medier* där brottsoffret vilseleds att genomföra en transaktion eller lämna ifrån sig kort- eller personuppgifter.

Två typer av bedrägerier genom social manipulation där anmälningarna är få, men brottsvinsterna är förhållandevis stora, är *romansbedrägerier* och *investeringsbedrägerier*. I romansbedrägerier inleder bedragaren typiskt sett en kärleksrelation med brottsoffret via sociala medier eller dejtingsidor för att få offret att vilja föra över pengar till bedragaren i ett senare skede. Investeringsbedrägerier mot privatpersoner innebär att en person vilseleds att investera pengar, ofta i någon typ av finansiell produkt som aktier, obligationer eller kryptovalutor. Kontakten föregås i regel av oseriösa annonser om produkterna i sociala medier med länkar till företag och webbplatser som ser ut att vara seriösa.

Sociala medier som plattform, liksom länkar till oseriösa företag, webbplatser och annonser används också i andra typer av bedrägerier, såsom i *kortbedrägerier* och *annonsbedrägerier* – det vill säga vilseledande försäljning eller köp av en annonserad vara eller tjänst.

Stora skador vid bedrägerier – särskilt genom social manipulation

Bedrägerier genom social manipulation innebär ofta stora ekonomiska förluster för brottsoffren. Många intervjupersoner beskriver att brottsoffren ofta upplever skam och skuldkänslor och tidigare studier visar att utsattheten kan få psykiska skadeverkningar och leda till otrygghet. Det kan i sin tur påverka tilltron till samhällets institutioner och system. Bedrägerier genom social manipulation drabbar, enligt intervjuerna, särskilt äldre personer.

Andra typer av bedrägerier, som kortbedrägerier och annonsbedrägerier, drabbar i stället främst personer i arbetsför ålder. De ekonomiska förlusterna är i de fallen förhållandevis små och de beskrivs inte vara lika förknippade med skam och skuld som bedrägerier genom social manipulation.

Sårbarheter som möjliggör bedrägerierna

Utifrån vår kartläggning av bedrägeribrottsligheten har ett flertal tekniska och strukturella sårbarheter liksom sårbarheter hos potentiella brottsoffer identifierats:

- Lättillgängliga uppgifter om bland annat namn, adress, ålder, familjesituation och fordonsinnehav möjliggör för bedragare att kartlägga potentiella brottsoffer och förbereda vilseledandet.
- Möjligheter att manipulera vem som visas som avsändare vid samtal, sms och e-post gör bedragaren trovärdig i sin kontakt med brottsoffret.
- Möjligheter att publicera oseriösa annonser, registrera oseriösa domäner och företag, liksom att använda målvakter som företrädare för dessa, medför att bedragare kan skapa trovärdighet genom till synes seriösa webbplatser, företag och annonser.
- En digital bank- och betalmarknad innebär dels en otillräcklig övervakning av transaktioner, dels stora möjligheter för bedragare att snabbt göra pengarna ospårbara.
- Trots ett flertal åtgärder kvarstår möjligheter att missbruka någon annans identitet för bankärenden och vid kortköp.
- Tillgång till specifika kompetenser för att förbereda och genomföra bedrägeriet (exempelvis tekniskt kunnande) samt till personer som kan användas som penningmålvakter möjliggör bedrägerierna.
- Digital okunskap och ovana, stress, brist på kritiskt förhållningssätt, riskbenägenhet, spänningsbehov, girighet, desperation, ensamhet samt behov av bekräftelse, förståelse, närhet och kärlek är alla sårbarheter knutna till potentiella brottsoffer. Digital ovana, stresskänslighet och brist på kritiskt förhållningssätt är sårbarheter särskilt förknippade med äldre personer.
- Avsaknad av tillgängliga alternativ till digitala tjänster gör att personer som saknar digital vana, kunskap och kanske motivation att lära sig tvingas att använda tjänster som de inte behärskar.

De sårbarheter som identifierats speglar i stor utsträckning människors beteendemönster. Vad människor gör, hur det görs och vad det finns för alternativ i kombination med mänskliga förmågor och egenskaper styr hur bedrägerier kan genomföras och vilka som drabbas.

Brottsförebyggande åtgärder har olika karaktär

I intervjuerna framkommer ett flertal brottsförebyggande åtgärder riktade mot de olika tekniska och strukturella sårbarheterna. Det inkluderar bland annat åtgärder som ska försvåra förberedelser för brott, exempelvis kontroller av domäner och användarkonton. Hit hör också åtgärder med syftet att försvåra vilseledanden i kontakten, exempelvis kontroller av annonser och initiativ mot manipulerade telefonnummer. Det finns också åtgärder i form av bland annat transaktionsövervakning och säker inloggning för att stoppa bedrägliga transaktioner, samt åtgärder för att försvåra för gärningspersoner att få tillgång till brottsvinster från bedrägerier.

Brås studie visar även på brottsförebyggande åtgärder som handlar om att stärka individers förmåga att stå emot bedrägeriförsök. En stor del av arbetet är riktat mot äldre för att öka deras möjligheter att skydda sig själva. Insatserna är ofta fokuserade på telefonbedrägerier och andra typer av social manipulation, i syfte att ge äldre mer kunskap om bedrägliga tillvägagångssätt liksom om hur digitala tjänster såsom bank-id fungerar.

Mer behöver göras för att åtgärderna ska få full effekt

Trots en bred uppsättning förebyggande åtgärder är det uppenbart att den brottsförebyggande verksamhet som bedrivs i dag inte är i närheten av tillräcklig för att komma till rätta med brottsproblemet bedrägerier mot privatpersoner.

Vissa åtgärder har stor förebyggande potential, men består hittills enbart av påverkansarbete eller är under planering. Det gäller bland annat ett förslag på en statlig e-legitimation, åtgärder mot bedräglig användning av manipulerade telefonnummer, lösningar kopplade till säkrare identifiering vid användning av digitala tjänster samt förslag om utökade kontroller av företag och av innehåll på onlineplattformar.

Det finns också flera omständigheter som påverkar möjligheterna att arbeta förebyggande mot vissa sårbarheter, såsom lagstiftning, förväntningar (exempelvis på snabba transaktioner) och brottens i många fall internationella karaktär. Intervjupersoner från banksektorn beskriver att det finns utmaningar med att hitta tillräckligt träffsäkra kontroller som träffar bedrägliga transaktioner men släpper igenom övriga.

Även åtgärder för att stärka individers motståndskraft mot bedrägerier är förknippade med ett stort antal utmaningar. Intervjupersoner ser bland annat svårigheter med att nå fram med information, särskilt till de grupper som är i allra störst behov av den, och några är tveksamma till om insatserna har en brottsförebyggande effekt ens när informationen når fram. Det finns även forskning som visar att informationsinsatsers påverkan på människors beteende inte är självklar. För att få en effekt behöver bland annat budskap och innehåll anpassas både utifrån målgrupp och sammanhang.

Brås bedömning

Bedrägerier mot privatpersoner är ett brott med allvarliga konsekvenser som drabbar både individ och samhälle. Telefonbedrägerier framträder som särskilt oroande eftersom de ofta innebär stora ekonomiska och känslomässiga skador för brottsoffret, riskerar att påverka förtroendet för samhällets institutioner och system samt ger stora brottsvinster till kriminella nätverk. Även andra bedrägerier får allvarliga konsekvenser. Brå bedömer därför att det är angeläget att generellt prioritera det brotts-förebyggande arbetet mot bedrägerier mot privatpersoner.

Brå har identifierat ett stort antal sårbarheter som möjliggör brott, både hos potentiella brottsoffer och i de tekniska och strukturella omständigheterna. En samlad bedömning är att med några få undantag träffas sårbarheterna av någon form av förebyggande åtgärd. Uppenbart är dock att bedragarna hela tiden utvecklar sina metoder och strategier och hittar nya sårbarheter i såväl teknik och struktur som hos individen. Den fortsatt omfattande och i flera avseenden ökande brottsligheten visar också att det förebyggande arbetet som görs inte är tillräckligt och att det finns behov av fortsatt utveckling och förbättring.

Bedrägeri handlar om att människor luras och i takt med att tekniken blir säkrare inriktar sig bedragarna mer och mer mot individen. Åtgärder med syfte att göra potentiella brottsoffer mer svårlurade är därmed nödvändiga. Åtgärderna måste dock utformas på ett sätt så att de blir än mer relevanta för målgrupperna, bland annat genom fler praktiska inslag. Samtidigt innebär digitaliseringen att enskilda individer dels fått ett ökat ansvar för att skydda sina banktillgångar, dels är beroende av digitala lösningar som de inte alltid behärskar. Banker och andra aktörer, privata liksom offentliga, som utvecklar och tillhandahåller de tjänster och system som

utnyttjas i bedrägerier behöver därför återta delar av ansvaret och genom säkrare lösningar bättre skydda individen.

Brå ser också ett behov av ett tydligare helhetsperspektiv i det bedrägeriförebyggande arbetet där teknik och information används tillsammans för att bättre möta bedragarnas snabba anpassningar. Genom att använda tekniska lösningar kan informationen bli mer träffsäker, relevant och tydlig. Informationen i sin tur behövs för korrekt användning av de tekniska lösningarna.

Brås rekommendationer:

- Polismyndigheten bör ta en ledande roll i det bedrägeriförbyggande arbetet. Bland annat krävs ett utökat stöd till polisregionerna och lokalpolisområdena om hur den lokala nivån kan inkludera bedrägerier i sina lägesbilder och åtgärdsplaner. För att säkerställa att de problembilder som polisen tar fram är relevanta för det bedrägeriförebyggande arbetet bör de inkludera även försöksbrott och anmälningar som direktavskrivs. Polisen behöver också uppdatera och höja relevansen i existerande informations- och utbildningsmaterial om bedrägerier genom ytterligare målgruppsanpassning och fler och mer anpassade praktiska inslag. Därtill krävs en bred implementering av den brottsförebyggande strategin inom myndigheten.
- Polismyndigheten bör i samverkan med exempelvis Sveriges kommuner och regioner, Stöldskyddsföreningen, Internetstiftelsen och Myndigheten för samhällsskydd och beredskap, utveckla och systematisera riktade informationsinsatser till barn och unga som riskerar att användas som penningmålvakter.
- För att försvåra förberedelser till bedrägerier och försvåra hanteringen av brottsvinster bör Bolagsverket, Internetstiftelsen, onlineplattformar och onlinesökmotorer utöka sina kontroller av företrädare för företag och domäner, och av webbplatser, användarkonton och annonser. Brå ser särskilt ett behov av att Bolagsverket i enlighet med förslagen i SOU 2023:34 utökar sina kontroller av företrädare för företag.
- Regeringen bör se över vad det finns för möjligheter att begränsa publiceringen av personuppgifter som kan användas för att kartlägga potentiella brottsoffer för bedrägerier.
- Post- och telestyrelsen, telefonoperatörerna och Telekområdgivarna bör fortsätta och påskynda arbetet mot manipulerade telefonnummer,

samt utveckla det arbetet till fler områden, såsom bedräglig användning av sms och mobiltelefonnummer.

- Regeringen bör ta vidare förslaget om en statlig e-legitimation. E-legitimationen behöver implementeras samt på sikt utvecklas.
- Samtliga banker bör säkerställa att Bank-id:s lösningar för säker identifiering och signering implementeras fullt ut. Osäkra alternativ bör samtidigt fasas ut. Bankerna bör också fortsätta utvecklingen av säkrare digitala banker, särskilt avseende behöriga transaktioner.[1] Områden där Brå särskilt ser utvecklingsmöjligheter är bankprodukter med frivilliga begränsningar, och individbaserad transaktionsövervakning.
- Olika samhällsaktörer bör utveckla användandet av pushnotiser och varningar som relaterar till individens aktivitet. Brå ser också en möjlighet att i högre utsträckning använda åtgärder som knuffar personer mot det säkra alternativet, så kallad nudging.
- Offentliga aktörer på alla nivåer bör utöka sitt stöd till personer som behöver hjälp med att genomföra digitala tjänster, såsom digitala bankärenden, digitala samhällstjänster och digital handel. Det gäller särskilt kommunerna som sedan den 1 juli 2023 (enligt lag 2023:196) har ett ansvar för brottsförebyggande arbete.
- Förväntade effekter av såväl tekniska och strukturella åtgärder som åtgärder för att stärka potentiella brottsoffer behöver utvärderas och följas upp. Tekniska och strukturella åtgärder bör även föregås av risk- eller sårbarhetsanalyser. Analyserna och utvärderingarna bör inkludera analyser av eventuella förflyttningar av brottsligheten, liksom om åtgärderna medför några oönskade konsekvenser, exempelvis för grupper som inte använder sig av nya lösningar eller rutiner.

[1] En behörig transaktion är när brottsoffret vilseleds att själv genomföra en transaktion. Se bilaga 2 Ordlista för utförligare förklaring.

1. Inledning

Bedrägeri är ett brott som drabbar många och som över tid ökat i omfattning. Enligt undersökningen *Svenskarna och internet* (Internetstiftelsen 2022) har 59 procent av vuxna internetanvändare utsatts för någon form av bedrägeriförsök på internet det senaste året, och sedan början av 2000-talet har antalet anmälda bedrägerier ökat kraftigt. Under 2022 polisanmäldes drygt 180 000 bedrägerier, vilket kan jämföras med drygt 50 000 år 2000 (Brå 2023). Det här är en utveckling som har skett parallellt med att den anmälda stöldbrottsligheten minskat kraftigt. Exempelvis minskade de anmälda inbrotten från cirka 130 000 till drygt 69 000, och anmälda bilstölder från 63 000 till 8 000, under motsvarande period. Dessutom rapporterar Polismyndigheten om att brottsvinsterna för bedrägerier är stora och har ökat över tid. Polisen uppskattar att under 2022 uppgick brottsvinsterna för bedrägerier till 5,8 miljarder kronor jämfört med 4,6 miljarder året innan och 4,2 miljarder under 2020 (Polismyndigheten 2023a).[2] Det finns också en koppling mellan bedrägerier och annan organiserad brottslighet i Sverige, där brottsvinster från bedrägerier bidrar till kriminella nätverks ekonomiska förutsättningar och kan återinvesteras i annan brottslighet (Mondani och Rostami 2022, se även Polismyndigheten 2021).

Den omfattande bedrägeribrottsligheten i kombination med att brotten i regel är komplicerade att utreda kräver att problemet inte enbart bekämpas genom utredning och lagföring. Med den nuvarande personuppklaringen för bedrägerier på 3 procent (Brå 2023) är det därtill osannolikt att hotet om straff fungerar avskräckande för potentiella gärningspersoner. Såväl polisen som Brå menar att det i stället behövs olika former av bedrägeri-förebyggande åtgärder för att minska inflödet av anmälningar (Brå 2016, Polismyndigheten 2019, Polismyndigheten 2016).

Brå initierade därför en studie om det brottsförebyggande arbetet mot bedrägerier mot privatpersoner med syftet att undersöka hur väl de brotts-

[2] De uppskattade brottsvinsterna för bedrägerier är enligt beräkningar från Centralförbundet mot alkohol och narkotika på samma nivåer som den totala omsättningen för narkotikaförsäljningen i Sverige. CAN:s beräkningar bygger på en rad antaganden och den totala omsättningen beräknas till 4,6 respektive 11,2 miljarder beroende på antagande. Uppskattningen är av omsättning och inte vinst, men man bedömer att det finns ett betydande vinstutrymme (CAN 2023).

förebyggande åtgärderna träffar de omständigheter och situationer som möjliggör brott. I den här rapporten redovisas studiens resultat.

Brottsförebyggande åtgärder mot bedrägerier

Med brottsförebyggande arbete avses i den här rapporten arbete, verksamhet och åtgärder som uttalat och primärt syftar till att förhindra att brott begås (jfr. Polismyndigheten 2022a, Brå 2020, Regeringen 2017 Skr. 2016/17:126). Systematiskt brottsförebyggande arbete bygger på en process där utgångspunkten för det brottsförebyggande arbetet är en kartläggning av brottsproblemets omfattning, struktur och utveckling samt en analys av orsakerna till brottsproblemet. Det kan vara såväl orsaker relaterade till gärningspersonen som till situationen och till såväl omständigheter som direkt påverkar brottsligheten som till dem som har en mer indirekt påverkan på brottsligheten. De åtgärder som sätts in mot brottsproblemet ska sedan baseras på beprövad kunskap om effektiva åtgärder mot just dessa orsaker (Brå 2018a, UNODC 2010).

Åtgärder med fokus på situationen

Brottsförebyggande arbete delas ofta upp i social brottsprevention och situationell brottsprevention, där den sociala preventionen tar sikte på orsaker relaterade till omständigheter och förutsättningar hos den potentiella gärningspersonen medan den situationella preventionen fokuserar på att förändra situationer som möjliggör brott (Thodelius & Ceccato 2022, Clarke 1997, Tonry & Farrington 1995).

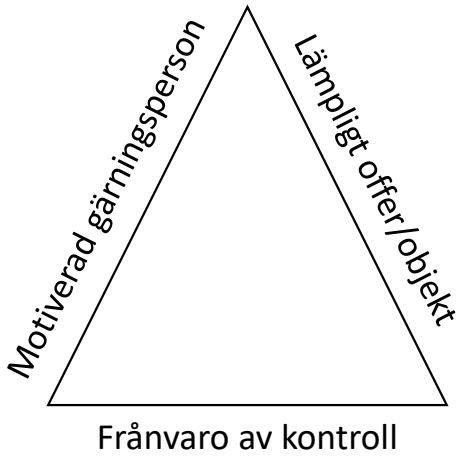
Av forskning om bedrägerier framgår att bedrägeribrottsligheten i dag i hög grad relaterar till den digitala utvecklingen och förändrade betalningsmönster (Rebovich & Byrne 2023, Engdahl 2022, Digital Fraud Committee 2022, Williams & Levi 2017, Brå 2016). En omfattande användning av internet för handel, bankärenden och kommunikation innebär ett betydande antal möjligheter till brott. Det innebär vidare att förebyggande åtgärder mot bedrägerier med fördel kan riktas mot att förändra dessa situationer.

Omständigheter och situationer som möjliggör brott

Omständigheter och situationer som orsaker till brott benämns ofta som rutinaktiviteter och tillfällesstrukturer och baseras på teorier om att brott uppstår när möjligheter uppenbarar sig i kombination med en låg upptäcktsrisk. Inom den så kallade rutinaktivitetsteorin beskrivs detta som

att tre förutsättningar måste finnas på plats för att ett brott ska begås: en motiverad förövare, ett lämpligt objekt och avsaknad av kontroll. Om en av förutsättningarna brister kommer brott inte att ske (Cohen & Felson 1979). Ursprungligen tar rutinaktivitetsteorin fasta på betydelsen av den fysiska platsen (Felson 1994), men modellen kan även tillämpas för att förstå och prioritera åtgärder som inte är bundna till en fysisk plats, vilket till exempel gäller för internetrelaterade brott (Williams & Levi 2017). De tre förutsättningarna bildar tillsammans den så kallade brottstriangeln som är utgångspunkten i såväl regeringens brottsförebyggande program som Brås metodstöd för lokalt brottsförebyggande arbete (Regeringen 2017, Brå 2018a). Situationell brottsprevention tar i första hand sikte på att påverka två av dessa förutsättningar: det lämpliga objektet och frånvaron av kontroll.

Figur 1 Brottstriangeln.



En bred definition av sårbarheter

Ytterligare ett begrepp för att benämna omständigheter som möjliggör brott är *sårbarheter*. Begreppet sårbarhet kan ha flera olika betydelser och används inom varierande områden. En vanlig definition av begreppet är att en sårbarhet är något som gör ett system känsligt för angrepp. I den här rapporten används begreppet sårbarhet något bredare och omfattar dels omständigheter relaterade till teknik, strukturer och det potentiella brottsoffret, dels gärningspersonernas möjligheter att förbereda brott och tillgodogöra sig brottsvinster.

Bedrägeriet är en del av en händelsekedja

Bedrägeri är dels den brottsbeteckning som regleras i 9 kap. 1–3 §§ brottsbalken (Om bedrägeri och annan oredlighet), dels ett begrepp som många gånger används bredare som ett samlingsbegrepp för att beskriva även andra brott eller övriga bedrägliga handlingar, till exempel skattebrott och bidragsbrott eller vilseledande marknadsföring (Engdahl 2022). När den specifika termen bedrägeri används i den här rapporten är det den legala definitionen av bedrägeri som avses, det vill säga handlingar som faller under brottsbeteckningen bedrägeri.

Ur ett brottsförebyggande perspektiv har det samtidigt ett värde att se på bedrägeriet som en del av en längre händelsekedja där de brotts-förebyggande åtgärderna kan ta sikte på olika delar av kedjan. Det kan dels handla om handlingar som begås som en del av förberedelserna inför bedrägeriet, dels om brott efter bedrägeriet för att tillgängliggöra brottsvinsten – alltså händelser som inte är en del av det faktiska bedrägeribrottet.

Den definition av bedrägeri som används i den här rapporten innebär att inte all upplevd utsatthet för bedrägeri, såsom vilseledanden[3] inom lagens gränser eller handlingar som regleras utanför straffrätten ingår i begreppet. Samtidigt ska man vara medveten om att såväl statistik över anmälda brott, undersökningar som mäter självupplevd brottsutsatthet, liksom andra uppgifter om brottslighet, är behäftade med en rad felkällor och därmed inte alltid motsvarar den legala definitionen. Felkällorna innebär både att handlingar som i lagens mening inte är brott kan komma med i beskrivningarna och att det förekommer brottsliga handlingar som inte kommer med, till exempel det så kallade mörkertalet i statistiken över anmälda brott. Det finns också svårigheter med definitioner i frågeundersökningar, liksom med händelser som ligger i gränslandet mellan bedrägerier och exempelvis vilseledande marknadsföring eller dåliga affärer.

Syfte och frågeställningar

Studiens syfte är att undersöka polisens och andra aktörers bedrägeri-förebyggande verksamhet och analysera hur träffsäkra åtgärderna är, det

[3] I den här rapporten används ordet vilseledande som ett substantiv. Ordet är bildat av verbet vilseleda, och det liknar det oböjliga adjektivet vilseledande som vi också använder i rapporten, som i vilseledande information. Ordet beskriver tydligt vad vi menar men förekommer ännu inte så ofta i språket.

vill säga hur väl de träffar de omständigheter och situationer som möjliggör brott.

För att uppfylla syftet med studien har vi utgått från två övergripande frågeställningar:

- I vilken mån träffar bedrägeriförebyggande åtgärder sårbarheter i tillfällesstrukturen?
- Hur kan det brottsförebyggande arbetet utvecklas för att bättre möta sårbarheterna i tillfällesstrukturen?

För att besvara de övergripande frågeställningarna har vi genomfört två kartläggningar. Den första kartläggningen beskriver brottsproblemet och identifierar omständigheter och situationer som möjliggör brott, det vill säga sårbarheter i tillfällesstrukturen. I den andra kartläggningen studeras polisens och andra aktörers bedrägeriförebyggande arbete. De övergripande frågeställningarna besvaras genom att de båda kartläggningarna ställs mot varandra i en analys av träffsäkerheten i de förebyggande åtgärderna.

Kartläggningen av brottsproblemet återfinns i kapitel 2 och 3, och kartläggningen av åtgärder i kapitel 4. Analysen av träffsäkerheten redovisas i rapportens avslutande kapitel (kapitel 5).

Metod och material

De båda kartläggningarna bygger på två separata material som till största delen består av intervjuer med nyckelpersoner. För kartläggningen om brottsproblemet kommer intervjupersonerna från polisens utredningsverksamhet samt andra myndigheter och organisationer som har kunskap om bedrägeribrottslighetens omfattning, utsatta grupper och gärningspersonernas tillvägagångssätt.[4]

I kartläggningen av de brottsförebyggande åtgärderna ingår flera olika verksamheter inom Polismyndigheten liksom ett flertal andra myndigheter, samt privata företag och övriga organisationer. Gemensamt för de intervjuade är att de bedriver någon form av bedrägeriförebyggande verksamhet, har kunskap om vilket bedrägeriförebyggande arbete som görs eller på annat sätt har kunnat bidra till kartläggningen. Sammantaget har

[4] Se bilaga 1 för en fullständig förteckning över vilka aktörer som ingår i intervjumaterialet, vilket skriftligt material som ingått samt övrig detaljerad information om metod och genomförande.

47 intervjuer med 56 personer samt 9 möten och samtal med 12 personer genomförts.

I båda kartläggningarna har även skriftligt material använts, bland annat en rad skriftliga rapporter, material från aktörernas webbplatser, material i form av kampanjsidor, samt utbildnings- och informationsmaterial som syftar till att förebygga bedrägerier.

I kartläggningen av brottsproblemet har även statistik använts för att komplettera intervjupersonernas uppfattning av bedrägeribrottslighetens omfattning. Uppgifterna kommer dels från Brås statistik över anmälda brott och den Nationella trygghetsundersökningen (NTU), dels från Polismyndigheten, Brottsoffermyndigheten och Konsumentverket.

Studiens metod och material innebär att kartläggningarna inte bör uppfattas som heltäckande. Det kan finnas typer av bedrägerier, sårbarheter och brottsförebyggande åtgärder som inte har fångats upp i varken intervjuer eller skriftliga källor. Vår bedömning är dock att materialet har en stor bredd och att det ger ett tillräckligt underlag för analysen.

2. Brottsproblemet bedrägeri mot privatperson

I det här kapitlet redovisar vi resultaten från kartläggningen av brottsproblemet. Kapitlet inleds med en sammanställning av uppgifter om brottsproblemets omfattning, följt av ett avsnitt där tillvägagångssätten för olika typer av bedrägerier beskrivs. Därefter beskrivs de som utsätts för bedrägerier och vilka skador bedrägerierna kan ha på individ- och samhällsnivå. I slutet av kapitlet sammanfattas typiska tillvägagångssätt och brottsoffer i en tabell. Kapitlet utgår från en samlad bedömning utifrån intervjuerna som gjordes för att kartlägga brottsligheten, liksom från skriftligt material, vilket innebär att det i regel inte specificeras vilka aktörer intervjupersonerna representerar.

Brottsproblemets omfattning

Brottsproblemets omfattning och struktur kan beskrivas utifrån ett flertal olika källor: den anmälda brottsligheten, frågeundersökningar som på olika sätt avser att mäta utsattheten för bedrägeri, en rad administrativa källor, och statistik över brottsvinster. Källorna ger något skilda bilder av vilka typer av bedrägerier som är vanligast.

Kortbedrägerier är vanligast i anmälningsstatistiken

Vid registrering av anmälda brott delas sedan 2019 bedrägeribrott in i nio övergripande klasser, varav fem är aktuella för brott mot privatpersoner[5]: *bedrägeri genom social manipulation, kortbedrägeri, annonsbedrägeri, identitetsbedrägeri* och *fakturabedrägeri.*[6] Bedrägerier genom social manipulation är när bedragaren skapar ett förtroende hos sitt brottsoffer och använder det till att förmå hen att genomföra en transaktion eller lämna ifrån sig uppgifter som möjliggör för bedragaren att genomföra transaktioner. Kategorin delas i sin tur in i fyra underkategorier:

[5] Dessa är dock inte uteslutande bedrägerier mot privatpersoner, utan inkluderar även brott mot företag och organisationer.

[6] Kortbedrägerier är när en bedragare använder en persons kort eller kortuppgifter för att genomföra ett köp. Annonsbedrägerier är vilseledande genom annonser eller svar på annonser. Identitetsbedrägeri är när någons identitet missbrukas för köp eller lån. Fakturabedrägeri är när någon vilseleds att betala en osann faktura.

befogenhetsbedrägerier, romansbedrägerier, investeringsbedrägerier och *övrig social manipulation.* [7]

Kortbedrägerier är den vanligaste bedrägeritypen sett till antalet anmälda brott: 40 procent av de anmälda bedrägerierna år 2022 vilket motsvarar cirka 72 000 anmälningar. Näst vanligast är bedrägerier genom social manipulation som står för cirka 20 procent av anmälningarna, följt av annonsbedrägerier och övriga bedrägerier på 14 procent vardera, identitetsbedrägerier 8 procent och fakturabedrägerier 4 procent.

I rapportens inledning framgår det att antalet anmälda bedrägerier har ökat kraftigt under hela 2000-talet. Mellan 2019 och 2021 minskade dock antalet anmälda bedrägerier med 21 procent, vilket beror på att antalet anmälda kortbedrägerier nästan halverades samt att identitetsbedrägerierna minskade kraftigt (Brå 2023). Under 2022 förändrades utvecklingen; antalet anmälda kortbedrägerier ökade och det totala antalet anmälda bedrägeribrott låg på ungefär samma nivå som året innan. Av den preliminära statistiken över anmälda brott första halvåret 2023 framkommer en fortsatt ökning av antalet anmälda kortbedrägerier, liksom av bedrägerier totalt, jämfört med motsvarande period år 2022 (Brå 2023). [8] Också anmälda bedrägerier genom social manipulation ökade första halvåret 2023, med 44 procent jämfört med motsvarande period året innan. I motsats till kort- och identitetsbedrägerier är det dock en brottstyp som oavbrutet ökat i omfattning de senaste åren, från 15 000 till 35 000 anmälningar mellan år 2019 och 2022 (Brå 2023). Enligt uppgifter från Nationellt bedrägericentrum (NBC) på Polismyndigheten består en stor andel av bedrägerier genom social manipulation av så kallade telefonbedrägerier. År 2022 anmäldes knappt 22 000 telefonbedrägerier,[9] vilket nästan är en dubblering jämfört med året innan.

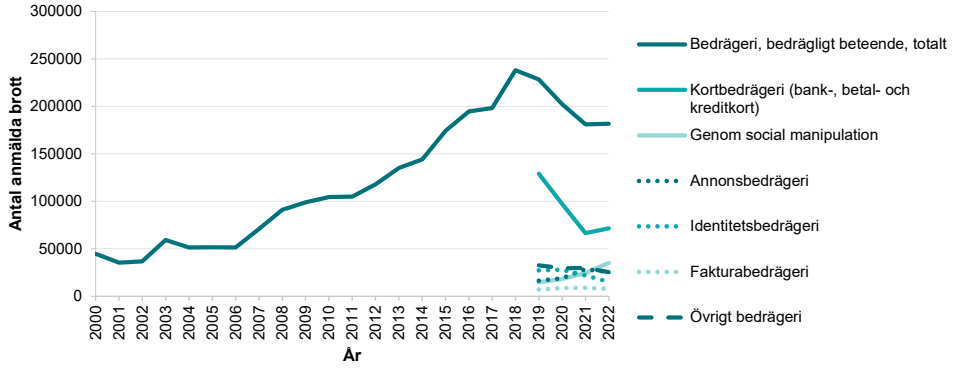
---

[7] Befogenhetsbedrägerier är när gärningspersonen utger sig för att vara någon med befogenhet, t.ex. en myndighetsperson eller banktjänsteman. Romansbedrägeri är när brottsoffret vilseleds inom ramen för en upplevd kärleksrelation. Investeringsbedrägeri är när brottsoffret vilseleds att investera pengar i en falsk produkt. Övrig social manipulation inkluderar bland annat social manipulation via sms, e-post eller sociala medier. En utförlig beskrivning av olika typer av bedrägerier följer längre fram i kapitlet.

[8] Bedrägerier totalt ökade med 26 % första halvåret 2023 jämfört med första halvåret 2022 enligt den preliminära statistiken. Kortbedrägerierna ökade med 57 % samma period. Identitetsbedrägerierna fortsatte dock att minska.

[9] Dessa siffror bygger på en genomgång av samtliga polisanmälda bedrägerier genom social manipulation genomförd av Nationellt bedrägericentrum. I telefonbedrägerier inkluderas utöver samtliga typer av telefonbedrägerier även en hel del sms-bedrägerier (t.ex. så kallat ”sms barn” där gärningspersonen utger sig för att vara brottsoffrets barn i behov av pengar).

Figur 2 Antal anmälda bedrägeribrott 2000–2022. Totalt och från 2019 uppdelat på bedrägerityp.[10] Källa: Brå 2023.



Övriga bedrägerityper är troligen underskattade

Enligt undersökningen *Svenskarna och internet* är det vanligaste bedrägeriförsöket att få bluff-epost-meddelanden och bluff-sms (Internetstiftelsen 2022). Även den Nationella trygghetsundersökningen (NTU) ger en annan bild än den registrerade brottsligheten genom att visa på en högre utsatthet för annonsbedrägerier än för kortbedrägerier.[11] Enligt uppgifter från Brottsoffermyndigheten är utsatthet för annonsbedrägeri det vanligaste skälet vid ansökan om brottsskadeersättning för bedrägeri.

Att bilderna skiljer sig mellan den registrerade brottsligheten och andra källor kan delvis förklaras av att den registrerade brottsligheten är beroende av brottsoffers benägenhet att anmäla brott. En varierande anmälningsbenägenhet mellan olika typer av bedrägerier kan i sin tur förklaras av olika omständigheter som har samröre med brottet, såsom hur allvarliga konsekvenser brottet har, liksom sannolikheten för uppklaring.[12] En omständighet som särskilt uppmärksammas i intervjuerna i samband med bedrägerier genom social manipulation är brottsoffrens skam och ovilja att berätta om sin utsatthet. Det kan också handla om att brottsoffret inte förstår att hen blivit utsatt för ett bedrägeri, att bedrägeriet är förknippat med ett medvetet risktagande, eller att beloppet är för lågt för att det ska uppfattas som tillräckligt allvarligt. Om en anmälan ökar

[10] Se bilaga 4 för figur med anmälda bedrägerier uppdelat på bedrägerityp för åren 2019–2022.

[11] I den senaste mätningen uppgav 5,7 procent att de utsatts för ett försäljningsbedrägeri/annonsbedrägeri, i jämförelse med 3,5 procent som angav att de utsatts för ett kort- eller kreditbedrägeri (NTU 2022). Indelningar och begrepp skiljer sig något mellan NTU och anmälningsstatistiken, men fungerar att jämföra i det här fallet.

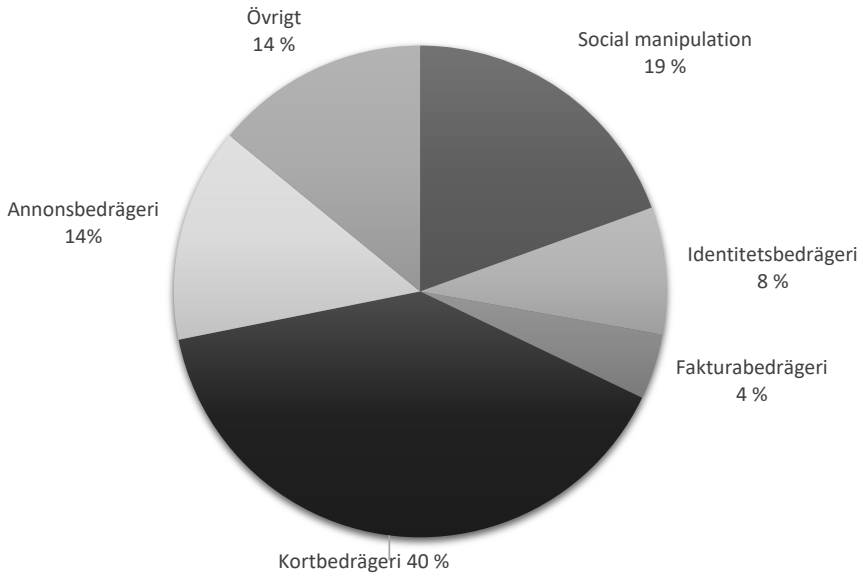
[12] Som framgått i inledningen är uppklaringen för bedrägeribrott låg. Personuppklaringen låg 2022 på 3 procent. Uppklaringen varierar dock något mellan olika bedrägerityper.

möjligheterna att få ersättning ökar dock incitamenten vilket exempelvis gäller vid kortbedrägerier. Det innebär att antalet anmälningar vid kortbedrägerier sannolikt är relativt korrekta, medan övriga anmälda bedrägerier av olika anledningar troligen är underskattade.

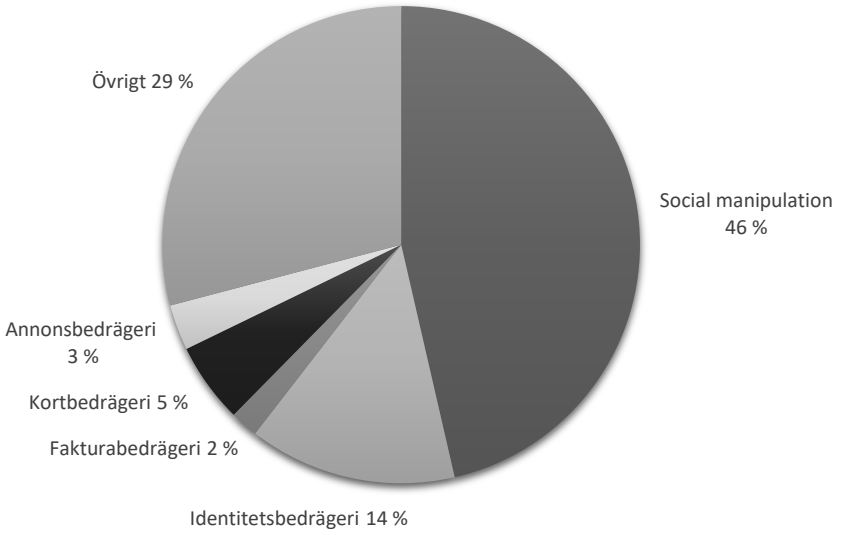
Störst brottsvinster för bedrägerier genom social manipulation

Nationellt bedrägericentrum (NBC) uppskattar brottsvinster för bedrägerier utifrån brottsanmälningar och konstaterar att bedrägerier genom social manipulation genererar de största brottsvinsterna. Där ingår investerings- och romansbedrägerierna som utgör en förhållandevis liten del av alla anmälda bedrägerier, med enbart cirka 2 500 respektive 1 300 anmälningar år 2022, samtidigt som de uppskattas stå för 21 respektive 10 procent av de sammanlagda brottsvinsterna (1,2 miljarder respektive 610 miljoner kronor år 2022). I social manipulation ingår även telefonbedrägerierna där brottsvinsterna har ökat markant de senaste åren, från cirka 156 miljoner kronor år 2020 till knappt 620 miljoner kronor år 2022. Kort- och annonsbedrägerierna omfattar däremot en mindre andel av de sammanlagda brottsvinsterna, drygt 315 miljoner respektive cirka 180 miljoner kronor i brottsvinster år 2022. Det kan i stor utsträckning förklaras av att brottsvinsterna vid varje kort- liksom annonsbedrägeri i regel är relativt låga.

Figur 3 Fördelning av anmälda bedrägeribrott 2022 (%). Källa: Brå 2023.



Figur 4 Fördelning av brottsvinster 2022 (%). Källa: Polismyndigheten 2023a.



Tillvägagångssätt vid bedrägerier

Som nämndes i inledningen är den bedrägliga transaktionen enbart en liten del av en längre kedja av händelser. Det är därför viktigt att se till hela händelsekedjan för att förstå brottsproblemet bedrägeri, vilka sårbarheter som är kopplade till bedrägerier och vilka insatser som behövs för att förebygga bedrägerierna. Det inkluderar förberedelserna inför ett bedrägeri och hur bedragarna tar kontakt med potentiella brottsoffer, vilka vilseledande strategier de använder för att förmå brottsoffret att föra över pengar (själva bedrägeriet) och bedragarnas hantering av brottsvinsterna. I det här avsnittet beskrivs olika bedrägerityper utifrån dessa premisser.

Som framgått här finns det olika typer av bedrägerier genom social manipulation, där brottskoderna inte helt överensstämmer med hur de i övrigt beskrivs i intervjuer och i det skriftliga materialet. I många fall är det mer relevant att utgå från tillvägagångssätten än brottskoderna, och det är därför utgångspunkten i våra beskrivningar. Se även sammanställningen i tabell 1 i slutet av kapitlet.

Telefonbedrägerier

En typ av social manipulation är telefonbedrägerier – också kallat vishing – där brottsoffren kontaktas via telefon och blir lurade att göra en transaktion eller lämna ifrån sig uppgifter som möjliggör för bedragaren att göra en transaktion.

Förberedelser och kontaktskapande

Telefonbedrägerierna föregås vanligtvis av en översiktlig kartläggning av potentiella brottsoffer för att välja ut lämpliga personer och för att få information som ger bedragaren trovärdighet i sin kontakt med dessa. Det förekommer även mer omfattande förarbeten genom dataintrång för att få information om och selektera en mindre grupp tilltänka offer (så kallat ”spear phishing”). Trovärdigheten förstärks även genom manipulerade telefonnummer, så kallat ”spoofade” nummer. Det innebär att bedragarens samtal kan se ut att komma från exempelvis en bank, polisen, en annan myndighet eller ett välkänt företag.

Vilseledande strategier (pitchar)

Vad bedragarna säger för att vilseleda brottsoffren – vilken så kallad pitch de använder – varierar över tid och brottsgruppering, och är även beroende av omvärldsläget och aktuella säkerhetsluckor. Till exempel kan bedragaren utge sig för att vara polis eller banktjänsteman och hävda att det pågår konstiga transaktioner på personens konto. Bedragaren kan också påstå att personen har en förfallen faktura eller inkassoskuld som måste betalas, att hen har blivit id-kapad eller ska få skadeersättning för ett tidigare brott som hen har utsatts för. Till yngre personer kan bedragarna enligt intervjuerna uppge att de måste uppdatera sina ungdomskonton till vuxenkonton.

Gemensamt för samtliga pitchar är att bedragaren försöker stressa och skrämma upp brottsoffret genom att ange att det är bråttom och att offret snabbt måste vidta någon åtgärd för att inte lida ekonomisk skada. Sedan erbjuder bedragaren sig att hjälpa till med åtgärden. Intervjupersonerna framhåller att bedragarna framstår som förtroendeingivande, hjälpsamma och vänliga, och att de ofta tillbringar lång tid i telefon med sina brottsoffer. Den föreslagna ”lösningen” inbegriper typiskt sett att personen ska identifiera sig med sin e-legitimation, logga in på sin internetbank med bank-id eller bankdosa, föra över pengar via Swish eller göra en vanlig bank- eller bankgiroöverföring. Bedragaren kan exempelvis säga att för att skydda eller få tillbaka sina pengar behöver personen föra över dem till ett säkert konto eller swisha ”stopp” och summan till den som försöker ta pengar från kontot. De kan även förmå brottsoffret att skapa ett nytt bank-

id genom att använda sin bankdosa eller sitt bank-id, alternativt ladda ner ett skärmdelningsprogram och dela sin skärm med bedragaren som i sin tur skapar ett nytt bank-id. Enligt flera intervjupersoner har det till följd av den tekniska utvecklingen skett en förskjutning från att brottsoffren tidigare släppt in bedragarna på sina konton, till att de själva genomför transaktionerna. Det har alltså gått från så kallade obehöriga till behöriga transaktioner.[13]

Det förekommer också så kallad fysisk vishing[14] där samtalet följs av ett fysiskt besök. Bedragaren kan till exempel säga att personen snabbt behöver åka till sin bank för att spärra sitt kort eller konto för att sedan erbjuda sig att skicka hem en bankman i stället. En annan pitch är att bedragaren påstår att den ringer från polisen och säger att det har skett ett inbrott hos grannen och uppmanar brottsoffret att hålla sig inne, kolla om alla värdesaker är kvar och vänta på att polisen ska komma. Väl inne hos personen ber bedragaren vanligtvis att få kort och kod och även andra värdesaker, såsom smycken.

Gärningspersonerna och penningtransaktionerna

Telefonbedrägerierna utförs enligt våra källor i stor utsträckning av personer med kopplingar till kriminella nätverk i Sverige. Dessa är organiserade i kluster som kan bestå av olika funktioner, inklusive en organisatör, personer som genomför telefonsamtalen och personer med teknisk kompetens. Flera av tjänsterna kan köpas av externa aktörer på dolda och oreglerade delar av internet (darkweb). Intervjupersoner beskriver exempelvis att det finns penningtvättsnätverk eller målvaktspooler som bidrar med målvakter, det vill säga personer som kan stå på konton, swishnummer och företag. Pengar förs typiskt sett över till målvaktskonton – antingen privatkonton eller företagskonton – för att sedan tas ut kontant eller föras vidare i flera led till olika konton i Sverige eller utomlands, till kryptoväxlar eller virtuella plånböcker. Enligt polisen finns det tecken på att unga utnyttjas som penningmålvakter. De berättar även att unga personer har använts vid hembesöken i den fysiska vishingen.

---

[13] En obehörig transaktion är när en transaktion görs utan konto- eller kortinnehavarens samtycke (t.ex. genom att kort- eller kortuppgifter stjäls och används eller att bedragaren kommer in på brottsoffrets konto och antingen själv kan genomföra transaktioner genom kapat bank-id eller lurar brottsoffret att godkänna transaktioner eller ge andra uppdrag till banken), medan en behörig transaktion är när brottsoffret genomför transaktionen helt själv (t.ex. vilseleds att själv swisha eller föra över pengar).

[14] Den här typen av förfaranden anmäls inte alltid som bedrägeri. Det gäller bland annat när stulna kort och kortuppgifter inte används. Enligt intervjuade poliser utreds den fysiska vishingen i vissa fall som stöld.

Social manipulation via sms, e-post eller sociala medier

Den här typen av social manipulation är när bedragaren kontaktar brottsoffret via sms, e-post eller sociala medier och lurar hen att genomföra en transaktion eller lämna ifrån sig kort- eller personuppgifter.

Förberedelser och kontaktskapande

Meddelandena skickas ofta ut till en stor mängd personer utan att föregås av något betydande kartläggningsarbete. Precis som vid telefonbedrägerierna förekommer dock att en mindre grupp potentiella brottsoffer väljs ut och kartläggs innan de kontaktas via e-post, sms eller på sociala medier. I vissa fall utger sig bedragarna för att vara personer med befogenhet, som myndigheter eller företag, medan de i andra fall utger sig för att vara någon brottsoffret känner, som en familjemedlem eller en vän. När brottsoffret kontaktas kan bedragaren ge sken av att vara någon annan genom manipulerade telefonnummer, snarlika eller kapade e-postadresser, eller kapade sociala mediekonton, och därmed öka sin trovärdighet. Bedragaren kan också studera hur exempelvis kapade personer brukar skriva med sina vänner på sociala medier för att framstå som mer trovärdig i kontakten med vännerna och lättare kunna bedra dem.

Vilseledandet och transaktionerna

När bedragaren utger sig för att vara någon med befogenhet är pitcharna ofta av enklare karaktär och består vanligtvis enbart av ett meddelande. Det kan exempelvis handla om sms eller e-postmeddelanden som ser ut att komma från en bank där mottagaren ombeds uppdatera sitt bank-id. Andra pitchar är meddelanden om att en faktura betalats två gånger med länk för återbetalning, eller ett meddelande som ser ut att komma från Skatteverket med länk till skatteåterbäring. Oavsett pitch inkluderar meddelandet i regel en länk eller ett telefonnummer som personen uppmanas klicka på eller ringa till. Syftet är oftast antingen att komma åt konto-, kort- eller inloggningsuppgifter, eller att placera en skadlig kod på personens dator eller telefon för att i ett senare led få tag på exempelvis lösenord och kortuppgifter. Uppgifterna kan sedan användas för att exempelvis kapa personens sociala mediekonton eller genomföra ett köp. Meddelandet kan alltså också vara en del i ett annat bedrägeri, till exempel det första steget i ett telefonbedrägeri, kort-, annons-, eller identitetsbedrägeri (se avsnitten *Kortbedrägerier*, *Annonsbedrägerier* och *Identitetsbedrägerier*).

I de fall bedragaren utger sig för att vara någon som brottsoffret känner, handlar det ofta om en något längre konversation via sms eller chattmeddelanden. Ett typexempel som beskrivs i intervjuerna är så kallade

barn- eller barnbarnsbedrägerier. Det kan börja med ett sms som inleds med ”hej mamma” följt av att ”barnet” uppger att hen har blivit av med sin telefon eller att telefonen är trasig och att hen behöver hjälp med att exempelvis betala en faktura. Ett annat exempel är när bedragaren har kommit över inloggningsuppgifter till en persons sociala mediekonto och kontaktar personens vänner. Bedragaren kan till exempel säga att hen hamnat i någon form av knipa och ber om ett lån eller annan hjälp som medför att vännen lämnar ifrån sig inloggningsuppgifter eller skickar pengar till bedragaren.

När det gäller hur gärningspersonerna är organiserade och penningtransaktionernas karaktär menar intervjuade poliser att sms-bedrägerierna har stora likheter med telefonbedrägerierna.

Romansbedrägerier

Vid romansbedrägerierna inleder bedragaren en kärleksrelation med brottsoffret i syfte att vilseleda hen till handlingar som skapar ekonomisk vinning för gärningspersonen.

Förberedelser och kontaktskapande

Enligt intervjuerna hittar bedragarna vanligtvis sina offer via sociala medier eller dejtingsidor. Typiskt sett använder bedragarna stulna eller falska bilder i sina profiler och ibland används också stulna filmer för att de ska verka mer trovärdiga i sin kontakt. Ofta förekommer inte något möte utan kontakten sker på distans, men den är frekvent och pågår under lång tid och upplevs av den bedragna som en stark och intim kärleksrelation. Relationsbyggandet används som strategi för att få offren att vilja föra över pengar till bedragaren i ett senare skede.

Olika vilseledande strategier mot kvinnor och män

I det typiska romansbedrägeriet mot kvinnor utger sig bedragaren för att vara exempelvis en manlig kirurg i ett krigsdrabbat land, sjökapten eller militär. Yrket gör det senare trovärdigt att personen plötsligt hamnar i en knepig situation och får akut behov av pengar. Det är vanligtvis ett yrke som både är traditionellt manligt, signalerar status och ger intryck av att personen har ekonomiska tillgångar. Syftet är att brottsoffret ska gå med på att tillfälligt hjälpa gärningspersonen genom att exempelvis betala en flygbiljett, sjukhusräkning, tullavgift eller borgensavgift. Det är ofta upprepade saker som händer och ett flertal olika transaktioner. Intervjupersoner beskriver att offren i romansbedrägerier i vissa fall vilseleds att investera i en falsk produkt och därmed också blir offer för ett

investeringsbedrägeri. I andra fall vilseleds offren att ta emot och skicka vidare pengar, och bidrar därmed till att tvätta vinster från ett annat bedrägeri.

Romansbedrägerier mot män beskrivs inte som lika vanligt som mot kvinnor. Även i dessa fall beskriver intervjupersoner att bedragarens pitch innebär att det akut uppstått behov av pengar. Pitchen handlar dock snarare om att bedragaren behöver hjälp med att betala en operation eller liknande, än om att bedragaren behöver låna pengar.

Pengarna går utomlands

Romansbedrägerierna är vanligtvis av internationell karaktär. Till exempel framställs att det är vanligt att callcenters utomlands används, att bedragarna kommunicerar på engelska och att pengarna försvinner utomlands. Finanspolisen beskriver att pengarna vid romansbedrägerierna i vissa fall först går till ett målvaktskonto i Sverige för att sedan skickas vidare utomlands genom kontoöverföringar, betalningstjänster eller betalningar via Swish och uttag i kontanter.

Investeringsbedrägerier

Investeringsbedrägerier mot privatpersoner innebär att en person vilseleds att investera pengar, ofta i någon typ av finansiell produkt som aktier, obligationer eller kryptovalutor.

Förberedelser och kontaktskapande

Förberedelserna inför ett investeringsbedrägeri inkluderar i regel upprättande av företag, webbplatser och annonser i syfte att skapa förtroende och tillit för produkten. Den vanligaste kontaktvägen vid investeringsbedrägerier är, enligt intervjupersonerna, att det potentiella brottsoffret ser en annons på en finansiell produkt, blir nyfiken, klickar på länken och anmäler intresse. Annonsen kan komma upp som ett sponsrat inlägg i sociala medier eller som en träff vid en aktiv sökning i en sökmotor. Den kan vara vinklad som att det är lite hemligt och speciellt, och inkludera falska rekommendationer från kända personer eller positiva omdömen från falska investerare. Ofta finns en länk till en webbplats med seriös framtoning och ibland även till falska myndighetssidor som visar att det bedrägliga företaget har tillstånd att förmedla finansiella produkter. Intervjupersoner beskriver också att bedragarna i vissa fall direkt vänder sig till en begränsad krets av personer som kan antas vara intresserade av att göra riskfyllda investeringar.

Vilseledandet och transaktionerna

Kort efter anmält intresse blir personen kontaktad. Bedragaren uppger sig för att vara placeringsrådgivare eller liknande och bygger upp ett förtroende genom att låta kunnig, hänvisa till webbplatser och intyg som verkar seriösa samt erbjuda olika former av garantier. Brottsoffret uppmanas inledningsvis att investera en relativt liten summa, såsom 2 500 kronor, och kan sedan genom ett eget konto till en till synes seriös webbsida följa hur investeringen ser ut att öka i värde. Bedragaren tar typiskt sett återkommande kontakt med brottsoffret under en längre tidsperiod för att övertala hen att göra ytterligare investeringar. Ofta uppger bedragaren att det är ett erbjudande och en möjlighet som bara gäller ”just nu”. Syftet är att brottsoffret inte ska hinna fundera, ta råd av någon eller göra ordentliga kontroller. När personen vill ta ut sina påstådda vinster är bedragaren ofta okontaktbar, alternativt övertalas personen i stället att göra ytterligare investeringar. Intervjupersoner beskriver också att det förekommer att personerna får ut en liten summa, för att på så sätt vilseledas att fortsätta investera i den falska produkten.

Nationellt bedrägericentrum (NBC) och Finansinspektionen beskriver att det är vanligt med en så kallad räddningsfas, efter att en person har insett att den har blivit lurad. Brottsoffret blir i dessa fall kontaktad av en person som till exempel utger sig för att vara en advokat, från ett försäkringsbolag eller en polis i ett annat land. Personen säger att den kan hjälpa brottsoffret att få tillbaka de förlorade pengarna mot en avgift, vilket innebär att brottsoffret återigen blir lurad på pengar.

I likhet med romansbedrägerierna ringer bedragarna i regel från callcenters utomlands och pratar engelska med brottsoffren. Pengarna går ofta till utländska kryptoväxlar genom att brottsoffret vilseleds att betala till en virtuell plånbok, eller till svenska företag som använder sig av penningmålvakter för att sedan skicka pengarna vidare till företag utomlands genom exempelvis osanna fakturor.

Kortbedrägerier

Kortbedrägerier är när en bedragare använder en persons kort eller kortuppgifter för att genomföra ett köp. Merparten av de anmälda kortbedrägerierna, cirka 80 procent, är utan fysiskt kort, så kallat CNP-bedrägeri (”card not present”), där enbart kortuppgifterna används för köp på internet.

Förberedelser och kontaktvägar

För att genomföra ett kortbedrägeri behöver bedragarna först komma över kortuppgifter eller kort med tillhörande pinkod. Det senare görs exempelvis genom att bedragaren ser över axeln när brottsoffret slår in sin kod och sedan stjäl brottsoffrets kort (så kallad ”shoulder surfing”), enbart stjäl kortet och använder det till små köp där det inte finns krav på pinkod eller vilseleder brottsoffret att lämna ifrån sig både kort och kod (se avsnittet *Telefonbedrägerier* om fysisk vishing). När det gäller CNP-bedrägerier föregås dessa vanligtvis av ett dataintrång. I vissa fall sker dataintrånget mot företag eller organisationer med stora register över kunder och kortuppgifter, där en stor mängd kortuppgifter stjäls för att sedan säljas vidare på ”darkweb”. I andra fall riktas dataintrånget direkt mot kortinnehavaren genom nätfiske,[15] genom falska annonser i sociala medier eller genom sökmotorer som länkar till webbplatser eller webbutiker som till synes är seriösa, där brottsoffren ombeds fylla i sina kortuppgifter. Webbutikerna kan se ut att vara svenska, med svenska domännamn och adresser.

Bedrägeriet och gärningspersonerna

I och med EU:s betaltjänstdirektiv (EU 2015/2366) finns sedan 2019 krav på stark kundautentisering[16] vid kortköp inom EU. Många av de bedrägliga kortköpen görs därför i webbutiker registrerade i länder utanför EU. Enligt polisen finns det också andra tillvägagångssätt för att komma runt kraven på stark kundautentisering, till exempel genom tecknande av abonnemang (se mer under avsnittet *Annonsbedrägerier*) eller genom flertalet köp med små belopp. Polisen beskriver också att betalningarna görs via e-plånböcker, betalningstjänster som inte kräver stark kundautentisering och på sidor där kunden redan har ett konto, vilket också skulle kunna tolkas som identitetsbedrägerier.

I materialet ges en samstämmig bild av att kortbedrägerierna i regel begås av utländska gärningspersoner. Även statistiken över anmälda brott visar att en majoritet av anmälda kortbedrägerier har en internationell anknytning (Brå 2023). Samma bild ges i en rapport av Europeiska centralbanken (ECB 2021). Polisen menar att det inom Sverige har skett en förflyttning av bedrägeribrottsligheten där samma grupper av gärnings-

[15] Se mer i avsnittet om social manipulation via sms, e-post eller sociala medier.

[16] Stark kundautentisering innebär att två av följande ska finnas för att det ska räknas som en giltig identifiering: någonting man kan (t.ex. kod), någonting man har (t.ex. kort, mobiltelefon) och unik egenskap (t.ex. fingeravtryck, ansikte). I Sverige har det i hög utsträckning uppfyllts genom att kunder använder bank-id eller annan e-legitimation.

personer som tidigare ägnade sig åt kortbedrägerier nu i stället genomför telefonbedrägerier (Polismyndigheten 2022b).

Annonsbedrägerier

Annonsbedrägerier – ibland kallat försäljningsbedrägerier – är när någon genom en annons vilseleds att betala för en vara eller tjänst som sedan inte levereras eller där det som levereras inte motsvarar informationen. Det kan också vara när den som publicerat en annons inte får betalning för en levererad vara eller på något annat sätt luras på pengar genom kontakt via annonsen.

Annonsbedrägerier på andrahandsmarknaden

Det typiska annonsbedrägeriet sker på digitala marknadsplatser där privatpersoner förekommer både som säljare och köpare. Vanligtvis behöver bedragaren innan bedrägeriet enbart skapa en falsk profil på den digitala marknadsplatsen och i vissa fall skapa en privatannons som läggs ut på sidan. De bedrägliga annonserna kan exempelvis vara på fordon, husdjur, elektronik eller babysaker. Ofta är priset förmånligt och bedragaren svarar snabbt och hävdar att det är bråttom då det finns många intressenter, vilket får brottsoffret att göra en förhandsbetalning. Efter betalningen går det inte längre att få kontakt med bedragaren och brottsoffret får aldrig varan. Vid annonser på större och dyrare varor, som maskiner och fordon, beskriver intervjupersoner att det är vanligt att bedragaren kan svara på detaljerade frågor och ge namn och adress på en person som rimligen kan ha lagt ut annonsen, såsom en bonde om det gäller en traktor, vilket skapar trovärdighet. Det förekommer även annonser på bostäder för andrahandsuthyrning, men där antingen ingen bostad finns eller där den hyrts ut mot förskottsbetalning till ett stort antal personer.

När det i stället är brottsoffret som lagt ut en annons på en digital marknadsplats, anger bedragaren typiskt sett att den inte själv kan komma och titta på och hämta varan utan att hen i stället kommer att skicka ett bud, men att en fraktkostnad behöver betalas i förskott. Något bud dyker dock inte upp och fraktkostnaden återbetalas inte som utlovat. Intervjupersoner beskriver också att personer som har lagt ut sin bil för försäljning blir erbjudna hjälp att sälja vidare bilen och förmås skriva över den på ett företag. Bilen säljs sedan vidare i flera steg, vilket medför att den ursprungliga ägaren varken får några pengar från försäljningen eller kan kräva att den beslagtas.

Vid samtliga betalningar beskriver intervjupersoner Swish som den vanligaste betalningslösningen, men det förekommer också att bedragarna skickar falska länkar som ser ut att gå till exempelvis marknadsplatsernas egna betaltjänster. I dessa fall kan det också bli ett kortbedrägeri då bedragaren efteråt kan använda brottsoffrets ifyllda kortuppgifter för ytterligare köp.

Annonsbedrägerier genom företagsannonser

En annan typ av annonsbedrägeri är genom företagsannonser eller annonser som ser ut att komma från företag. Dessa bedrägerier kräver mer förberedelser, eftersom webbplatser och ibland även företag behöver upprättas – i regel med målvakter som företrädare – och annonser behöver skapas och läggas ut på olika plattformar.

Brottsoffret ser vanligen en annons i sociala medier, en app, ett onlinespel eller en sökmotor, klickar på den och kommer till en webbutik där den gör en beställning och betalar med kort. Webbutikerna marknadsför typiskt sett enbart någon eller ett par enstaka produkter till ett väldigt lågt pris. Efter betalningen får brottsoffret dock ingen vara eller en vara av en helt annan kvalitet än den som har marknadsförts.

Det förekommer också så kallade ”abonnemangsfällor” och andra typer av vilseledande avtal, där en person ser en annons eller på annat sätt får ett erbjudande om en billig vara, en vinst eller liknande. När personen fyller i sina kortuppgifter för att få ta del av vinsten eller varan godkänner den dock samtidigt ett avtal om ett abonnemang som innebär att pengar dras varje månad från kortet. Intervjupersoner beskriver att det varierar i vilken mån avtalsvillkoren framgår som de ska och att gränsen mellan otillbörlig marknadsföring, vilseledande avtal och bedrägeri kan vara hårfin.

Både ensamma och organiserade gärningspersoner

Den samlade bilden från intervjuerna är att det nog både finns organiserade gärningspersoner bakom annonsbedrägerierna och de som agerar ensamt och relativt spontant. De ensamma gärningspersonerna beskrivs som relativt ”lokala”, medan de organiserade annonsbedrägerierna i stor utsträckning verkar ske från andra länder än Sverige. Det senare gäller bland annat företagsannonserna, abonnemangsfällorna och de tillvägagångssätt där falska betalningslösningar används.

Identitetsbedrägerier

Identitetsbedrägeri – ibland kallat kreditbedrägeri – är när någon utan lov använder någon annans identitet för att genomföra ett köp eller ta ett lån. Enligt intervjuerna riktas en del av identitetsbedrägerierna mot företag och kreditgivare. När privatpersoner är brottsoffer handlar det i stor utsträckning om att deras identiteter eller personuppgifter kapas och används för att genomföra köp eller ta krediter. Som nämnts tidigare kan telefonbedrägerierna i vissa fall resultera i ett identitetsbedrägeri eller i olovlig identitetsanvändning genom att bedragaren skapar ett nytt bank-id i personens namn. För att undvika att den utsatta personen upptäcker att hens identitet har använts, berättar intervjupersoner att bedragaren kan hänvisa personens post genom en tillfällig eftersändning så att kreditupplysningar med mera inte kommer fram till den utsatta.

Kapade identitetsuppgifter kan också vara en länk i en längre händelsekedja inför och efter bedrägeriet. Det handlar exempelvis om att id-kapade personer får stå på företag, domäner eller telefonabonnemang, eller att personernas sociala mediekonton kapas och används för att bedra personens vänner (se avsnittet *Social manipulation via sms, e-post eller sociala medier*). Det förekommer även så kallat ”friendly fraud”, alltså när den som påstår sig ha utsatts för bedrägeriet och vars identitet har använts är med på upplägget och den verkliga målsägaren exempelvis är kreditgivaren.

Enligt polisen finns det kopplingar mellan identitetsbedrägerier och organiserad brottslighet i Sverige (Polismyndigheten 2021).

Fakturabedrägerier

Fakturabedrägerier är när någon vilseleds att betala en faktura för en vara eller tjänst som den inte har beställt, till exempel så kallade bluffakturor. I likhet med identitetsbedrägerierna riktas en del av fakturabedrägerierna mot företag, organisationer och offentlig sektor. Också när de riktas mot privatpersoner kan företag dock vara inblandade på så sätt att de osanna fakturorna skickas ut från e-postadresser kapade från företag. Enligt intervjuerna förekommer det också att fakturorna skickas ut efter ett telefonsamtal där bedragaren uppger att den har ett bra erbjudande om exempelvis ett el- eller telefonabonnemang. I likhet med de vilseledande avtalen som resulterar i en så kallad ”abonnemangsfälla” kan bedragarna vilseleda personer att på det sättet skriva på avtal eller tacka ja till ett erbjudande som sedan innebär att personen får hem en eller flera fakturor.

Också fakturabedrägerier har enligt polisen kopplingar till organiserad brottslighet i Sverige (Polismyndigheten 2021).

Brottsoffren och skador

Äldre drabbas särskilt av social manipulation

Många av de som drabbas av bedrägerier genom social manipulation är äldre personer. Andelen anmälda bedrägerier genom social manipulation mot äldre eller funktionsnedsatta har också ökat över tid, från 47 procent 2019 till 62 procent 2022.[17] För befogenhetsbedrägerier specifikt har andelen anmälda brott mot äldre motsvarande period ökat från 55 procent till 76 procent (Brå 2023). Enligt intervjupersonerna i den här rapporten är det särskilt telefonbedrägerierna som riktas mot och drabbar äldre personer, från 70–80 år och uppåt. Intervjupersoner inom polisen beskriver också att bedragarna i vissa fall har inriktat sig enbart på personer över 90 år, exempelvis vid den fysiska vishingen. Barn- och barnbarnsbedrägerier samt romans- och investeringsbedrägerier tycks i stället drabba främst personer i övre medelåldern eller nyblivna pensionärer.

Det finns en samsyn bland intervjupersonerna om att telefonbedrägerier, och andra bedrägerier genom social manipulation med en överrepresentation av äldre brottsoffer, i högre utsträckning drabbar kvinnor än män. Också romansbedrägerierna beskrivs drabba fler kvinnor än män. Vid investeringsbedrägerier är dock den allmänna bilden att män är överrepresenterade.

Det finns även exempel på att specifika språkgrupper drabbas särskilt av bedrägerier genom social manipulation, där bedragaren använt ett gemensamt minoritetsspråk för att skapa tillit. Därtill beskrivs att bedragarna i telefonbedrägerierna i vissa fall söker på adresser i förmögna områden för att rikta bedrägerierna dit.

Övriga bedrägerier drabbar främst andra grupper

När det gäller kort- och annonsbedrägerierna finns det en samsyn bland intervjupersonerna om att dessa främst drabbar personer i arbetsför ålder. Motsvarande bild framkommer även i NTU där andelen som rapporterat utsatthet för försäljningsbedrägeri är lägst i de äldsta åldersgrupperna. Av

[17] I statistiken inkluderar kategorin både äldre och funktionsnedsatta. Intervjupersoner inom polisen menar dock att det är få personer med funktionsvariationer som ingår i kategorin. Intervjupersoner från seniororganisationer understryker också att det finns en stor variation inom gruppen äldre.

NTU framgår också att utsattheten för såväl kort- som annonsbedrägerier är något högre bland personer med utländsk bakgrund än bland personer med svensk bakgrund. När det gäller identitets- och fakturabedrägerierna finns det ganska lite information om särskilt utsatta brottsoffer, utöver det att de i vissa fall riktas specifikt till företag.

En allmän uppfattning bland intervjupersonerna är att barn och unga inte faller offer för bedrägerier i särskilt stor utsträckning. När de drabbas handlar det dock typiskt sett om situationer som främst gäller yngre personer, såsom snabba köp i onlinespel, i sociala medier eller på köp- och säljsidor. Det förekommer också att unga utsätts för bedrägerier genom förfrågningar via kapade konton på sociala medier eller genom en målgruppsanpassad pitch i telefonbedrägerier.

Stora skador vid bedrägerier – särskilt vid social manipulation

De individuella skadorna vid ett bedrägeri beror mycket på vilken typ av bedrägeri som brottsoffret utsätts för. De ekonomiska skadorna vid kort- och annonsbedrägerierna är förhållandevis små; ofta handlar det om belopp mellan hundra och några tusen kronor. Dessutom ersätter bankerna normalt förlorade belopp vid kortbedrägerier. Bedrägerier genom social manipulation kan i stället leda till mycket stora ekonomiska skador för brottsoffren, som kan bli lurade på tiotusentals till flera miljoner kronor, summor som i de flesta fall inte ersätts.[18]

Ett återkommande tema i intervjuerna är att de som utsätts för bedrägerier genom social manipulation också skäms mycket över att ha blivit lurade. I vissa fall resulterar skammen och skuldkänslorna i att de inte vill eller vågar berätta varken för anhöriga, vänner eller polisen om vad de har utsatts för. Det gäller enligt intervjuerna särskilt romansbedrägerier eftersom personerna blir dubbelt lurade – både på pengar och kärlek. Några intervjupersoner menar att det även kan gälla äldre personer, som inte vill bli beskyllda för att vara glömska, virriga eller dementa. En liknande bild framkommer i Brå-rapporten *Brott mot äldre* (2018) där det beskrivs att äldres brottsutsatthet för bland annat bedrägerier fått långvariga psykiska efterverkningar.

Därtill kan bedrägerierna skapa ökad otrygghet. Enligt intervjuerna gäller också det framförallt äldre personer, som kan begränsa eller förändra sitt

[18] Sedan en HD-dom 2022 har bankerna dock börjat ersätta brottsoffer för vissa obehöriga transaktioner (se vidare i kapitel 4).

beteende till följd av rädsla för att utsättas för bedrägerier. Samma bild framkommer i NTU (Brå 2022a) där 40 procent i gruppen 75–84 år rapporterar oro för bedrägeri i samband med internetköp. Det kan exempelvis jämföras med 23 procent i gruppen 16–19 år. Enligt *Svenskarna och internet* är det 40- och 50-talister som begränsar sig mest (runt 60 procent) i sin internetanvändning på grund av otrygghet, vilket bland annat inkluderar oro för nätbedrägerier (Internetstiftelsen 2022). Samma undersökning visar att kvinnor begränsar sin internetanvändning mer på grund av oro än vad män gör.

Möjligheten att genomföra bedrägerierna, liksom den låga uppklarningsgraden, kan påverka människors benägenhet att använda såväl digitala finansiella tjänster som samhällstjänster, och i förlängningen även skada befolkningens tilltro till samhällets institutioner och system. Utöver den individuella skadan kan bedrägerierna därmed få allvarliga konsekvenser på samhällsnivå.

Sammanfattande tabell över typiska tillvägagångssätt

I tabell 1 sammanfattas de typiska tillvägagångssätten vid bedrägerier mot privatpersoner som har beskrivits i det här kapitlet. Tabellen inkluderar även typiska brottsoffer.

Tabell 1 Typiska tillvägagångssätt vid bedrägerier mot privatpersoner

Brottstyp	Förberedelser inför kontakt	Bedrägeriet/ vilseledandet	Transaktionen	Typiska brottsoffer
Telefonbedrägeri	Kartläggning av brottsoffer, manipulerade telefonnummer	Vilseledande telefonsamtal	Bank-transaktioner (inkl. Swish)	Äldre
Social manipulation via sms, e-post eller sociala medier	Falska & kapade e-postadresser & sociala mediekonton, manipulerade telefonnummer	Vilseledande sms-, e-post- & chatt-meddelanden	Bank- & betal-transaktioner	Vuxna (inkl. övre medelåldern), barn & unga
Romansbedrägeri	Falska profiler på sociala medier	Vilseledande kärleksrelation	Transaktioner utomlands	Kvinnor i övre medelåldern
Investerings-bedrägeri	Oseriösa företag, webbplatser & annonser	Vilseledande investerings-erbjudande	Transaktioner utomlands	Män i övre medelåldern
Kortbedrägeri	Dataintrång eller stulna kort & pinkoder	Kort- & pinstöld, fysisk vishing	Korttransaktioner	Vuxna
Annonsbedrägeri	Oseriösa annonser, företag, webbplatser	Vilseledande annonser/kontakt	Bank- & kort-transaktioner (inkl.	Vuxna, barn & unga

Brottstyp	Förberedelser inför kontakt	Bedrägeriet/ vilseledandet	Transaktionen	Typiska brottsoffer
	& sociala mediekonton	genom annonser	Swish)	
Identitetsbedrägeri	Dataintrång, telefonbedrägeri		Betaltransaktioner & krediter	Vuxna, företag
Fakturabedrägeri	Osanna fakturor, falska & kapade e-postkonton	Vilseledande fakturor eller erbjudanden	Fakturabetalningar	Vuxna, företag, offentlig sektor

3. Sårbarheter

I det här kapitlet redovisas de sårbarheter som vi har identifierat utifrån kartläggningen av brottsproblemet som har beskrivits i kapitel 2. Med sårbarheter menar vi de omständigheter och situationer som möjliggör genomförandet av bedrägeriet. Vissa av sårbarheterna är generiska och gäller för i stort sett samtliga typer av bedrägerier, andra är väldigt specifika och endast giltiga vid vissa typer av tillvägagångssätt. De olika sårbarheterna är inte heller oberoende utan kan förutsätta eller förstärka varandra. I slutet av kapitlet finns en figur som visar hur olika sårbarheter aktualiseras i olika steg av den händelsekedja där bedrägeriet ingår.

Öppna källor och dataintrång möjliggör kartläggning av potentiella brottsoffer

I kapitel 2 framkommer att bedrägerier många gånger föregås av någon form av kartläggning, dels för att välja ut lämpliga brottsoffer, dels som information att använda för att bli trovärdig i vilseledandet. Kartläggningar möjliggörs bland annat genom att uppgifter om namn, adress, exakt lägenhetsdörr, ålder, familjesituation och fordonsinnehav finns tillgängliga på olika öppna källor på internet. Mot en avgift går det också att få uppgifter om fullständigt personnummer och inkomst. Så länge webbplatserna har ett så kallat utgivningsbevis skyddas publiceringen av personuppgifter av yttrandefrihetsgrundlagen. En enskild individ kan vända sig direkt till en webbplats och be att få sina uppgifter borttagna, men webbplatsen behöver inte följa den enskildas önskan (Integritetsskyddsmyndigheten 2023, Myndigheten för press, radio och tv 2023). Flera intervjupersoner nämner den lättillgängliga informationen som en sårbarhet, särskilt vad det gäller bedrägerier genom social manipulation mot äldre.

Enligt flera intervjupersoner förekommer det även att uppgifter som inte är offentliga om potentiella brottsoffer, som banktillhörighet, inhämtas genom dataintrång. I dessa fall är det någon form av otillräcklig informationssäkerhet (teknisk eller mänsklig) som är sårbarheten och som möjliggör tillgången till uppgifterna.

Manipulering av avsändare vilseleder redan i kontaktförsöket

Att bedragare kan manipulera vilket telefonnummer eller vilken avsändare som visas i kontakten med det potentiella brottsoffret, så kallad ”spoofing”, är också en tydlig sårbarhet. Genom att bedragaren kan ge sken av att vara någon annan, såsom en bank, en myndighet eller en investeringsmäklare, har vilseledandet påbörjats redan innan det potentiella brottsoffret lyft på luren, öppnat sms:et, öppnat e-postmeddelandet eller klickat på länken. Därmed ökar också sannolikheten för att bedragaren ska lyckas övertyga det potentiella brottsoffret med sin ”pitch”. Många gånger är det dessutom förknippat med stora svårigheter för brottsoffret att kontrollera avsändarens äkthet.

Det finns ett flertal olika tekniska lösningar som möjliggör den här typen av manipulation av vilket telefonnummer som visas hos mottagaren vid samtal och sms. Vid samtal via virtuella telefonväxlar från utländska callcenters eller via utländska servrar kan bedragaren välja vilket nummer som ska visas för mottagaren, exempelvis ett lokalt nummer som skapar trovärdighet eller ett nummer som tillhör eller liknar numret till en specifik aktör, till exempel en bank.[19] Det finns även onlinetjänster och applikationer för att välja vilket telefonnummer som ska visas hos mottagaren vid samtal samt vid sms. När det gäller sms kan dessa lägga sig i direkt anslutning till riktiga sms från samma aktör. Vilseledande avsändarnamn vid e-postadresser manipuleras inte på samma sätt genom tekniska tjänster utan styrs fritt av avsändaren. Bedragare kan också genom intrång kapa existerande e-postkonton eller konton på sociala medier och utge sig för att vara en specifik person som brottsoffret dessutom eventuellt redan känner.

Ett annat sätt är att registrera domäner och därmed e-postadresser som är snarlika en känd trovärdig avsändare, exempelvis en myndighet, bank eller ett annat företag där mottagaren är kund.

Konstruktionen av domännamn används även för att skapa trovärdighet för webbplatser, länkadresser och för olika former av falska annonser med varor och tjänster. Bedragarna kan till exempel byta ut en bokstav i domännamnet eller registrera allmänt hållna domännamn som till exempel uppdatera, AB eller info, för att sedan lägga till en subdomän med samma

[19] Att bedragaren använder ett liknande nummer blir aktuellt när den specifika aktören spärrat numret mot manipulerade telefonnummer. Se vidare i kapitel 4.

namn som ett existerande företag eller en myndighet. För den som inte vet hur domäner är uppbyggda kan webbplatsen på så sätt se ut att tillhöra företaget eller myndigheten. Webbplatserna kan användas för bland annat oseriösa webbutiker och oseriösa webbplatser för finansiella tjänster samt som platshållare för ytterligare förtroendemarkörer såsom falska certifieringar, tillstånd och kundomdömen. Ibland finns det ett existerande företag kopplat till domännamnet. I dessa fall företräds företagen typiskt sett av målvakter. Sårbarheten här är att det är relativt enkelt att registrera en ny domän och ett nytt företag, liksom att publicera annonser, och att de kontroller som görs inte räcker till. Enkelheten att starta företag och att ha målvakter som företrädare relaterar även till andra aspekter än vilseledandet (se avsnittet *Tillgång till utförare och kompetens* om transaktioner till företag).

En digital bank- och betalmarknad möjliggör bedrägerier

Att bankärenden sker digitalt och i regel är obevakade av bankpersonal är en självklar förutsättning för flera typer av de bedrägerier som beskrivs i kapitel 2. Det är också en omständighet som tas upp av flera intervjupersoner. De digitala banktjänsternas flexibilitet och smidighet möjliggör en mängd transaktioner varje dag. Kopplat till det finns ett flertal konkreta sårbarheter:

- *Bedrägliga transaktioner stoppas inte av bankernas övervakningssystem*. Bankerna har övervakningssystem där misstänkta transaktioner flaggas och kontrolleras och ibland stoppas. Trots den övervakning som sker förekommer bedrägliga transaktioner som avviker från kunders tidigare beteenden och transaktionsmönster. Det kan till exempel vara överföringar (till privata konton eller företag) av ovanligt stora belopp till en ny mottagare, ett stort antal upprepade bedrägliga transaktioner av små belopp till en eller flera nya mottagare, oväntade internationella transaktioner, transaktioner vid avvikande tider på dygnet och så vidare.
- *Fragmenterat förlopp*. Vid många typer av transaktioner är förloppet uppdelat och de olika inblandade aktörerna har bara kontroll över det steg i kedjan som de själva hanterar, till exempel Bank-id, banken och Swish. Att ingen aktör har hela bilden försvårar identifierandet av bedrägliga transaktioner.

- *Snabba betallösningar och transaktioner*. Flera intervjupersoner uttrycker att samhället har förväntningar och ställer krav på att transaktioner och betalningar ska gå snabbt. Det finns också olika lösningar och tjänster för att hantera snabba och direkta transaktioner, dels särskilda tjänster som Swish, dels rutiner för transaktioner mellan konton. De snabba transaktionerna gör det svårare att identifiera och stoppa bedrägliga transaktioner liksom att spåra pengarna vid genomförda transaktioner. Kryptovalutor, virtuella plånböcker och så kallade ”open banking”-tjänster[20] är enligt flera intervjupersoner också lösningar som gör det svårare att spåra och stoppa bedrägliga transaktioner.
- *Enkelt att ändra satta gränser*. I de tjänster som går att begränsa, till exempel beloppsgränser i Swish, är det relativt enkelt att själv justera de satta gränserna utan någon förstärkt identitetskontroll eller fördröjning.

Sårbarheter avseende identifikation

Möjligheter att nyttja någon annans identitetshandling är en allvarlig sårbarhet eftersom det öppnar upp för ett flertal möjliga bedrägerier. En särskilt viktig nyckel är inloggningen och signeringar av uppdrag (godkännanden av transaktioner) i internetbanken liksom att från internetbanken utfärda ett nytt mobilt bank-id till en ny enhet.

En aspekt av sårbarheten är att det i vissa fall går att logga in på internetbanken på distans, det vill säga att den som får åtkomst till internetbanken befinner sig på en annan plats än den som gör identifieringen. Det innebär att bedragaren kan komma in på brottsoffrets internetbank genom att vilseleda personen att ge ifrån sig koder från en bankdosa eller signera med bank-id. Bank-id är generellt säkrare än bankdosor, men det finns banker som inte implementerat Bank-id:s samtliga tillgängliga säkerhetslösningar. Att använda skärmdelningsverktyg är också ett sätt för bedragarna att komma in i brottsoffrets internetbank och på så sätt runda de säkerhetslösningar som finns.

[20] ”Open banking” är ett system som innebär att andra aktörer än bankerna kan förmedla transaktioner. Det möjliggörs genom API:er som ger tredje part tillgång till bankernas information. I och med att transaktionen går genom en tredje part innebär det att den bank där kontot som pengarna skickas från inte har information om vilket det mottagande kontot är och mottagande bank på motsvarande sätt inte har information om vilken bank och vilket konto som pengarna kommer från.

Andra sårbarheter avseende identifiering är internetbaserade kortköp som inte omfattas av betaltjänstdirektivet (EU 2015/2366). Som framgått tidigare gäller det butiker utanför EU. Dessutom finns det undantag från kraven på stark kundautentisering inom EU för vissa typer av abonnemang och låga belopp. Det senare gäller även för fysiska kortköp. Vid köp av fysiska varor är ytterligare ett sårbart moment själva identifieringen när en vara hämtas ut, eftersom det inte alltid krävs att personen visar sin id-handling och att den granskning av id-handlingar som görs är manuell. Även vid köp via betalningsförmedlare är kraven på identifiering inte alltid lika strikta och i vissa fall baseras säkerheten på frivilliga val. Några intervjupersoner har även tagit upp att vissa kreditgivare inte kräver stark identifikation vid ansökan om lån och för att göra en kreditupplysning.

Bristande identitetskontroller kan också vara något som möjliggör olika typer av förberedelser för bedrägeri. Bland annat är det möjligt att göra en tillfällig eftersändning av post utan att identifiera sig vilket gör det svårt för personer som utsatts för identitetsbedrägeri att upptäcka att krediter tagits i deras namn. Det finns ett antal valbara tilläggstjänster som privatpersoner kan skaffa för att minska risken för identitetsmissbruk, men de kräver alla en aktiv handling av individen. En annan del är bristande identitetskontroll vid publiceringen av privata annonser på digitala marknadsplatser eller vid skapande av konton på sociala medier. Det finns även en koppling till den bristande kontrollen vid registrering av domäner och företag som nämnts i avsnittet *Manipulering av avsändare vilseleder redan i kontaktförsöket*.

Tillgång till utförare och kompetens

En förutsättning för att bedrägerier ska kunna genomföras är att gärningspersonerna har tillgång till personer, information, tjänster och kompetenser, för att förbereda och genomföra bedrägeriet och för att tillgängliggöra brottsvinsten. Dessa förutsättningar ingår inte självklart i begreppet sårbarheter, men eftersom de är en del av vad som möjliggör bedrägeriet inkluderas de ändå här som en del av rapportens breda användning av sårbarhetsbegreppet.

Beroende på typ av bedrägeri och tillvägagångssätt kan det som ett led i förberedelserna krävas tillgång till målvakter som kan stå som ägare av företag eller innehavarare av domäner eller telefonabonnemang. Det kan också behövas information om potentiella brottsoffer, om bankernas varierande säkerhetslösningar och hur sårbarheter bäst utnyttjas. Därtill kan bedragarna behöva mer avancerade kompetenser för att planera ett

komplicerat brottsupplägg, kanske med vissa tekniska element, såsom upprättandet av avancerade webbsidor för ett investeringsbedrägeri. Vid telefonbedrägerier och investeringsbedrägerier behövs även personer med god social förmåga som kan genomföra de vilseledande samtalen. Flera intervjupersoner beskriver att det finns en illegal marknad för olika delar av ett brottsupplägg, där man kan köpa in de resurser och kompetenser som behövs på ”darkweb”.

När det gäller tillgängliggörandet av brottsvinster handlar det om att pengarna som brottsoffren bedras på måste ta vägen någonstans. Tillgången till penningmålvakter är i det sammanhanget en förutsättning i flera bedrägerier. Det behövs alltså personer som kan stå som mottagare för transaktionerna för att sedan skicka vidare pengarna till andra penningmålvakter, ta ut pengar kontant, skicka vidare utomlands eller på annat sätt placera pengarna så att de tappar spårbarhet samt blir tillgängliga för dem som ska ta del av brottsvinsten. Flera intervjupersoner berättar att det är vanligt att penningtvättsnätverk eller målvaktspooler används, och att särskilt värdefull är tillgången till ostraffade personer, liksom tillgången till dem som har konton i samma bank som det potentiella brottsoffret för att överföringen ska gå snabbt. Ofta handlar det om unga personer som inte alltid förstår hur allvarlig brottslighet de bidrar till när de accepterar att ta emot och lämna vidare pengar eller lånar ut sitt bank-id.

Sårbarheter hos potentiella brottsoffer

Bedrägerier mot privatpersoner handlar i grunden om att vilseleda en människa och det blir därför centralt att förstå sårbarheterna hos potentiella brottsoffer. Det handlar om att olika faktorer kan göra individer mer eller mindre sårbara för att känna tillit till bedragaren eller för att någon med bedrägligt syfte ska kunna bygga upp ett tillräckligt förtroende.

Äldre är särskilt sårbara

En sådan sårbarhetsfaktor som nämns av flera intervjupersoner är okunskap om och ovana vid att använda digitala tjänster, vilket är något som många gånger är särskilt aktuellt hos de allra äldsta delarna av befolkningen. Vid telefonbedrägerier mot äldre handlar det till exempel om okunskap om att man inte kan stoppa en transaktion genom Swish, att man genom att acceptera en skärmspegling släpper in någon på sin dator, och vad det innebär för risker att på uppmaning av någon logga in på sin internetbank. Det handlar också om att det nummer som visas på

nummerpresentatören inte är tillförlitligt, att avsändarnamn vid e-post inte är detsamma som avsändaradress, hur ett domännamn är uppbyggt och så vidare. Okunskap och ovana kan också göra att man blir mer lättstressad vilket utnyttjas av bedragare. Den här sårbarheten är också något som bekräftas i rapporten *Brott mot äldre* (Brå 2018b) där intervjuade brottsutsatta uttrycker att de haft begränsade kunskaper när det gäller den tekniska utvecklingen och beteendet på internet, och att det ökat risken för att bli lurad.

Andra sårbarheter som flera intervjupersoner menar är särskilt förknippade med äldre är svårigheter att ta till sig stora mängder ny information, nedsättningar i syn, hörsel och rörelse, samt en större benägenhet att lyssna på auktoriteter och en vilja att vara tillmötesgående och trevlig. Det senare är också något som framkommer i Brås rapport *Brott mot äldre* (Brå 2018b s. 12) där äldre brottsoffer uttrycker att de ”haft en allt för hög grad av god tro och brist på sund skepticism”. Några av intervjupersonerna i den här studien menar att den typen av sårbarhet också är särskilt förknippad med kvinnor och att kvinnor därför är mer utsatta för bland annat telefonbedrägerier. Andra hävdar att förklaringen till kvinnors överrepresentation ligger i att de lever längre än män och att det finns fler äldre ensamma kvinnor än män, liksom att bedragarna i högre utsträckning riktar sina bedrägeriförsök mot kvinnor. Det finns också några intervjupersoner som menar att den stora utsattheten hos äldre inte handlar om deras egenskaper eller oförmåga att skydda sig utan helt enkelt om att äldre personer generellt har mer pengar på banken än yngre personer.

Många sårbarheter hos potentiella brottsoffer gäller oavsett ålder

Flera av sårbarheterna hos potentiella brottsoffer är aktuella oavsett åldersgrupp. Särskilt tydligt är att gärningspersonerna i flera typer av bedrägerier använder stress och människors benägenhet att agera mindre rationellt i stressade situationer, liksom att brottsoffren inte ska hinna rådgöra med någon tredje part. I vissa fall handlar stressen om rädsla för att någonting farligt ska hända om man inte tar emot den falska hjälp som gärningspersonen erbjuder. I andra fall framställs det som bråttom att till exempel göra en bra investering eller ett bra köp och då handlar stressen om att man inte vill gå miste om att göra en bra affär eller att tjäna pengar. När det gäller bra investeringar menar flera intervjupersoner att män är en särskilt sårbar grupp. Några intervjupersoner menar att det i viss mån är människors girighet som gör dem sårbara i den här typen av situationer.

Andra egenskaper eller omständigheter hos individen som kan göra en person sårbar är ensamhet och ett behov av bekräftelse, förståelse, närhet och kärlek, vilket ofta är fallet i romansbedrägerierna. Det kan också handla om nyfikenhet eller en längtan efter spänning, men även om ett medvetet risktagande och en bristande motivation att göra tillräckliga kontroller, eller att inte ha tillräckligt säkra lösenord och andra säkerhetslösningar. Risktagande kan också vara förknippat med omständigheter som gör personer desperata, exempelvis efter en bostad, pengar eller en produkt till ett bra pris.

Beteendemönster kan förklara variationer i utsatthet

Att kort- och annonsbedrägerier främst drabbar personer i arbetsför ålder kan sannolikt i hög grad förklaras av olika gruppers beteendemönster. Exempelvis framgår det av Internetsstiftelsens rapport *Svenskarna och internet* att nästan samtliga personer födda på 70-, 80- och 90-talet har e-handlat det senaste året och att andelen i de äldre grupperna är betydligt lägre (Internetstiftelsen 2022). En intervjuperson inom polisen nämner att de sett särskilda risker att utsättas för kortstöld med efterföljande kortbedrägeri i samband med krogbesök och alkoholpåverkan.

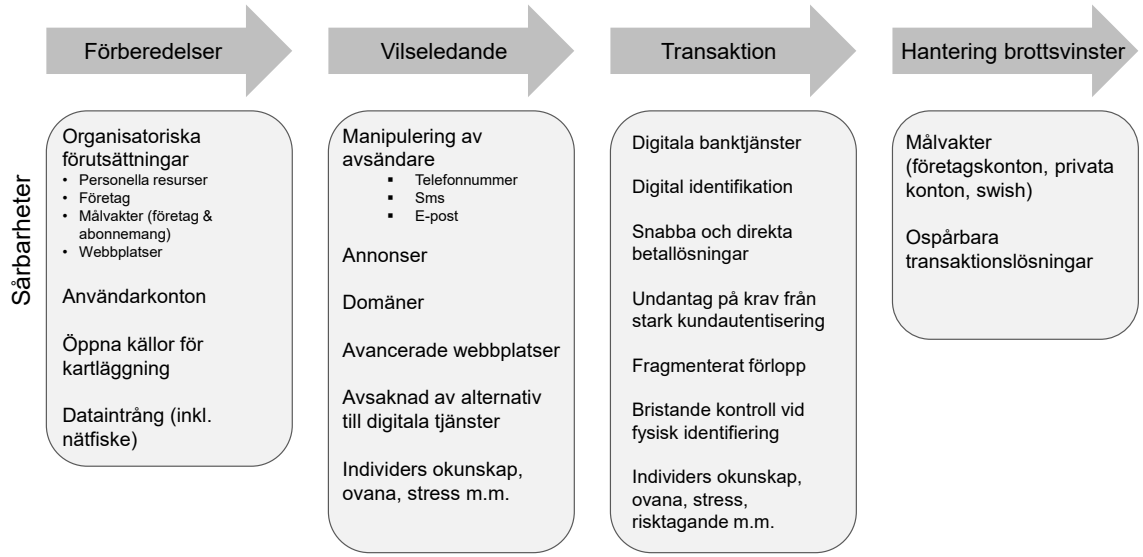
Som nämnts tidigare bedöms barn och unga inte vara en särskilt sårbar grupp, vilket förklaras med att de vanligtvis inte har stora ekonomiska tillgångar. I de fall de utsätts handlar det dock också i stor utsträckning om deras beteendemönster: att de befinner sig på sociala medier, spelar online-spel och e-handlar.

Avsaknad av tillgängliga alternativ till digitala tjänster

Personer som saknar vana, kunskap och många gånger vilja att använda digitala tjänster hade i hög grad antagligen valt bort digitala tjänster om det funnits andra alternativ som fungerade för dem. På så sätt blir det en sårbarhet att det finns få fysiska bankkontor, många kontantfria butiker och tjänster liksom att såväl marknadsföring och viktig information samt avtal många gånger skickas och tecknas via e-post, sms eller samtal. Att människor i stor utsträckning kommunicerar med varandra via skriftliga meddelanden (sms och chattar) i stället för att ringa är en annan aspekt. Flera intervjupersoner menar även att det inte finns tillräckligt med hjälp för att lära sig hantera till exempel sin e-legitimation och internetbank. Personer som väljer bort digitala tjänster på grund av osäkerhet och rädsla får därmed svårt att delta i flera delar av samhället.

Sammanfattningsvis kan vi konstatera att de sårbarheter som identifieras i den här rapporten i stor utsträckning speglar aktuella rutinaktiviteter i människors vardag. Vad människor gör, hur det görs och vad det finns för alternativ, i kombination med mänskliga förmågor och egenskaper, styr hur bedrägerier kan genomföras och vilka som drabbas. I figur 5 sammanfattas också de identifierade sårbarheterna utifrån de olika stegen i bedrägeriers händelsekedja.

Figur 5 Sårbarheter utifrån bedrägeriers händelsekedja.



4. Brottsförebyggande åtgärder mot bedrägerier mot privatpersoner

I det här kapitlet beskrivs resultaten från projektets kartläggning av bedrägeriförebyggande åtgärder.[21] Kapitlet är strukturerat i tre delar där den första delen beskriver vilka incitament och drivkrafter aktörerna har för att arbeta bedrägeriförebyggande. Den andra delen beskriver brottsförebyggande åtgärder som inriktar sig på sårbarheter i de tekniska och strukturella omständigheterna. I den tredje delen beskrivs brottsförebyggande åtgärder mot sårbarheter hos potentiella brottsoffer, för att stärka individers motståndskraft mot bedrägerier.

Både åtgärder mot tekniska och strukturella sårbarheter, och åtgärder för att stärka motståndskraften hos potentiella brottsoffer, syftar till att påverka situationer som möjliggör brott, det vill säga situationell brottsprevention. Indelningen av åtgärderna kan också kopplas till brottstriangeln och till de förutsättningar som enligt rutinaktivitetsteorin måste finnas på plats för att ett brott ska kunna ske: en motiverad gärningsperson, ett lämpligt brottsoffer och frånvaro av kontroll. Åtgärder för att stärka potentiella brottsoffer tar sikte på det lämpliga brottsoffret, och åtgärder mot de strukturella omständigheterna på frånvaron av kontroll. Intervjupersonernas beskrivningar av den brottsförebyggande verksamheten innefattar däremot få åtgärder med fokus på den motiverade gärningspersonen och det är inte heller studiens fokus.[22]

Åtgärderna som presenteras och diskuteras gör inte anspråk på att vara heltäckande, utan bygger på den information som delats i intervjuer med ett antal nyckelaktörer. Vår bedömning är dock att vi har fått med de väsentligaste delarna av det pågående brottsförebyggande arbetet. Vi har bland annat intervjuat olika delar av Polismyndigheten och andra myndigheter med ett allmänt eller specifikt brottsförebyggande uppdrag. Intervjuer har också gjorts med företag vars produkter används som verktyg vid bedrägerier mot privatpersoner (t.ex. banker och digitala

[21] Se bilaga 3 för en förteckning över de åtgärder som ingår i Brås kartläggning.

[22] Se rapportens inledning för en beskrivning av situationell brottsprevention, rutinaktivitetsteorin och brottstriangeln.

marknadsplatser) och med andra typer av organisationer med brottsförebyggande vision.

Incitament hos de brottsförebyggande aktörerna

För att förstå vilka åtgärder som har genomförts för att förebygga bedrägerier är det relevant att se över vilka förutsättningar som finns för att arbeta bedrägeriförebyggande och vilket ansvar olika aktörer ser sig ha respektive bör ha. I takt med att bank- och betalmarknaden blivit mer digital har det skett en förskjutning av kontrollen av privatpersoners transaktioner, från bankpersonal till individen själv. Även andra delar av samhällets digitala utveckling ställer krav på individen som delar av befolkningen kan ha svårt att hantera. Flera av studiens intervjupersoner från såväl myndigheter, privat sektor och övriga aktörer är kritiska till i vilken mån samhället tar sitt ansvar. De menar att såväl privat som offentlig sektor har tjänat på digitaliseringen, men att de inte fullt ut tar ansvar och förebygger den brottslighet som utvecklingen har möjliggjort.

I intervjupersonernas beskrivningar och resonemang framträder tre övergripande teman för aktörernas incitament att arbeta bedrägeri-förebyggande: formellt uppdrag och ansvar; ekonomiska incitament; och informellt samhällsansvar. Hos de flesta av de intervjuade aktörerna finns drivkrafter inom mer än ett av dessa teman.

Formellt uppdrag och ansvar

Myndigheter styrs och drivs i första hand av sin instruktion och sitt årliga regleringsbrev. För vissa myndigheter är det brottsförebyggande uppdraget uttalat och arbetet relativt omfattande. I andra fall blir de brotts-förebyggande åtgärderna enbart en större eller mindre konsekvens i utförandet av det uppdrag de har, exempelvis konsumentskydd, en stabil finansmarknad, och tillgänglig och säker kommunikation.

För Polismyndigheten är det formella uppdraget tydligt, eftersom det brottsförebyggande arbetet är ett av polisens grunduppdrag (2 § polislagen [1984:387]). Polismyndigheten har också sedan 2022 en brotts-förebyggande strategi som innebär att det brottsförebyggande arbetet ska vara en integrerad del i all verksamhet och hos alla medarbetare (Polismyndigheten 2022a). Flera intervjupersoner menar dock att den bedrägeriförebyggande verksamheten inte prioriteras tillräckligt inom myndigheten. Till exempel är det bara någon enstaka av alla på varje regional bedrägerisektion som arbetar helt eller delvis brottsförebyggande.

Nationellt drivs det bedrägeriförebyggande arbetet av Nationellt bedrägericentrum (NBC) på polisens nationella avdelning (Noa) där det under våren 2023 arbetade fyra personer med brottsförebyggande arbete. Vissa lokalpolisområden arbetar brottsförebyggande mot bedrägerier, men lokala brottsförebyggare berättar att det är ett svårt och ofta ett ostrukturerat arbete. Det beror, enligt dem, på att bedrägerierna oftast sker digitalt medan de lokala lägesbilderna och således åtgärdsplanerna är fokuserade på fysiska platser. Brås intervjupersoner berättar att det finns processer för hur den brottsförebyggande verksamheten ska integreras på olika nivåer i verksamheten, men att processerna inte är tillräckligt kända och därför inte implementerade inom hela myndigheten.

Även övriga aktörer styrs i viss mån av formella regler. Flera intervjupersoner hänvisar till att de krav som penningtvättslagen[23] ställer på bland annat bankerna medför att stora resurser läggs på monitorering och rapportering av transaktioner som är misstänkt penningtvätt. Åtgärder mot bedrägeri prioriteras dock inte på samma sätt eftersom det inte finns motsvarande lagkrav. Annan relevant formell reglering är EU-förordningen om en inre marknad för digitala tjänster (EU 2022/2065) från oktober 2022. Förordningen håller på att implementeras i Sverige och innebär bland annat ett utökat ansvar för mycket stora onlineplattformar och mycket stora onlinesökmotorer[24] att ta bort illegalt innehåll samt att en eller flera myndigheter ska utses som ansvariga för att utöva tillsyn över dessa. Tidigare i rapporten nämns även EU:s betaltjänstdirektiv som ställt krav på stark kundautentisering vid kortbetalningar (EU 2015/2366).

Ekonomiska incitament

Ekonomi och lönsamhet som drivkraft för att arbeta brottsförebyggande är väldigt synligt i materialet när det kommer till de privata aktörerna. Det ses i hög grad som en självklarhet, men flera intervjupersoner formulerar kritik om att det är först när den ekonomiska skadan drabbar bankerna och inte enbart enskilda kunder som de verkligen prioriterar sitt bedrägeriförebyggande arbete.

[23] Lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism.

[24] Mycket stora onlineplattformar och mycket stora onlinesökmotorer inkluderar bland annat Facebook, Amazon, YouTube, Instagram och Google. Vissa delar av förordningen gäller även andra leverantörer av förmedlingstjänster, såsom internetleverantörer, domänregister, marknadsplatser online, appbutiker och sociala nätverk.

För företagen är det hela tiden en avvägning mellan kostnaden för säkerhet och kostnaden för bedrägerier. Kostnader för säkerhet består exempelvis av utvecklingskostnader för övervakningssystem, men också i risken att en ökad säkerhet innebär minskad användarvänlighet och därmed färre kunder och lägre omsättning och vinst. Kostnader för bedrägerier kan i sin tur vara både direkta och indirekta. Direkta kostnader kan exempelvis vara när banker eller andra företag behöver ersätta bedragna kunder. Indirekta kostnader av bedrägeri kan bland annat vara ett skadat varumärke och risken att kunder och annonsörer väljer bort företag som uppfattas som osäkra eller oseriösa. Ett par intervjupersoner utanför företagssektorn menar att risken att tappa kunder på grund av krångligare lösningar borde kunna vägas upp genom att marknadsföra företaget som extra säkert. Intervjupersoner från polisen berättar att de genom att hota med att gå till media eller prata med media lyckats påverka företag att använda säkrare lösningar.

Ett flertal intervjupersoner menar att ett avgörande från Högsta domstolen om bankernas skyldighet att ersätta bedrägeriutsatta kunder (NJA 2022 s. 522) samt ett flertal vägledande beslut från Allmänna reklamationsnämnden (ARN)[25] har fått stor betydelse för bankernas driv i de brottsförebyggande frågorna. Avgörandena innebär dock enbart ersättningsansvar till kunder utsatta för bedrägeri genom obehöriga banktransaktioner. Några intervjupersoner hoppas därför på framtida avgöranden som innebär motsvarande praxis för bedrägliga behöriga transaktioner (se även i avsnittet *Telefonbedrägerier* i kapitel 2 om en upplevd förskjutning från obehöriga till behöriga bedrägliga transaktioner).

Informellt samhällsansvar

Flera aktörer inom samtliga sektorer motiverar även sitt bedrägeriförebyggande arbete utifrån den samhällskada och individskada som brottsligheten innebär. Intervjupersoner hänvisar till att äldre luras till att ofrivilligt sponsra den organiserade brottsligheten, att otrygghet på internet är ett demokratiproblem, att tilltron till bankväsendet riskeras och så vidare. Flera berättar också att de i enskilda möten med brottsoffer ser stora lidanden på grund av såväl ekonomisk som känslomässig skada.

[25] Bl.a. referat 2022–1266 och 2022–03828.

Åtgärder mot tekniska och strukturella sårbarheter

I beskrivningen av brottsproblemet framgår att bedragare utnyttjar olika typer av tekniska och strukturella sårbarheter för att genomföra bedrägerierna. Bland annat använder bedragarna målvakter som företrädare för företag och konton, manipulerar vem som visas som avsändare i kontakt med brottsoffer och hittar säkerhetsluckor som möjliggör bedrägliga transaktioner. I det här avsnittet presenteras de åtgärder som genomförs i syfte att minska dessa sårbarheter.

Åtgärder mot förberedelser

Det finns flera exempel på strukturella och tekniska åtgärder mot bedragarnas möjligheter att förbereda ett bedrägeri. När det gäller tillgång till målvakter beskriver Ekobrottsmyndigheten (EBM) att de arbetar aktivt för att det ska bli **svårare att använda målvakter.** Arbetet bedrivs framför allt genom påverkansarbete gentemot andra aktörer, till exempel samverkar EBM med Bolagsverket för att få dem att bli hårdare i sina kontroller och öka deras förmåga att säkerställa riktigheten i sina register. [26] På EBM pågår även ett arbete för att se över möjligheterna att dela information med myndigheter (såsom Bolagsverket och Skatteverket) och banker i syfte att förebygga återkommande missbruk av identiteter. I juni 2023 lämnades ett betänkande (SOU 2023:34) som bland annat syftar till att försvåra användningen av målvakter, liksom av stulna, kapade eller fiktiva identiteter som företrädare för företag. Bland annat föreslås att Bolagsverket bör göra fler kontroller i registreringsärenden samt samverka med andra myndigheter (såsom EBM och Skatteverket) för att säkerställa riktigheten i sina register och för att kunna identifiera målvakter. Myndigheten föreslås också kunna förelägga om personlig inställelse när det behövs för att kunna säkerställa företagsföreträdares identitet.

Internetsstiftelsen ansvarar för registrering av domäner under toppdomänerna .se samt sköter drift och administration av toppdomänen .nu. Inom ramen för sin verksamhet bedriver de ett **förebyggande arbete mot bedräglig användning av domäner.** Enligt en intervjuperson arbetade Internetstiftelsen tidigare löpande med övervakning av domänregistreringar. Internetstiftelsen menar att de nu arbetar mer proaktivt genom att påverka återförsäljare av domäner att så långt det är möjligt kräva identifiering med e-legitimation vid registrering. De menar

[26] Brå har inte intervjuat företrädare för Bolagsverket eller Skatteverket om deras del av arbetet.

att korrekta uppgifter om vem som har domänen minskar risken att den används i ett bedrägeri. Emellanåt tar Internetstiftelsen även in särskilda resurser för att gå igenom och kontrollera registret och de har särskilda verktyg för att upptäcka, kontrollera och eventuellt stänga ner misstänkta domäner. De arbetar också med att påverka myndigheter att göra så kallade skyddsregistreringar vilket innebär att man registrerar snarlika domännamn för att undvika missbruk.

Det förekommer även internationella och europeiska **polisinsatser för att stänga ner forum på ”darkweb”** där det bland annat säljs stulna kort- och användaruppgifter, andra kriminella tjänster att använda vid bedrägerier och hela bedrägeriupplägg. Den svenska polisen deltar i varierande grad i dessa insatser.

Flera av de digitala marknadsplatserna har infört identitetsverifiering med syftet att motverka falska konton. I beskrivningar av sitt säkerhetsarbete berättar Blocket hur de över tid utvecklat **starkare verifiering av användarkonton** (identitetskontroller). Identifieringen görs antingen genom bank-id eller sms och det verifierade kontot krävs för att lägga upp en annons eller svara på en annons via Blockets egen meddelandetjänst. Blocket beskriver även att de **granskar alla annonser** och stoppar dem som bedöms vara bedrägliga eller som anmäls som tveksamma av andra användare. På Traderas webbplats beskrivs liknande åtgärder (Tradera 2023). Även Facebook beskriver kontroller för att motverka falska användarkonton och kontokapningar, exempelvis att de i vissa fall kräver tvåfaktorsautentisering eller identifikation genom fotografi.

Vad gäller gärningspersonernas kartläggningar av potentiella brottsoffer genom uppgifter från öppna källor framkommer enbart indirekta åtgärder; seniororganisationer beskriver att de i sitt **påverkansarbete** driver att det ska bli svårare för obehöriga att komma åt vissa uppgifter, som ålder och familjesituation.

I övrigt är de förebyggande åtgärder mot förberedelser som beskrivs i intervjuerna relativt begränsade. Endast en intervjuperson inom företagssektorn tar upp åtgärder mot dataintrång som en del av det förebyggande arbetet mot bedrägeri. Från bland annat Brås tidigare studie av dataintrång vet vi dock att såväl offentliga som privata aktörer löpande arbetar för att förbättra den tekniska säkerheten i syfte att **förebygga dataintrång** (Brå 2022b). Av kapitel 2 och 3 har det också framkommit att social manipulation via sms, e-post eller sociala medier ofta är inledande

steg i just dataintrång. Därmed blir förebyggande åtgärder mot den typen av social manipulation även förebyggande åtgärder mot just dataintrång.

Åtgärder mot manipulering av avsändare

Tidigare i rapporten framkommer att möjligheten att manipulera vem som visas som avsändare i samtal och sms är en tydlig sårbarhet. Nationellt bedrägericentrum (NBC) berättar att de som en del av sitt förebyggande arbete försöker påverka bland annat telefonoperatörer att utveckla lösningar mot bedräglig användning av manipulerade telefonnummer. De åtgärder som tidigare genomförts är dels ett system med en manuell spärrlista med utvalda nummer som skyddas mot manipulerade telefonnummer, dels separata överenskommelser mellan banker och sms-tjänster för att bankernas namn inte ska kunna missbrukas. Därutöver pågår det ett arbete i samverkan mellan Telekområdgivarna, ett flertal telefonoperatörer och Post- och telestyrelsen (PTS). Arbetet består i att ta fram tekniska lösningar, vägledningar och föreskrifter och fokuserar i första hand på manipulerade fasta svenska telefonnummer där samtalen kommer från utländska servrar. Intervjupersoner berättar att aktörerna arbetar vidare med att hitta åtgärder mot manipulerade mobiltelefonnummer och sms.

Andra åtgärder mot sårbarheter relaterade till kontakten mellan bedragare och potentiella brottsoffer är verifierade meddelandetjänster som Blocket och Tradera tillhandahåller (se även avsnittet *Åtgärder mot förberedelser*) och varningar som användare får när de flyttar kontakten utanför plattformen. Även Konsumentverket arbetar mot bedrägliga kontakter via annonser genom att driva ärenden mot annonser och mot webbutiker som inte följer gällande regler.

Ytterligare en typ av åtgärd är såväl polisens som Internetstiftelsens påverkansarbete gentemot centrala aktörer att inte bifoga länkar i e-post- eller sms-utskick till medborgare eller användare. Tanken är att om myndigheter och andra centrala aktörer slutar använda länkar i sina meddelanden blir det svårare för bedragarna att lura människor att klicka på länkar. Polisen nationellt berättar även att de genom internationell samverkan bedriver påverkansarbete mot stora onlineplattformar som bland annat Meta (som äger bl.a. Facebook och Instagram) och Google för att få dem att ta ett större ansvar mot exempelvis oseriösa annonser. Arbetet består i att man samlar tillvägagångssätt och statistik om hur

onlineplattformarna fungerar som möjliggörare för bedrägerier och presenterar det för plattformsägarna.

Åtgärder mot bedrägliga transaktioner

Banktransaktioner

I kapitel 2 och 3 framkommer att såväl obehöriga som behöriga[27] bedrägliga transaktioner kan genomföras från brottsoffers bankkonton utan att stoppas av bankernas övervakningssystem.

Flera intervjupersoner inom banksektorn beskriver att det har gjorts en hel del åtgärder för att förebygga obehöriga transaktioner. En sådan åtgärd är Bank-id:s lösningspaket *Säker start* som genom autostart eller en dynamisk qr-kod knyter enheten (datorn, telefonen eller surfplattan) som får åtkomst till internetbanken, till samma fysiska plats som enheten med bank-id:t. På så sätt motverkas att ett potentiellt brottsoffer ger en bedragare åtkomst till sitt bankkonto.[28] Lösningen skyddar dock inte vid inloggning via bankdosa eller andra alternativa lösningar.

Andra åtgärder för att skydda mot missbruk av digital identifikation i samband med banktransaktioner och där implementeringen pågår, är olika former av regler och villkor som sätts upp för att bedöma risken för missbruk vid användning eller utfärdande av ett bank-id. Sådana risksituationer kommer kräva en särskild kontroll genom exempelvis scanning av chip och foto i ett fysiskt pass alternativt nationellt identitetskort, i form av ett telefonsamtal till banken eller genom att fysiskt infinna sig på ett bankkontor.[29]

Ytterligare en åtgärd som kan skapa förutsättningar för säkrare identifikationer vid användning av digitala banktjänster är ett förslag på en statlig e-legitimation som Myndigheten för digital förvaltning (DIGG) utformat på uppdrag av regeringen. Enligt förslaget ska e-legitimationen

---

[27] Se kapitel 2 och bilaga 2 för förklaring av behöriga respektive obehöriga bedrägliga transaktioner.

[28] Bank-id har ställt krav på att alla som använder Bank-id:s tjänster (företag, myndigheter och organisationer) ska implementera Säker start senast 1 maj 2024, men enligt uppgift från Bank-id har bankerna redan fullföljt sin implementering.

[29] Risksituationer är exempelvis när ett nytt mobilt bank-id utfärdas till en ny enhet som inte har platstjänster påslaget, när ett nytt bank-id utfärdas genom identifiering via bankdosa eller när bankens webbtjänst eller webbtjänst för utgivning har använts (eftersom det finns risk att skärmdelning används i dessa fall). Det kan också vara när en transaktion till en ny mottagare görs väldigt nära i tid från skapandet av ett nytt bank-id, genom inloggning med ett bank-id på en mobil enhet med avslagna platstjänster, eller från ett bank-id eller en dator som befinner sig på en oväntad plats. Enligt uppgifter från Bank-id ska de flesta av dessa kontroller ha implementerats under första halvåret 2023.

tillgängliggöras för alla svenska medborgare och personer med samordningsnummer och inte kräva att användaren har en egen smarttelefon eller dator. Förslaget är att e-legitimationen ska utfärdas av en statlig aktör som säkerställer grundidentifieringen. E-legitimationen ska sedan kunna användas för utfärdande av andra e-legitimationer eller identifieringslösningar med lägre tillitsnivå, så kallad id-växling (DIGG 2023). I december 2022 tillsattes även en utredning som bland annat ska lämna förslag på vilken eller vilka myndigheter som ska ansvara för grundidentifieringen vid utfärdandet av e-legitimation och hur kontrollen ska gå till (Regering Dir. 2022:142). Några intervjupersoner uttrycker en förhoppning om att en statlig e-legitimation kan leda till en uppdelad trafik där den statliga e-legitimationen används vid identifiering vid olika samhällstjänster och att ett bank-id används vid ekonomiska transaktioner.[30] Det skulle i sin tur kunna minska risken för att bedragare blir insläppta i privatpersoners internetbanker till följd av andra typer av signeringar.

Bedrägliga behöriga transaktioner är enligt flera intervjupersoner inom banksektorn betydligt svårare att förebygga och stoppa. I och med att det är brottsoffret som godkänner transaktionen från sin egen enhet finns inte samma möjligheter att sätta upp regler avseende misstänkt inloggning och identifikation. Intervjupersonerna menar dock att det sker övervakning på bankerna av transaktioner som genomförs från och till kundernas bankkonton med syftet att stoppa bedrägerier genom såväl behöriga som obehöriga transaktioner.

En bild som framträder är att bankerna i första hand gör sin övervakning dels på gruppnivå där individer grupperas och riskbedöms utifrån egenskaper som exempelvis ålder, dels genom att skräddarsy produkter för olika kundgrupper beroende på bedömd risk. Vilka typer av transaktioner som en kund kan göra, exempelvis avseende belopp eller utlandstransaktioner, begränsas av grupptillhörighet eller vilken produkt det är man har. För att en transaktion som bryter mot begränsningarna ska kunna genomföras krävs någon ytterligare åtgärd, såsom en personlig kontakt med banken. En del av den här typen av övervakning är också de generella begränsningar som finns på vissa produkter oavsett kund, bland

[30] Det finns redan alternativa e-legitimationer som kan användas för olika typer av tjänster (dock inte inloggning i internetbanken). Mest använd är Freja id som flera offentliga och privata aktörer godkänner som giltig e-legitimation. Också Skatteverkets id-kort innehåller en e-legitimation. Den går för närvarande enbart att använda på Skatteverkets webbplats (skatteverket.se).

annat beloppsgränser på Swish samt extrakontroller och fördröjningar vid utlandsbetalningar.

Vissa intervjuade banktjänstemän menar att det även finns en övervakning som bygger på individuellt anpassade regler. Reglerna kan sättas utifrån tidigare beteendemönster för att fånga upp olika typer av avvikande transaktioner. När en transaktion bryter mot en regel flaggas den och blir eventuellt stoppad direkt alternativt utsatt för någon form av extra kontroll.

Bankerna beskriver att deras utmaning ligger i att hitta tillräckligt träffsäkra kontroller som stoppar bedrägliga transaktioner men släpper igenom övriga. En intervjuperson berättar att på hens bank stoppar man ungefär tusen misstänkta transaktioner varje dag men att huvudparten stoppas felaktigt. Samtidigt lyckas bedragarna fullborda ett stort antal brott varje år.

Att påverka bankerna till att fokusera mer på säkerhet och att utveckla lösningar för att mer träffsäkert stoppa bedrägliga transaktioner nämns även av polisen som en del av deras förebyggande arbete. Bland annat har polisen initierat och driver sedan september 2022 en samverkan med storbankerna och Bankföreningen med syfte att förebygga bedrägerier.[31] Även Konsumentverket och Konsumentombudsmannen (KO) bedriver arbete där syftet är att påverka bankerna. KO har även drivit ett ärende som lett fram till ny praxis avseende bankernas ersättningsskyldighet gentemot kunderna vid obehöriga transaktioner (se avsnittet *Ekonomiska incitament* om vägledande beslut i ARN). I januari 2023 beslutade KO att även driva ett ärende avseende bedrägliga behöriga transaktioner (Konsumentverket 2023). Enligt intervjupersoner är målet bland annat att skapa starkare incitament hos bankerna att arbeta förebyggande mot bedrägerier. Även seniororganisationer berättar att de arbetar aktivt för att påverka bankerna på det här området.

Korttransaktioner och fakturabetalningar

Både intervjuade poliser och företrädare för såväl andra myndigheter som civilsamhället är överens om att betaltjänstdirektivet EU 2015/2366 som nämnts tidigare i rapporten har varit en avgörande brottsförebyggande åtgärd mot bedrägliga korttransaktioner. I flera sammanhang lyfts betaltjänstdirektivet också fram som ett gott exempel på hur man genom

[31] Samverkan om bedrägerier är numera inkluderat i SAMLIT – Swedish Anti-Money Laundering Intelligence Task Force – där polisen och bankerna kan dela information med varandra.

reglering eller annan typ av strukturella åtgärder kan få en tydlig brottsförebyggande effekt. Sedan januari 2023 gäller motsvarande krav på betalningar via faktura och betaltjänster (Prop. 2022/23:9).

Som framgått av kapitel 2 och 3 omfattar dock kraven på stark kundautentisering inte alla former av kortköp. Dessutom kan ett EU-direktiv enbart ställa krav på kort som är utfärdade och e-handlare som är registrerade inom EU. Med syftet att förebygga bedrägliga transaktioner som inte omfattas av direktivet sker i likhet med övervakningen av banktransaktioner även en övervakning av korttransaktioner. Den här övervakningen görs dock inte av bankerna utan av kortföretagen.[32]

Intervjupersoner inom polisen beskriver också att de som en del av sitt förebyggande arbete mot kortbedrägerier bedriver påverkansarbete mot stora e-handelsaktörer för att få dem att utveckla sina kontroller vid kortköp och på så sätt motverka bedrägliga transaktioner.

Transaktioner i samband med annonsbedrägerier

Både Blocket och Tradera erbjuder integrerade betallösningar, dock inte Facebook marketplace. Blocket förklarar att lösningarna går ut på att köpare och säljare kan komma överens om att pengarna ska föras över till plattformen som säkrar dem fram till dess att köparen fått och kunnat kontrollera produkten som den köpt. På Traderas webbplats beskrivs att även Swish-betalningar kan göras inom den integrerade lösningen (Tradera 2023). I intervjun med Blocket framgår att syftet med de integrerade betallösningarna är att förebygga bedrägerier. Ett viktigt arbete för Blocket är dock att få sina användare att använda tjänsterna och förstå hur de fungerar så att de inte ska kunna missbrukas av bedragare.

Åtgärder för att försvåra hanteringen av brottsvinster

Att inrikta arbetet mot gärningspersonernas hantering av brottsvinster med syftet att försvåra för bedrägerier är något som beskrivs av flera intervjupersoner. Polismyndigheten menar också att en stor del av de misstänkta transaktioner som rapporteras i arbete mot penningtvätt består av misstänkta brottsvinster från bedrägerier (Polismyndigheten 2023b). Det medför att det omfattande arbetet mot penningtvätt som bedrivs av

[32] I en artikel på Visas webbplats (Visa 2023) beskrivs exempelvis hur de använder artificiell intelligens för att göra individanpassad övervakning av kortköp.

bland att Polismyndigheten och bankerna också inkluderar åtgärder som indirekt riktar sig mot bedrägerier.[33]

Inom ramen för det bedrägeriförebyggande arbetet bedrivs det dock inom Polismyndigheten främst sporadiska informationsinsatser riktade mot potentiella möjliggörare för penningtvätt, bland annat bil-, klock- och smyckeshandlare, samt mot unga personer i syfte att motverka rekrytering av penningmålvakter.

Åtgärder för att stärka individers motståndskraft

I kapitel 2 och 3 beskrivs hur bedragare utnyttjar olika typer av sårbarheter hos potentiella brottsoffer, såsom okunskap och oförmåga att ta till sig digital information, stress, nyfikenhet, ensamhet och girighet. Åtgärderna som genomförs för att möta dessa sårbarheter har lite olika karaktär, både vad det gäller form och innehåll. Merparten är dock inriktade på att öka individers kunskap för att därigenom stärka deras motståndskraft mot bedrägerier.

Medvetandehöjande åtgärder med olika fokus

Fokus i informationen varierar beroende på aktörens uppdrag och målgrupper. En del av de aktiviteter som genomförs tar sikte på att öka individers digitala kunskap och förståelse, bland annat för hur internet, digital identifiering och domäner fungerar. I dessa fall beskriver intervjupersoner att det handlar om att bygga människors förmåga och självförtroende att själva bedöma vad som är trovärdigt, att använda digitala tjänster på ett säkert sätt och ”bli sunt kritiska”. Exempelvis finns informationskampanjen *Tänk säkert*,[34] som drivs av Myndigheten för samhällsskydd och beredskap (MSB) i samverkan med Polismyndigheten och i samarbete med en rad olika myndigheter, företag och civilsamhällesorganisationer. Den har som övergripande syfte att stärka människors kunskap om informations- och cybersäkerhetsfrågor. Flera av de aktiviteter som genomförts inom ramen för kampanjen, och även kurser,

[33] Åtgärderna inkluderar bland annat bankernas arbete med att bevaka transaktioner för att identifiera misstänkt penningtvätt, stoppa transaktioner och spärra konton och bank-id:n; verksamhetsutövares rapportering om misstänkt penningtvätt till Finanspolisen (Fipo); Fipo:s arbete med att sammanställa och sprida den kunskapen; utredning och lagföring av penningmålvakter, samt Samordningsfunktionen mot penningtvätt och finansiering av terrorism (Polismyndigheten 2023b). Arbetet mot penningtvätt regleras framförallt i lag (2017:630) om åtgärder mot penningtvätt och finansiering av terrorism samt lag (2014:307) om straff för penningtvättbrott.

[34] Kampanjen har drivits av MSB som en del av EU:s informationssäkerhetsmånad sedan 2018. Under 2022 fick MSB och Polismyndigheten i uppdrag av regeringen att utöka kampanjen, både i tid och omfattning.

artiklar, guider och skrifter som tagits fram och förmedlats av bland annat MSB, Internetstiftelsen och Stöldskyddsföreningen (SSF), handlar om digital säkerhet på ett mer generellt plan. Den här typen av information inkluderar även när myndigheter, organisationer och företag beskriver hur deras och andras produkter och tjänster kan användas på ett säkert sätt, till exempel hur man kan handla säkert eller hur ett bank-id ska användas.

En annan del av det förebyggande informationsarbetet riktar sig specifikt mot bedrägerier, på att öka individers kunskap om bedrägliga tillvägagångssätt och på vad den enskilda individen kan göra för att inte utsättas för ett bedrägeri. Eftersom Polismyndigheten har ett tydligt brottsförebyggande uppdrag har deras brottsförebyggande informationsinsatser bedrägeribrottet som utgångspunkt, i syfte att ”stärka allmänheten mot bedrägerier” som en polis uttryckte det. Ett annat exempel är Sveriges bankers kampanj *Svårlurad!*[35] som syftar till att göra människor svårlurade genom att beskriva vanliga tillvägagångssätt vid bedrägerier och ge konkreta brottsförebyggande tips och råd.

Beroende på aktörernas fokus och ansvarsområden så varierar informationen i de olika informationssatsningarna. Till exempel beskrivs tillvägagångssätt och förebyggande åtgärder mot investeringsbedrägerier av Finansinspektionen, medan Finansiell id-teknik (som tillhandahåller Bank-id) fokuserar på bedrägerier där bank-id används, och konsumentorganisationer koncentrerar sig på konsumentrelaterade bedrägerier. Fokus i informationen som förmedlas ligger ofta på vad man kan göra för att skydda sig i olika situationer. Det kan till exempel handla om att inte lämna ut kort- eller kontouppgifter eller logga in på Bank-id på uppmaning från någon som ringt upp, att vara försiktig med vilka länkar man klickar på, att våga lägga på luren och att inte lita på den som ringer. Intervjupersoner understryker att de försökt göra tipsen få, koncisa och konkreta samtidigt som de ska kunna appliceras på flera olika typer av situationer. Informationen sprids på en rad olika webbplatser, i sociala medier, nyhetsbrev, medlemstidningar, seminarier, webbinarier och möten.

Det finns också olika typer av varningar och varningslistor som både kan inkludera varningar för specifika tillvägagångssätt vid bedrägerierna, och varningar för exempelvis osäkert användande av en produkt eller för ett

[35] Kampanjen drevs av storbankerna och Bankföreningen våren 2023.

specifikt företag som begår bedräglig verksamhet.[36] Det kan till exempel handla om att olika aktörer i samband med Black Friday varnar för falska leveransmeddelanden, om varningar angående en aktuell pitch i telefonbedrägerierna, eller varningar om att en specifik webbplats är osäker. Varningarna sprids i media, sociala medier, via e-post och i aktörernas egna kanaler, produkter och nätverk.

Flera intervjupersoner tar därtill upp att de i enskilda fysiska eller digitala samtal med brottsoffer eller potentiella brottsoffer ger information, vägledning och råd med koppling till bedrägerier.[37]

Åtgärder inriktade mot äldre

En stor del av arbetet med att stärka människors motståndskraft är riktat mot äldre. Insatserna handlar ofta om telefonbedrägerier och andra typer av social manipulation. Prioriteringen motiveras i intervjuerna med att det är en typ av bedrägeri som ökar både i omfattning, brottsvinster och skada för brottsoffren likväl som för samhället. En intervjuperson menar att det också främst är äldre som efterfrågar förebyggande information om bedrägerier.

Huvudparten av informationsinsatserna syftar till att ge äldre mer kunskap om bedrägliga tillvägagångssätt liksom om hur digitala tjänster såsom bank-id fungerar, för att öka deras möjligheter att skydda sig själva. Åtgärderna är dock inte enbart inriktade på okunskap och ovana, utan handlar även om att göra de äldre bättre rustade att hantera stressiga situationer, att våga lägga på luren om de känner sig obekväma, och bli mer misstänksamma vid samtal även om den som ringer verkar förtroendeingivande. Syftet är därmed att komma åt sårbarheter som stress, viljan att vara trevlig och tillmötesgående och benägenheten att lyssna på auktoriteter. Flera av insatserna inriktas inte heller enbart på att förebygga brott, utan även på att minska den potentiella skadan som bedrägerier direkt eller indirekt kan ha på äldre. Flera intervjupersoner nämner i det sammanhanget ordet ”våga” – att de vill att äldre ska våga använda digitala tjänster och våga berätta när de har utsatts för ett

[36] Exempel på varningslistor är Stöldskyddsföreningens digitala varningsgrupp samt Finansinspektionen och Svenska Handels varningslistor.

[37] Till exempel konsumentrådgivning, Digidelcenter som ger digital handledning, och samtal till brottsofferjourer.

bedrägeri; de vill alltså minska oron för att utsättas liksom minska skammen för dem som har utsatts.

I intervjuer med regionala brottsförebyggare och kommunpoliser framgår det att polisen på regional och lokal nivå ofta fokuserar sina bedrägeriförebyggande insatser på telefonbedrägerier mot äldre. Det gör de bland annat genom att hålla lokalt framtagna föreläsningar för lokala seniororganisationer eller genom att utbilda polisvolontärer att föreläsa, och genom att dela ut informationsblad till hemtjänsten, via grannsamverkan, på bibliotek och på andra mötesplatser där äldre vistas. De går också ut med brottsförebyggande information och varningar i lokal media och i lokala sociala mediegrupper. Det finns även exempel på lokala informationsinsatser som riktats specifikt mot äldre kvinnor.

På nationell nivå skickade polisen ut ett vykort till alla över 70 år våren 2023 med tre konkreta tips kopplade till telefonbedrägerier. En intervjuperson inom polisen berättar att ”tanken är att man ska spara vykortet, sätta det på kylskåpet och att man också ska fundera på vad man ska säga när någon ringer”. Polismyndigheten har också i samarbete med seniororganisationer och Brottsofferjouren tagit fram utbildningsmaterialet *Försök inte lura mig*,[38] med handledning, filmer, praktiska övningar och underlag till diskussion och reflektion om hur äldre kan skydda sig mot bedrägerier på stan, i hemmet och på nätet. I samverkan med Utbildningsradion (UR) producerades på samma tema tre filmer hösten 2020. Tanken är att utbildningen ska användas av till exempel lokala seniororganisationer eller brottsofferjourer för att ge äldre ökad medvetenhet och bättre kunskap om hur de kan skydda sig mot bedrägerier. Intervjuade representanter på seniororganisationer berättar att de utöver utbildningarna även sprider information om bedrägerier via bland annat möten, medlemstidningar, nyhetsbrev och sociala medier.

Också bankernas kampanj *Svårlurad!* har telefonbedrägerier mot äldre som huvudfokus. Därtill har flera aktörer, såsom Internetstiftelsen och SSF, utbildnings- och informationsmaterial, guider och artiklar riktat specifikt mot äldre. Till exempel har SSF tagit fram en klisterlapp med råd till äldre som kan klistras fast på exempelvis mobiltelefonen. Enligt Internetstiftelsen fokuserar de på digital identifikation, eftersom det ofta

[38] Utbildningspaket framtaget 2015 av Polismyndigheten i samarbete med PRO, SPF Seniorerna, SKPF Pensionärerna och Brottsofferjouren med målgruppen äldre personer. Utbildningen uppdaterades år 2019.

används vid telefonbedrägerier mot äldre. Båda organisationerna samverkar även med andra aktörer för att sprida materialet fysiskt.

Utöver åtgärder riktade direkt mot äldre inkluderar flera aktörer informationsinsatser mot anhöriga till äldre, så att de anhöriga ska kunna förmedla sin kunskap till sina föräldrar, mor- och farföräldrar. Bland annat har Polismyndigheten ett samtalsstöd till anhöriga, *Prata med nära och kära om bedrägerier*, med samtalsguide, filmer, tips och diskussionspunkter. De har också tagit fram ett informationspaket till personer som pratar med äldre med inriktning på telefonbedrägerier, och haft en annonskampanj till anhöriga på sociala medier i samband med att vykortet till äldre skickades ut. Det finns också exempel på lokala informationsinsatser i skolor för att få skolungdomarna att förmedla sin kunskap om bedrägerier till sina äldre anhöriga. En del av kampanjen *Svårlurad!* riktar sig specifikt till äldres anhöriga med uppmaningen att prata om bedrägerier med sina anhöriga och att hjälpa dem att använda digitala tjänster på ett säkert sätt.

Åtgärder inriktade mot andra grupper än äldre

Trots att unga och barn inte är en särskilt utsatt grupp när det gäller bedrägerier, finns det en del informations- och utbildningsinsatser som är specifikt inriktade mot dessa grupper. Exempelvis ger MSB bidrag till Unga forskare för att föreläsa om cybersäkerhet, och både SSF och Internetstiftelsen har tagit fram specifikt material till skolungdomar, lärare och föräldrar. Ett annat exempel är organisationen HackShield som i samarbete med Stiftelsen Tryggare Sverige har utvecklat ett spel och lektionsmaterial om cybersäkerhet för barn och skolor (Stiftelsen Tryggare Sverige 2023). Insatserna handlar i huvudsak mer generellt om digital säkerhet och kompetens, där bedrägeri i vissa fall är en del. De är framförallt inriktade på sårbarheter kopplade till okunskap och ovana vid att hantera digitala tjänster, men även på att öka barns och ungas motivation till att använda sig av olika typer av säkerhetslösningar. Flera intervjupersoner berättar att det i stor utsträckning handlar om källkritik, säkra lösenord med mera, där det övergripande syftet är att ”bygga barnens kompetens inför framtiden”.

Utöver de riktade satsningarna på äldre och yngre, har en stor del av informationsarbetet antingen allmänheten generellt eller ”vuxna” som målgrupp. Kampanjen *Tänk säkert* riktas exempelvis i huvudsak till personer som är digitalt aktiva och är ”ute på internet”. En intervjuperson

inom kampanjen understryker att de ville nå personer som ”försöker göra saker snabbt, som vill spara tid” för att dessa löper större risk att utsättas till följd av sitt beteende. En slutsats av det är att det finns en ambition att minska sårbarheter kopplade till girighet, risktagande och bristande motivation för att använda säkerhetslösningar genom att öka människors digitala kunskap. Under 2022 gav regeringen medskicket att kampanjen skulle fokusera på bedrägerier, vilket medförde att MSB och polisen valde att rikta den mot nätfiske, utifrån att de bedömde att där var risken att utsättas störst. De myndigheter, företag och organisationer som deltog anpassade dock informationen till sina målgrupper och kanaler. Flera intervjupersoner inom polisen tar också upp att de i annonskampanjer på Facebook måste avgränsa till ett visst åldersspann och att de då valt bort yngre och äldre till förmån för de mitt emellan. Några intervjuade poliser på regional nivå berättar att de i sociala medier ofta fokuserar på annonsbedrägerier, eftersom de som drabbas av sådana bedrägerier också är aktiva på sociala medier.

Det är relativt ovanligt att insatser riktar sig till specifika språkgrupper, men både inom ramen för *Tänk säkert* och *Svårlurad!* lades information ut på flera språk. En intervjuperson berättar därtill att de håller föreläsningar för samhällskommunikatörer som i sin tur förmedlar informationen till nyanlända.

5. Avslutande analys och Brås bedömning

Ett brott med stor skada

I den här rapporten har vi beskrivit hur bedrägerier mot privatpersoner går till, vilka sårbarheter som möjliggör brotten och vilka förbyggande åtgärder som görs. Telefonbedrägerier är den typ av bedrägeri som framträder som särskilt skadlig; det har skett en ökning över tid, brottsvinsterna är stora och de som drabbas består i hög grad av särskilt sårbara grupper, i första hand äldre. Även andra former av bedrägerier får allvarliga konsekvenser för såväl individen som samhället. Drabbade individer skadas dels ekonomiskt, dels psykologiskt genom bland annat känslor av skam och otrygghet. Samhällsskadan består dels i risken för minskad tilltro till samhällets institutioner och system med bland annat ökat utanförskap som följd, dels i stora brottsvinster till kriminella.

Mer behöver göras för att åtgärderna ska få full effekt

I samtliga typer av bedrägerier finns det sårbarheter både relaterade till potentiella brottsoffer, som exempelvis stress och okunskap, och till tekniska och strukturella omständigheter, som exempelvis digitala transaktionslösningar och möjligheter att manipulera telefonnummer.

En samlad bedömning är att med några få undantag träffas de flesta sårbarheterna av någon form av förebyggande åtgärd.[39] Det finns åtgärder som ska försvåra för förberedelser av bedrägerier, exempelvis kontroller av domäner och användarkonton. Andra åtgärder syftar till att försvåra vilseledanden i själva kontakten, exempelvis kontroller av annonser och initiativ mot manipulerade telefonnummer. Det finns också åtgärder i form av övervakning och kontroller för att försvåra bedrägliga transaktioner från bankkonton och kort. I viss mån bedrivs även verksamhet för att försvåra hanteringen av brottsvinster med uttalat syfte att just förebygga bedrägerier mot privatpersoner.

Även de åtgärder som riktas mot potentiella brottsoffer träffar de flesta sårbarheter som vi har identifierat. Kampanjer, utbildningar och annat

[39] Se tabell 4 och tabell 5 i bilaga 3 för en kortfattad beskrivning av de bedrägeriförebyggande åtgärderna utifrån identifierade sårbarheter, inklusive en bedömning av i vilken mån de förebyggande åtgärderna täcker de identifierade sårbarheterna.

material innehåller information om hur internet och digital identifiering fungerar, generellt om informationssäkerhet samt information om hur bedrägerier kan gå till, både i allmänhet och genom specifika varningar. Genom ökad medvetenhet förväntar sig avsändarna en minskad sårbarhet gentemot såväl stress som risktagande, osund tillit och bristande motivation till kontroll. Många av dessa åtgärder tar sikte på särskilda målgrupper och har ett anpassat budskap, och många gånger prioriteras telefonbedrägerier mot äldre särskilt.

Trots en bred uppsättning förebyggande åtgärder sker det en omfattande bedrägeribrottslighet mot privatpersoner, med allvarliga konsekvenser för individ och samhälle. Det är uppenbart att den brottsförebyggande verksamhet som bedrivs i dag inte är i närheten av tillräcklig för att komma till rätta med brottsproblemet bedrägerier mot privatpersoner. I det här avslutande kapitlet kommer vi med utgångspunkt i en analys av nuläget ge förslag på åtgärder för att utveckla det bedrägeriförebyggande arbetet.

Åtgärder under planering behöver tas vidare

Vissa åtgärder har stor förebyggande potential, men består hittills enbart av påverkansarbete eller är under planering. Det är viktigt att dessa planer nu övergår i konkreta lösningar. Det finns bland annat långt gångna planer på att införa en statlig e-legitimation. Det är Brås bedömning att det skulle ha en brottsförebyggande effekt i och med en säkrare grundidentifiering och möjlighet för fler att använda e-legitimation. Även de åtgärder som är på gång för att försvåra bedräglig användning av manipulerade telefonnummer är viktiga för att minska risken för att potentiella brottsoffer vilseleds i telefonbedrägerierna. Samtidigt kommer åtgärderna inte att stoppa alla typer av manipulering av avsändare och det krävs ytterligare initiativ och utveckling inom området. Det aktualiseras särskilt vid en eventuellt ökad användning av avancerade tekniker för manipulering av avsändare, så kallad ”deep fake”, som bland annat möjliggörs genom artificiell intelligens (AI).

Några lösningar kopplade till säkrare identifiering vid användning av digitala banktjänster har helt nyligen implementerats fullt ut vilket är positivt. Samtidigt finns det vissa begränsningar av i vilken omfattning de kan användas. Det gäller exempelvis personer som inte har svenskt pass eller nationellt id-kort eller de som av andra skäl loggar in i internetbanken med annan lösning än bank-id. Det finns även lösningar som Bank-id utvecklat, men där implementeringen ännu inte har påbörjats.

Åtgärder bör riktas mot hela kedjan av händelser

Det är angeläget att i det brottsförebyggande arbetet se på bedrägeriet som en del av en händelsekedja, och att rikta åtgärderna såväl mot de förberedande stegen som mot de brott som följer på bedrägeriet vid hanteringen av brottsvinsten. Vår kartläggning av det bedrägeriförebyggande arbetet visar dock på otillräckliga åtgärder mot de förberedande stegen inför ett bedrägeri. Exempelvis finns behov av noggrannare kontroller av företrädare för företag, användarkonton, annonser och webbplatser. I det sammanhanget ser Brå positivt på förslaget om att Bolagsverket ska få en tydligare kontrollerande roll av företrädare för företag (SOU 2023:34), liksom att stora onlineplattformar och onlinesökmotorer får utökat ansvar för att ta bort illegalt innehåll (EU 2022/2065). Brå ser även behov av att se över möjligheterna att begränsa publiceringen av personuppgifter som kan användas för att kartlägga potentiella brottsoffer. Det finns dessutom behov av riktad information till unga som riskerar att användas som penningmålvakter.

Åtgärder behöver förhålla sig till olika omständigheter

Det finns omständigheter, önskade eller oönskade beroende på perspektiv, som påverkar möjligheterna att arbeta aktivt mot vissa sårbarheter. Det gäller bland annat offentlighetsprincipen och yttrandefrihetsgrundlagen, som påverkar möjligheterna att förhindra kartläggning av potentiella brottsoffer utifrån öppna källor. Andra omständigheter som påverkar det bedrägeriförebyggande arbetet är förväntningar och regleringar som kräver snabba och enkla transaktioner, förekomsten av finansiella online-tjänster som exempelvis handel med kryptovalutor, samt banksekretessen som begränsar bankernas möjligheter att dela information med varandra.

Vissa förebyggande åtgärder begränsas även av brottens internationella karaktär. Det gäller bland annat arbetet mot manipulerade telefonnummer där intervjupersoner med kunskap om telefoni ser behov av internationella ramverk. Även i påverkansarbetet gentemot onlineplattformar och onlinesökmotorer finns behov av internationell samverkan för att få plattformarna att utöka sina kontroller av användare och annonser. Också arbetet med att motverka kortbedrägerier försvåras av att kraven på stark kundautentisering enbart gäller kortköp inom EU. För att få ytterligare genomslag behöver den här typen av åtgärder gälla globalt.

En övergripande och central omständighet är även den generella digitaliseringen. Här ser Brå ett behov av ett utökat stöd till dem som har

svårt att ta del av den digitala utvecklingen vad gäller genomförandet av digitala samhällstjänster, digitala bankärenden och konsumentfrågor.

Omfattande teknisk utveckling behövs inom banksektorn

I likhet med många av intervjupersonerna såväl inom som utanför banksektorn ser Brå ett behov av att förbättra bankernas transaktionsövervakning och utveckla system som på ett bättre sätt fångar upp bedrägliga transaktioner. Det gäller särskilt bedrägerier genom behöriga transaktioner. En möjlighet är en ökad användning av frivilliga begränsningar. Det kan vara beloppsgränser, begränsningar när på dygnet en transaktion kan göras, hur snabbt en transaktion över ett visst belopp ska genomföras, att visa typer av transaktioner ska kräva dubbla signeringar och så vidare. För att en sådan utveckling ska få effekt krävs att kunder i behov av den extra säkerheten får kännedom om och lockas av produkterna. Det krävs också utveckling av anpassade system och säkra lösningar för att låsa upp frivilliga begränsningar.

Andra behov är förbättrad övervakning baserad på kundernas individuella transaktionsmönster, där transaktioner stoppas, flaggas eller på andra sätt begränsas när de avviker från vad banken förväntar sig utifrån tidigare beteenden. En sådan övervakning kan omfatta samtliga kunder och produkter och kräver därmed ingen särskild information till kunderna. Möjligen kan AI användas för att göra den individbaserade övervakningen mer träffsäker.

Brå menar att det är bankerna som måste driva utvecklingen av säkrare banktjänster. De har ett ansvar gentemot sina kunder och gentemot samhället. Samtidigt finns potential för bankerna att använda säkerhetslösningar, såsom frivilliga begränsningar, för att locka kunder. Det kan alltså även finnas ekonomiska incitament som kan bidra till att förbättra bankernas brottsförebyggande arbete.

Informationsinsatser behöver följas upp

Samtliga samhällsaktörer tar upp problem med de åtgärder som syftar till att stärka potentiella brottsoffers motståndskraft mot bedrägerier. De ser bland annat svårigheter med att nå fram med information, särskilt till de grupper som är i allra störst behov av den. Det gäller dels många äldre som kanske varken deltar i träffar och utbildningar hos seniororganisationer eller tar del av information och varningar på internet, dels grupper som anser sig ha tillräcklig kunskap och därför varken söker eller tar del av

relevant information. I rapporten framgår att det görs särskilda satsningar för att nå dessa grupper, exempelvis genom att sprida information via anhöriga och de fysiska vykort som Polismyndigheten skickat till ett stort antal hushåll under våren 2023. En uppföljning av en tidigare motsvarande satsning på vykort i Polisregion Syd visar dock att det kan vara svårt att nå fram även med vykort (Edman m.fl. 2022). I uppföljningen av 2022 års Tänk säkert-kampanj framkommer att 33 procent i målgruppen äldre nåtts av kampanjen, vilket är betydligt lägre än målgruppen unga där motsvarande andel är 51 procent (MSB 2022). En riktad informationssatsning mot kvinnor mellan 70 och 85 år i Jämtlands län under våren 2023 visade dock på bättre resultat – 72 procent av de som fått ett informationsbrev om hur man kan skydda sig mot bedrägerier svarade på uppföljande frågor som visar att de tagit del av informationen. Uppföljningen indikerar att det är möjligt att nå fram med information. Brå ser dock ett fortsatt behov av uppföljningar av hur väl informationen har nått fram till dem som behöver den, och fler innovativa sätt att nå ut till de mest sårbara grupperna.

Informationen måste anpassas för att få effekt

Även i de fall informationen når fram är det inte säkert att den får effekt, det vill säga att mottagarna påverkas i sitt agerande i önskvärd riktning. Intervjupersoner från olika aktörer uttrycker tveksamhet till om information verkligen kan ha en bedrägeriförebyggande effekt och är delvis kritiska till det arbete som görs. Det finns också ett flertal studier som visar på att det är tveksamt om informationsinsatser påverkar människors beteende. I en uppföljning av Polismyndighetens satsning på vykort framkommer att en majoritet av dem som hade utsatts för försök till bedrägeri inte ansåg sig hjälpta av vykorten i sin förmåga att stå emot bedrägeriförsöket (Tornberg m.fl. 2023). Det finns också ett flertal utvärderingar av olika informationskampanjer som visar på svaga, inga eller till och med oönskade effekter, bland annat kampanjer mot ungdomars droganvändning, för ökad anmälningsbenägenhet, om pensionssystemet och mot stor alkoholkonsumtion (Espinosa & Stoop 2021, Allara m.fl. 2015, Finseraas m.fl. 2015).

Samtidigt ger forskningen inte underlag för ett generellt uttalande att informationsinsatser aldrig kan påverka människors beteende och ifall de kan ha en bedrägeriförebyggande effekt eller inte.

En vanlig utgångspunkt inom forskningen är att det inte finns någon direkt länk mellan information och beteende, men att information kan påverka en människas beteende via hens attityd (Fishbein & Ajzen 2010, Jagers m.fl. 2009, Sacco & Silverman 1981). Det finns bland annat uppföljningar av informationskampanjer om informationssäkerhet som visar att en ökad medvetenhet kan leda till en ökad benägenhet att vidta säkerhetsåtgärder, men att budskap och innehåll måste anpassas både utifrån målgrupp och sammanhang för att människor ska känna att informationen är relevant för dem och något som de ska agera på (Brady & Heini 2020, Bada m.fl. 2014, se även Montagni m.fl. 2022, Wallenius 2022, Espinosa & Stoop 2021, Allara m.fl. 2015). Flera intervjupersoner uttrycker liknande ståndpunkter och menar även att de behöver få folk att prata med varandra, dela erfarenheter och kanske praktiskt förbereda sig. Om budskap förmedlas genom lokala sociala nätverk minskar också risken för att informationen leder till osund oro och skuldbeläggande av dem som drabbas, vilket annars kan vara en risk (Horgan 2019).

Faktorerna vi nämnt här är i viss utsträckning synliga i de åtgärder som har presenterats i rapporten, exempelvis flera kampanjer särskilt riktade gentemot äldre med innehåll som har bedömts som särskilt relevant för just dessa grupper samt motsvarande till barn och unga. Lokala träffar och informationsmöten anordnade av seniororganisationer eller kommunpoliser hör också hit. Dessa aktiviteter behöver dock anpassas ytterligare och bli än mer relevanta för att nå fram och kunna påverka beteendet hos de tilltänkta målgrupperna. För Polismyndigheten kan en ökad målgruppsanpassning bland annat kräva ett ökat stöd till, och erfarenhetsutbyte med lokalpolisområdena, för att de bättre ska kunna inkludera bedrägerier i lokala lägesbilder och rikta sina förebyggande åtgärder rätt.

Därtill behöver olika typer av kunskapshöjande åtgärder i högre grad innehålla praktiska inslag. Det för att informationen ska leda till ett förändrat beteende och för att komma åt sårbarheter hos potentiella brottsoffer som kopplar till bland annat stress, artighet och tilltro till auktoriteter. Forskning visar att beslutsfattande vid stress i högre grad styrs av tidigare erfarenheter och beteenden än av kunskap och överväganden (Sjöberg m.fl. 2006). Praktiska övningar är ett sätt att skapa erfarenhet som kan styra agerandet. I det förebyggande arbetet mot telefonbedrägerier skulle till exempel de praktiska inslagen kunna bestå av rollspel och praktisk träning på att exempelvis inte vara tillmötesgående vid samtal när någon ringer och erbjuder hjälp.

Ett helhetsperspektiv på teknik och individ

Många intervjupersoner pekar på att det behövs såväl information och kunskap som tekniska och strukturella åtgärder för att kunna förebygga bedrägerier. De understryker behov av åtgärder mot flera sidor av brottstriangeln eller mot samtliga förutsättningar som enligt rutinaktivitetsteorin behövs för att ett brott ska kunna ske (Cohen & Felson 1979).

Att ett helhetsperspektiv på teknik och mänskligt beteende är avgörande för att lyckas i det brottsförebyggande arbetet framgår även av forskningen (Back & LaPrade 2019). Genom exempelvis pushnotiser och varningar baserade på individens aktivitet kan tekniken bidra till mer målgruppsanpassad och relevant information till individen. På motsvarande sätt kan tydlig och lättillgänglig information motivera till säkra val och korrekt användning av exempelvis digitala tjänster.

Flera intervjupersoner inom den privata sektorn understryker att det måste vara enkelt att göra rätt – det behöver vara enkelt att förstå och smidigt att välja att ha den säkraste inställningen. Det kan till exempel handla om att den säkraste lösningen är förvald vid valbara åtgärder. Den här typen av åtgärder angränsar till så kallad ”nudging” (puffning). Nudging är ett synsätt där påverkan av människors beteende inte går via attityder utan andra åtgärder som helt enkelt knuffar människors beteende i en specifik riktning. Det centrala är inte vad människor vill göra, känner att de borde göra eller tror att de gör, utan vad man faktiskt gör (Lemoine m.fl. 2019, Thaler & Sunstein 2008). Brå ser stora möjligheter med nudging och att genom att integrera de två perspektiven information och teknik styra människor mot ett säkert beteende.

Bedragarna hittar hela tiden nya sårbarheter

Vikten av ett helhetsperspektiv stärks av att bedragarna tenderar att anpassa sina tillvägagångssätt och hitta nya kryphål när säkerheten höjs. Företag och individer som inte hänger med i den tekniska utvecklingen riskerar dessutom att bli ännu mer utsatta. Intervjupersoner menar att en förhöjd säkerhet har medfört att bedragarna i högre utsträckning angriper individen direkt genom social manipulation och på senare tid särskilt genom bedrägliga behöriga transaktioner. Det är troligen också en förklaring till att just äldre och extra sårbara personer i allt högre grad har blivit måltavlor för bedrägerier. En trolig utveckling är därtill att bedragarna i framtiden använder sig av AI i sin manipulation av brottsoffer,

vilket ökar sårbarheten ytterligare. Den tekniska säkerheten och individens förmåga att skydda sig blir därmed två delar beroende av varandra.

Brås bedömning

Bedrägerier mot privatpersoner är ett brott med allvarliga konsekvenser som drabbar både individ och samhälle. Telefonbedrägerier framträder som särskilt oroande eftersom de ofta innebär stora ekonomiska och känslomässiga skador för brottsoffret, riskerar att påverka förtroendet för samhällets institutioner och system samt ger stora brottsvinster till kriminella nätverk. Även andra bedrägerier får allvarliga konsekvenser. Brå bedömer därför att det är angeläget att generellt prioritera det brotts-förebyggande arbetet mot bedrägerier mot privatpersoner.

Brå har identifierat ett stort antal sårbarheter som möjliggör brott, både hos potentiella brottsoffer och i de tekniska och strukturella omständigheterna. En samlad bedömning är att med några få undantag träffas sårbarheterna av någon form av förebyggande åtgärd. Uppenbart är dock att bedragarna hela tiden utvecklar sina metoder och strategier och hittar nya sårbarheter i såväl teknik och struktur som hos individen. Den fortsatt omfattande och i flera avseenden ökande brottsligheten visar också att det förebyggande arbetet som görs inte är tillräckligt och att det finns behov av fortsatt utveckling och förbättring.

Bedrägeri handlar om att människor luras och i takt med att tekniken blir säkrare inriktar sig bedragarna mer och mer mot individen. Åtgärder med syfte att göra potentiella brottsoffer mer svårlurade är därmed nödvändiga. Åtgärderna måste dock utformas på ett sätt så att de blir än mer relevanta för målgrupperna, bland annat genom fler praktiska inslag. Samtidigt innebär digitaliseringen att enskilda individer dels fått ett ökat ansvar för att skydda sina banktillgångar, dels är beroende av digitala lösningar som de inte alltid behärskar. Banker och andra aktörer, privata liksom offentliga, som utvecklar och tillhandahåller de tjänster och system som utnyttjas i bedrägerier behöver därför återta delar av ansvaret och genom säkrare lösningar bättre skydda individen.

Brå ser också ett behov av ett tydligare helhetsperspektiv i det bedrägeriförebyggande arbetet där teknik och information används tillsammans för att bättre möta bedragarnas snabba anpassningar. Genom att använda tekniska lösningar kan informationen bli mer träffsäker,

relevant och tydlig. Informationen i sin tur behövs för korrekt användning av de tekniska lösningarna.

Brås rekommendationer:

- Polismyndigheten bör ta en ledande roll i det bedrägeriförbyggande arbetet. Bland annat krävs ett utökat stöd till polisregionerna och lokalpolisområdena om hur den lokala nivån kan inkludera bedrägerier i sina lägesbilder och åtgärdsplaner. För att säkerställa att de problembilder som polisen tar fram är relevanta för det bedrägeriförebyggande arbetet bör de inkludera även försöksbrott och anmälningar som direktavskrivs. Polisen behöver också uppdatera och höja relevansen i existerande informations- och utbildningsmaterial om bedrägerier genom ytterligare målgruppsanpassning och fler och mer anpassade praktiska inslag. Därtill krävs en bred implementering av den brottsförebyggande strategin inom myndigheten.
- Polismyndigheten bör i samverkan med exempelvis Sveriges kommuner och regioner, Stöldskyddsföreningen, Internetstiftelsen och Myndigheten för samhällsskydd och beredskap, utveckla och systematisera riktade informationsinsatser till barn och unga som riskerar att användas som penningmålvakter.
- För att försvåra förberedelser till bedrägerier och försvåra hanteringen av brottsvinster bör Bolagsverket, Internetstiftelsen, onlineplattformar och onlinesökmotorer utöka sina kontroller av företrädare för företag och domäner, och av webbplatser, användarkonton och annonser. Brå ser särskilt ett behov av att Bolagsverket i enlighet med förslagen i SOU 2023:34 utökar sina kontroller av företrädare för företag.
- Regeringen bör se över vad det finns för möjligheter att begränsa publiceringen av personuppgifter som kan användas för att kartlägga potentiella brottsoffer för bedrägerier.
- Post- och telestyrelsen, telefonoperatörerna och Telekområdgivarna bör fortsätta och påskynda arbetet mot manipulerade telefonnummer, samt utveckla det arbetet till fler områden, såsom bedräglig användning av sms och mobiltelefonnummer.
- Regeringen bör ta vidare förslaget om en statlig e-legitimation. E-legitimationen behöver implementeras samt på sikt utvecklas.
- Samtliga banker bör säkerställa att Bank-id:s lösningar för säker identifiering och signering implementeras fullt ut. Osäkra alternativ

bör samtidigt fasas ut. Bankerna bör också fortsätta utvecklingen av säkrare digitala banker, särskilt avseende behöriga transaktioner. Områden där Brå särskilt ser utvecklingsmöjligheter är bankprodukter med frivilliga begränsningar, och individbaserad transaktionsövervakning.

- Olika samhällsaktörer bör utveckla användandet av pushnotiser och varningar som relaterar till individens aktivitet. Brå ser också en möjlighet att i högre utsträckning använda åtgärder som knuffar personer mot det säkra alternativet, så kallad nudging.
- Offentliga aktörer på alla nivåer bör utöka sitt stöd till personer som behöver hjälp med att genomföra digitala tjänster, såsom digitala bankärenden, digitala samhällstjänster och digital handel. Det gäller särskilt kommunerna som sedan den 1 juli 2023 (enligt lag 2023:196) har ett ansvar för brottsförebyggande arbete.
- Förväntade effekter av såväl tekniska och strukturella åtgärder som åtgärder för att stärka potentiella brottsoffer behöver utvärderas och följas upp. Tekniska och strukturella åtgärder bör även föregås av risk- eller sårbarhetsanalyser. Analyserna och utvärderingarna bör inkludera analyser av eventuella förflyttningar av brottsligheten, liksom om åtgärderna medför några oönskade konsekvenser, exempelvis för grupper som inte använder sig av nya lösningar eller rutiner.

Referenslista

Allara, E. m.fl. (2015). ”Are mass-media campaigns effective in preventing drug use? A Cochrane systematic review and meta-analysis.” *BMJ open*, 5(9), e007449.

Back, S., och LaPrade, J. (2019). ”The future of cybercrime prevention strategies: Human factors and a holistic approach to cyber intelligence.” *International Journal of Cybersecurity Intelligence & Cybercrime*. Volym 2, nr 2, s. 1–4.

Bada, M., Sasse, A.M. och Nurse, J.R.C. (2014). *Cyber Security Awareness Campaigns: Why do they fail to change behavior?* Finns tillgänglig: https://arxiv.org/abs/1901.02672 Hämtad: 2023-05-10.

Brady, S. och Heini, C. (2020). *Cybercrime: Current Threats and Responses. A review of the research literature*. Dublin: Department of Justice and Equality.

Brottsförebyggande rådet, Brå (2016). *Bedrägeribrottsligheten i Sverige. Kartläggning och åtgärdsförslag*. Rapport 2016:9. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2018a). *Orsaksanalys i lokalt brottsförebyggande arbete*. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2018b). *Brott mot äldre. Om utsatthet och otrygghet*. Rapport 2018:7. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2020). *Samverkan i lokalt brottsförebyggande arbete*. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2022a). *Nationella trygghetsundersökningen 2022. Om utsatthet otrygghet och förtroende*. Rapport 2022:9. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet (2022b). *Polisanmälda dataintrång. Karaktär, utmaningar, utvecklingsområden*. Rapport 2022:8. Stockholm: Brottsförebyggande rådet.

Brottsförebyggande rådet, Brå (2023). *Statistik över anmälda brott*. https://statistik.bra.se/solwebb/action/index

Clarke, R.V. (1997). *Situational Crime Prevention. Successful Case Studies*. New York: Harrow & Heston.

CAN (2023). *Narkotikaprisutvecklingen I Sverige 1988-2022*. CAN Rapport 219. Stockholm: CAN.

Cohen, L. E., och Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review*, 588–608.

Digital Fraud Committee (2022). *Fighting Fraud: Breaking the Chain*. Committee Office, House of Lords, London. Finns tillgänglig: https://committees.parliament.uk/publications/31584/documents/177260/default/ Hämtad: 2022-12-20.

Edman, E. m.fl. (2022). *Åldringsbedrägerier i Malmö. En kartläggning av sårbarhetsfaktorer, informationsspridning och brottsförebyggande åtgärder*. Malmö: Malmö universitet.

Engdahl, O. (2022). *Kriminologiska perspektiv på bedrägerier och ekonomisk brottslighet*. Stockholm: Liber.

Espinosa, R. och Stoop, J. (2021). ”Do People Reallly Want to Be informed? Ex-ante Evaluations of Information-Campaign Effectiveness.” *Experimental Economics*, 24(4), 1131–1155.

EU 2022/2065. *Förordningen om en inre marknad för digitala tjänster*. Strasbourg: Europaparlamentet och rådet. Finns tillgänglig: https://eur-lex.europa.eu/legal-content/SV/TXT/HTML/?uri=CELEX:32022R2065&qid=1685436160304. Hämtad 2023-05-30.

EU 2015/2366. *Direktivet om betaltjänster på den inre marknaden*. Strasbourg: Europaparlamentet och Europarådet. Finns tillgänglig: https://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A32015L2366. Hämtad 2023-05-30.

Europeiska centralbanken, ECB (2021). *Seventh report on card fraud*. October 2021. Frankfurt: European Central Bank. Finns tillgänglig: https://www.ecb.europa.eu/pub/cardfraud/html/ecb.cardfraudreport202110~cac4c418e8.en.html#toc11. Hämtad 2023-08-09.

Finseraas, H., Jakobsson, N., och Svensson, M. (2015). ”Do knowledge gains from public information campaigns persist over time? Results from a survey experiment on the Norwegian pension reform.” *Journal of Pension Economics & Finance*, 16(1), 108–117.

Fishbein, M. och Ajzen, I. (2010). *Predicting and Changing Behavior. The Reasoned Action Approach*. New York: Psychology Press.

Horgan, S.H. (2019). *Cybercrime and Everyday Life: Exploring public sensibilities towards the digital dimensions of crime and disorder*. Edinburgh: University of Edinburgh.

Integritetsskyddsmyndigheten (2023). Har du svårt att få bort något om dig från nätet? Finns tillgänglig: https://www.imy.se/privatperson/dataskydd/vi-guidar-dig/utgivningsbevis/ Hämtad: 2023-06-29.

Internetstiftelsen (2022). *Svenskarna och internet 2022*. Stockholm: Internetstiftelsen. Finns tillgänglig: https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2022/. Hämtad: 2023-09-01.

Jagers, S., Martinsson, J. och Nilsson, A. (2009). *Kan vi påverka folks miljöattityder genom information? En analys av radiosatsningen ”Klimatfeber”*. Rapport till Expertgruppen för miljöstudier 2009:4. Stockholm: Finansdepartementet.

Konsumentverket (2023). *Bedrägeridrabbad får KO-stöd i tvist mot banken*. Pressmeddelande 17 januari 2023. Finns tillgängligt: https://www.konsumentverket.se/aktuellt/nyheter-och-pressmeddelanden/pressmeddelanden/2023/bedrageridrabbad-far-ko-stod-i-tvist-mot-banken/ Hämtat: 2012-08-22.

Lemoine, I., Lindström, K., Lindström, L. och Salzer, S. (2019). *Nudging i praktiken. Så gör organisationen det lätt att göra rätt*. Stockholm: Natur och kultur.

Mondani, H. och Rostami, A. (2022). ”Samarbete i brott: Organiserad brottslighet i Sverige 1995–2015”. I Rostami, A. och Sarnecki, J. (red.) *Det svenska tillståndet. En antologi om brottsutvecklingen i Sverige*. Lund: Studentlitteratur.

Montagni, I., m.fl. (2022). ”Mixed-methods evaluation of a prevention campaign on binge drinking and cannabis use addressed to young people.” *Journal of Substance Use*, 1–6.

Myndigheten för digital förvaltning (DIGG) (2023). *En säker och tillgänglig statlig e-legitimation. Slutredovisning av regeringsuppdrag att föreslå hur en statlig e-legitimation kan utformas*. (I2022/01335).

Myndigheten för press, radio och tv (2023). Det här är ett utgivningsbevis. Finns tillgänglig: https://www.mprt.se/regelverk/utgivningsbevis/ Hämtad: 2023-06-29.

Myndigheten för samhällsskydd och beredskap (MSB) (2022). *Slutredovisning av regeringsuppdrag. Uppdrag till Myndigheten för samhällsskydd och beredskap gällande: Informationskampanj till allmänhet och företag om informations- och cybersäkerhet*. (Ju2022/01292).

Polismyndigheten (2016). *Nationellt bedrägericenter. Intressant just nu om bedrägerier*. Informationsblad A116.272/2015. Nationellt bedrägericenter, Nationella operativa avdelningen, Polismyndigheten.

Polismyndigheten (2019). *Analys av kärnverksamheten mot 2024. Underlag för dimensionering och förmågeutveckling*. Rapport A240.625/2019. Nationella operativa avdelningen, Polismyndigheten.

Polismyndigheten (2021). *De organiserade bedrägerierna. En rapport om bedrägerier kopplade till organiserade kriminella miljöer*. Dnr: A354.340/2021.

Polismyndigheten (2022a). *Polismyndighetens strategi för det brottsförebyggande arbetet*. PM 2022:12. A153.079/2020.

Polismyndigheten (2022b). *Vishinganalys*. Rapport A114.656/2022. Nationellt bedrägericentrum, Nationella operativa avdelningen, Polismyndigheten.

Polismyndigheten (2023a). *Brottsvinsterna för bedrägeribrottsligheten 2022. Analys*. Rapport A232.846/2023. Nationellt bedrägericentrum, Nationella operativa avdelningen, Polismyndigheten.

Polismyndigheten (2023b). *Finanspolisens årsrapport*. Polismyndigheten, april 2023.

Prop. 2022/23:9. *Stark kundautentisering vid fakturabetalningar online*. Stockholm: Justitiedepartementet. Finns tillgänglig på regeringens webbplats: https://www.regeringen.se/rattsliga-dokument/proposition/2022/10/prop.-2022239. Hämtad 2023-05-30.

Rebovich, D. och Byrne, J.M. (2023). *The New Technology of Financial Crime. New crime commission technology, new victims, new offenders, and new strategies for prevention and control*. New York: Routledge.

Regeringen skrivelse, Skr. 2016/17:126. *Tillsammans mot brott. Ett nationellt brottsförebyggande program*. Finns tillgänglig på regeringens webbplats: https://regeringen.se/tillsammansmotbrott. Hämtad 2023-05-30.

Sacco, V. F., och Silverman, R. A. (1981). ”Selling crime prevention: The evaluation of a mass media campaign.” *Canadian Journal of Criminology*, 23(2), 191–202.

Sjöberg, M., Wallenius, C. och Larsson, G. (2006). *Ledarskap och beslutsfattande under stress vid komplexa räddningsinsatser: en sammanfattande rapport*. ILM Serie I:24. Stockholm: Försvarshögskolan.

SOU 2023:34. *Bolag och brott – några åtgärder mot oseriösa företag*. Betänkande av Utredningen om bolaget som brottsverktyg. Stockholm: Elanders Sverige AB.

Stiftelsen Tryggare Sverige (2023). *Utvärderat koncept som ger barn kunskaper och färdigheter i cybersäkerhet kommer till Sverige*. Finns tillgänglig: https://www.mynewsdesk.com/se/stiftelsen-tryggare-sverige/pressreleases/utvaerderat-koncept-som-ger-barn-kunskaper-och-faerdigheter-i-cybersaekerhet-kommer-till-sverige-3254890. Hämtad 2023-08-23.

Thaler, R. och Sunstein, C. (2008). *Nudge: Improving Decisions about Health, Wealth, and Happiness*. New Haven CT: Yale University Press.

Thodelius, C. och Ceccato, V. (2022). *Kriminologiska perspektiv på situationsbaserad brottsprevention*. Stockholm: Liber.

Tonry, M. och Farrington, D (1995). ”Strategic Approaches to Crime Prevention”. *Crime & Justice*, 19, 1–20.

Tornberg, E., Mhana, F. och Kasumi, R. (2023). *Telefonbedrägerier mot äldre. En effektanalys av polisens brottsförebyggande informationssatsning*. Examensarbete i kriminologi. Malmö universitet.

Tradera (2023). *Traderabetalning* och *Säkerhetscenter*. Finns tillgänglig: https://info.tradera.com. Hämtad 2023-05-23.

UNODC (2010). *Handbook on the crime prevention guidelines. Making them work*. Criminal Justice Handbook Series. New York: United Nations.

Visa (2023). *Outsmarting Fraudsters with Advanced Analytics*. Finns tillgänglig: https://usa.visa.com/visa-everywhere/security/outsmarting-fraudsters-with-advanced-analytics.html. Hämtad 2023-05-23.

Wallenius, C. (2022). ”Do Hostile Information Operations Really Have the Intended Effects? A Literature Review.” *Journal of Information Warfare,* 21(2), 21–35.

Williams, M.L. och Levi, M. (2017). ”Cybercrime prevention”. I (red.) Tilley, N. och Sidebottom, A. *Handbook of crime prevention and community safety*. New York: Routledge.

Bilageförteckning

Bilaga 1 Metod och material

Den här studien består av tre delar: en kartläggning av brottsproblemet, en kartläggning av polisens och andra aktörers bedrägeriförebyggande arbete, samt en analys av träffsäkerheten hos de brottsförebyggande åtgärderna som utgår från de båda kartläggningarna. Studien bygger i huvudsak på kvalitativt material – intervjuer samt analyser av skriftligt material – kompletterat med statistik. Här redogörs för det material som har använts.

Intervjuer med nyckelpersoner

Studien bygger framförallt på intervjuer med nyckelpersoner hos centrala aktörer. Syftet med intervjuerna inom ramen för den första kartläggningen var att få en översiktlig förståelse för brottsproblemet, vilka som utsätts för bedrägerier liksom sårbarheter i tillfällesstrukturen. Intervjupersonerna bestod av personer med god kännedom om brottsproblemet. Eftersom kartläggningen syftar till att ge en samlad beskrivning av brottsproblemet utifrån intervjuerna presenteras i texten specifika aktörer bara när det bedöms som särskilt relevant.

Intervjuerna inom ramen för den andra kartläggningen syftade till att få kunskap om det bedrägeriförebyggande arbetet som genomförs av olika aktörer. Intervjupersonerna bestod här av personer med kunskap om det brottsförebyggande arbetet. Eftersom den andra kartläggningen syftar till att beskriva det brottsförebyggande arbetet är det till skillnad från den första kartläggningen i stället många gånger relevant att specificera vilka aktörer intervjupersonerna representerar.

Intervjuerna inkluderar de här aktörerna:

Polismyndigheten (17 intervjuer med 19 personer):
- nationellt: 6 intervjuer
- regionalt: 11 intervjuer.

Övriga statliga myndigheter (10 intervjuer med 14 personer):
- Åklagarmyndigheten: 1 intervju
- Brottsoffermyndigheten: 1 intervju
- Myndigheten för samhällsskydd och beredskap: 1 intervju
- Finansinspektionen: 2 intervjuer
- Konsumentverket: 1 intervju (2 personer)
- Post- och telestyrelsen: 1 intervju (4 personer)
- Ekobrottsmyndigheten: 1 intervju
- länsstyrelserna: 1 intervju

- Myndigheten för digital förvaltning: 1 intervju.

Företag (8 intervjuer med 9 personer):

- Finansiell Id-teknik: 2 intervjuer
- Microsoft: 1 intervju
- Blocket: 1 intervju
- 3 storbanker: 3 intervjuer
- Meta: 1 intervju (2 personer).

Övriga aktörer (12 intervjuer med 14 personer):

- Internetstiftelsen: 2 intervjuer (3 personer)
- Svensk handel: 1 intervju
- Stöldskyddsföreningen: 1 intervju
- Bankföreningen: 1 intervju
- Sparbankernas riksförbund: 1 intervju
- Brottsofferjouren: 1 intervju
- Konsumenternas: 1 intervju
- Telekområdgivarna: 1 intervju
- seniororganisationer: 3 intervjuer (4 personer).

Minnesanteckningar från samtal eller möten:

- Polismyndigheten: 7 samtal (2 nationellt, 3 regionalt, 2 lokalt)
- telefonoperatörer: 2 samtal med 5 personer.

Vilka aktörer som har intervjuats har inte legat fast från start utan har till stor del vuxit fram efter hand och till följd av den kunskap som har utvecklats under arbetets gång. Det har också skett ett visst snöbollsurval.

I rapportens inledning framgår att utgångspunkten i valet av intervjupersoner skiljer sig mellan de båda kartläggningarna. I viss mån finns det en överlappning mellan de båda kartläggningarna vad det gäller aktörer och nyckelpersoner. Analyserna har dock gjorts separat för respektive kartläggning. Samtliga intervjuer har genomförts under hösten 2022 eller våren 2023.

Varje intervju har genomförts med stöd av en intervjuguide framtagen utifrån studiens frågeställningar och anpassad efter den aktuella intervjupersonen. Intervjuerna genomfördes antingen fysiskt eller digitalt och varade ifrån cirka 45 minuter till upp till 2 timmar. Nästan alla intervjuer genomfördes tillsammans av projektets två medarbetare. Intervjuerna spelades in och sammanfattande anteckningar togs antingen under tiden intervjun genomfördes eller i efterhand. Materialet har sedan

bearbetats, systematiserats och analyserats för att uppfylla syftet med studien.

Dokumentanalys

I båda kartläggningarna har skriftligt material använts för att komplettera intervjuerna. För kartläggningen av brottsproblemet inkluderar materialet bland annat skriftliga rapporter och information från webbplatser, medan materialet som användes i kartläggningen av det brottsförebyggande arbetet bland annat inkluderar kampanjsidor, samt utbildnings- och informationsmaterial som syftar till att förebygga bedrägerier.

Dokumentanalysen inkluderar de här källorna till kartläggningen av brottsproblemet:

Rapporter och övrigt skriftligt material från Polismyndigheten:

- Polismyndigheten (2022). *Kortbedrägeri – Card-not-present (CNP). Tematisk rapport*. Rapport A554.326/2022. Nationellt bedrägericentrum.
- Polismyndigheten (2022). *Nationella operativa avdelningens strategiska inriktning 2020–2024, revidering 2022*. Beslutsprotokoll Noa 61/2022, ärende A279.313/2021.
- Polismyndigheten (2022). *Brottsofferanalys*. Rapport A221025/2022. Nationellt bedrägericentrum.
- Polismyndigheten (2022). *Tematisk rapport om investeringsbedrägerier*. Rapport A214.558/2022. Nationellt bedrägericentrum.
- Polismyndigheten (2022). *Vishinganalys*. Analys A114.656/2022. Nationellt bedrägericentrum.
- Polismyndigheten (2022). *Bedrägerier och penningtvätt. Analys av bedrägerier ur ett brottsvinstperspektiv*. Rapport A697.130/2021, Saknr: 423. Finanspolissektionen.
- Polismyndigheten (2022). Lägesbild för januari–augusti 2022 samt för december 2022. Nationellt bedrägericentrum.
- Polismyndigheten (2022). *Rapport angående BF-funktion Region Syd*. Polisregion Syd, 2022-01-17.
- Polismyndigheten (2021). *De organiserade bedrägerierna. En rapport om bedrägerier kopplade till organiserade kriminella miljöer*. Rapport A354.340/2021. Nationellt bedrägericentrum.
- Polismyndigheten (2021). *Internrevisionens uppföljande granskning av polisregionernas handläggning av bedrägeriärenden*. Rapport

A244.678/2016, Saknr: 977. Internrevisionen.
- Polismyndigheten (2020). *Hantering av bedrägeribrottsligheten i ett framåtblickande perspektiv. Att långsiktigt stärka Polisens förmåga att förebygga och utreda bedrägeribrott*. Rapport A231.788/2020.
- Polismyndigheten (2020). *Bedrägeribrottsligheten i Sverige 2019. Årsrapport*. Nationellt bedrägericenter.
- Polismyndigheten (2019). *Beslut om placering m.m. av Nationellt bedrägericenter (NBC) vid nationella operativa avdelningens utredningsenhet*. Beslutsprotokoll Noa 103/20, ärenden A176.096/2019.
- Polismyndigheten (2019). *Analys av kärnverksamheten mot 2024. Underlag för dimensionering och förmågeutveckling*. Rapport A240.625/2019, Saknr: 190. Nationella operativa avdelningen.
- Polismyndigheten (2015). *Bedrägerier mot äldre. En studie av anmälda förmögenhetsbrott mot äldre juni–december 2014*. Rapport A023.211/2015. Nationellt bedrägericenter.

Övrigt skriftligt material:

- Brottsofferjouren i Sverige (2021). Tema Bedrägeribrott. *Tidningen Brottsoffer*, nr 4/2021, s. 9–16. Finns tillgänglig: https://www.brottsofferjouren.se/om-oss/tidningen-brottsoffer/arkiv-tidningen-brottsoffer/.
- Dagens juridik (2022). FI: ”Bedragarna blir alltmer raffinerade i sitt tillvägagångssätt”. Finns tillgänglig: https://www.dagensjuridik.se/nyheter/fi-bedragarna-blir-alltmer-raffinerade-i-sitt-tillvagagangssatt/. Publicerad: 2022-10-05. Hämtad: 2022-10-06.
- Europol (2022). *EU SOCTA 2021 – European Union Serious and organized crime threat assessment. A corrupting influence: The infiltration and undermining of Europe’s economy and society by organized crime*. Luxembourg: Publications Office of the European Union.
- Finansinspektionen (2022). *Fler varningar för bedrägerier 2021*. Finns tillgänglig: https://www.fi.se/sv/publicerat/nyheter/2022/fler-varningar-for-bedragerier-2021/. Publicerad: 2022-01-18. Hämtad 2022-09-20.
- Finansinspektionen (2022). *Konsumentskyddsrapport 2022*. Dnr: 21-33605, 7 april 2022.
- Finansinspektionen (2021). *Investeringsbedrägerier. Så kan det gå till*. Finns tillgänglig:

https://www.fi.se/sv/konsumentskydd/investeringsbedragerier/sa-kan-det-ga-till/. Sidan senast granskad: 2021-08-09. Hämtad: 2022-10-07.
- Internetstiftelsen (2022). *Hjälp ditt barn tänka säkert på nätet*. Finns tillgänglig: https://internetstiftelsen.se/tanksakert/foralder/?utm_source=collab&utm_medium=referral&utm_campaign=trafik&utm_content=sk. Hämtad: 2022-10-18.
- Internetstiftelsen (2022). *Tänk säkert: fördjupande artiklar*. Finns tillgängliga: https://internetkunskap.se/sakerhet-pa-natet/. Hämtade: 2022-10-19.
  - Så blir du lurad via öppna nätverk
  - Hur säker är din e-legitimation?
  - Därför är din router en stor säkerhetsrisk
  - Så avslöjar du falska webbsidor
  - Därför vill kriminella kapa just dig på Facebook och Instagram
  - Därför vill kriminella smitta dig med skadlig kod
  - Så undviker du att bli utsatt för kortbedrägerier
  - Så används smarta prylar för att spionera på dig
  - Hur kan jag undvika att bli lurad av nätfiske?
  - Oroar du dig för bank-id-bedrägerier? Så här får du koll!
  - Så blir mobilen din värsta fiende
  - Passa dig för det här när du handlar på nätet
  - Är det inte dags att bry dig lite mer om dina lösenord?
  - Så slipper du bli lurad när du handlar begagnat på nätet
  - Så lurar kriminella dig genom bluffmejl
- Norman, T. (2019). *The Social Costs of Card-Not-Present Fraud in Sweden*. Masteruppsats i ekonomi, våren 2019.
- Sigblad, A. (2022). Bedragarna ligger alltid steget före. Finansliv. Finns tillgänglig: https://www.finansliv.se/artikel/bedragarna-ligger-alltid-steget-fore/. Publicerad: 2022-11-02. Hämtad: 2022-11-03.
- Svensk Handel (2020). *Handelns utsatthet för IT-relaterad brottslighet*. Finns tillgänglig: https://www.svenskhandel.se/api/documents/rapporter/svensk-handels-bedragerirapport-2020-2.pdf. Hämtad: 2022-11-07.
- Tänk säkert (2022). *Fördjupning om nätfiske*. Finns tillgänglig: https://tanksakert.sakerhetskollen.se/fordjupning-natfiske-phishing. Hämtad: 2022-10-18.
- Tänk säkert (2022). *Social manipulation – vad är det och hur du*

undviker att drabbas. Finns tillgänglig: https://tanksakert.sakerhetskollen.se/social-manipulation. Hämtad: 2022-10-18.

- Tänk säkert (2022). *Undvik att bli lurad – lär dig känna igen annonsbedrägerier*. Finns tillgänglig: https://tanksakert.sakerhetskollen.se/annonsbedragerier. Hämtad: 2022-10-18.

I likhet med intervjuerna har de analyserade dokumenten och övrigt material valts ut löpande. Urvalet har dels gjorts genom egna sökningar, dels genom att intervjupersoner liksom Brås kontakt på Nationellt bedrägericentrum (NBC) har tillfrågats om relevanta dokument. Dokumenten bearbetades, systematiserades och analyserades tillsammans med intervjuerna för kartläggningen av brottsproblemet.

Dokumentanalysen inkluderar de här källorna till kartläggningen av det brottsförebyggande arbetet:

- samtliga intervjuade aktörers webbplatser
- webbsidor inom ramen för kampanjen *Tänk säkert* (MSB, Säkerhetskollen/Stöldskyddsföreningen, Internetstiftelsen)
- kampanjen *Svårlurad!*
- utbildningspaketet *Försök inte lura mig*
- samtalsstödet *Prata med nära och kära om bedrägerier*
- svarsbrev med återkoppling på bedrägeriinsats från Länsstyrelsen Jämtlands län, Polismyndigheten och Stöldskyddsföreningen
- rapporter och annat skriftligt material som intervjupersoner skickat, men som enbart förtydligar eller exemplifierar det bedrägeriförebyggande arbete som de redan har beskrivit i intervjuerna.

Övrigt skriftigt material som beskriver olika aktörers bedrägeriförebyggande arbete har när det använts refererats till löpande i rapporten.

En översiktlig innehållsanalys gjordes i syfte att få en överblick över de olika aktörernas förebyggande arbete.

Statistik

I den första kartläggningen användes statistik för att komplettera intervjupersonernas uppfattning av brottsproblemets omfattning. Det handlar dels om Brås statistik över anmälda brott och uppgifter från den

Nationella trygghetsundersökningen (NTU), dels om statistiska uppgifter från Nationellt bedrägericentrum (NBC), Brottsoffermyndigheten och Konsumentverket. Statistiken från NBC inkluderar statistik över brottstyper utifrån den anmälda brottsligheten, liksom statistik över brottsvinster. Statistiken från Brottsoffermyndigheten och Konsumentverket utgår från myndigheternas kontakter med brottsoffer respektive konsumenter. Också statistik om internetvanor och utsatthet för brott på internet som redovisas i Internetstiftelsens rapport *Svenskarna och internet* presenteras i rapporten. Statistiken har enbart använts deskriptivt och främst för att ge en nulägesbild. Statistik över anmälda brott finns uppdelat på bedrägerityp från år 2019.

De olika källorna mäter olika saker och är behäftade med olika typer av fel. Till exempel kan vi anta att det finns ett stort mörkertal i statistiken över anmälda brott samt att mörkertalets storlek (människors anmälningsbenägenhet) varierar mellan olika typer av bedrägerier, liksom att det finns svårigheter med definitioner i frågeundersökningar.

Bilaga 2 Ordlista

Artificiell Intelligens (**AI)** ett samlingsbegrepp för datorsystem med intelligent beteende, dvs. system med kognitiva förmågor som att lära av erfarenheter, lösa nya problem, planera och generalisera.

CNP står för **card not present** och är alltså kortbedrägerier där enbart kortuppgifter används och inte det fysiska kortet.

Deep fake innebär att videor, ljud och bilder manipuleras med hjälp av teknik för att se ut att vara autentiska. Begreppet skulle kunna översättas med ingående bluff eller ingående förfalskning.

Domännamn är det som skrivs in för att komma till en webbplats, t.ex. polisen.se. Domännamn under toppdomänen .se registreras hos Internetstiftelsen. Den som har ett registrerat domännamn kan sedan lägga till subdomäner utan att registrera dessa, t.ex. kan polisen lägga till ”info” som subdomän och därmed skapa sidan info.polisen.se. På samma sätt kan den som registrerat domänen info.se lägga till ”polisen” som subdomän och därmed skapa sidan polisen.info.se.

Kryptovaluta är en virtuell valuta som fungerar oberoende av banker och nationella system och som inte är knuten till någon specifik penningenhet. Valutan används vid internetsbaserade transaktioner inom ett specifikt nätverk och handlas via en **kryptoväxel**. Varje kryptoenhet har en unik kod.

En **målvakt** är en person som syns utåt vid ett brottsupplägg. Det kan vara som innehavare av ett företag, en domän, en bil, ett telefonabonnemang, ett bankkonto och så vidare.

Nätfiske, också kallat **phishing**, är när bedragaren kontaktar potentiella brottsoffer via e-post, sms eller chattmeddelanden i syfte att få personen att klicka på en länk till en bedräglig webbplats eller ladda ner en fil med skadligt innehåll. Många bedrägerier föregås av ett dataintrång som möjliggörs genom nätfiske.

En **obehörig transaktion** är när en transaktion görs utan konto- eller kortinnehavarens samtycke. Det kan t.ex. ske genom att kort- eller kortuppgifter stjäls och används eller att bedragaren kommer in på brottsoffrets konto och antingen själv genomför transaktioner med hjälp av ett kapat bank-id eller lurar brottsoffret att godkänna transaktioner eller ge andra uppdrag till banken. En **behörig transaktion** är när brottsoffret

genomför transaktionen helt själv, t.ex. vilseleds att själv swisha eller föra över pengar.

Open-banking är ett system som innebär att andra aktörer än bankerna kan förmedla transaktioner. Det möjliggörs genom API:er som ger tredje part tillgång till bankernas information. I och med att transaktionen går genom en tredje part innebär det att den bank där kontot som pengarna skickas från inte har information om vilket det mottagande kontot är och mottagande bank på motsvarande sätt inte har information om vilken bank och vilket konto som pengarna kommer från.

En **QR-kod** är en tvådimensionell streckkod, också kallad **rutkod** eller **optisk kod**, som innehåller information (text och/eller siffror) som kan läsas av genom olika appar i mobiltelefonen eller surfplattan. **Rörlig QR-kod** är när bilden ständigt förändras för att på så sätt omöjliggöra för en bedragare att lura till sig en stillbild av en QR-kod som visas på brottsoffrets enhet.

Smishing kommer från sms-phishing och innebär bedrägeri som sker över sms. I rapporten benämns det **sms-bedrägeri** eller **social manipulation via sms**. Sms kan i likhet med e-postmeddelanden vid nätfiske innehålla länkar, men också en uppmaning att ringa upp ett specifikt telefonnummer.

Spear phishing är nätfiske riktat mot och anpassat för specifika individer eller grupper av individer.

Spoofing är när bedragaren genom att manipulera telefonnummer som visas i kontakten med potentiella brottsoffer får samtalen att se ut att komma från exempelvis en bank, polisen, en annan myndighet, ett välkänt företag, en vän eller en anhörig.

Stark kundautentisering innebär att två av följande ska finnas för att det ska räknas som en giltig identifiering: någonting man kan (t.ex. kod), någonting man har (t.ex. kort, mobiltelefon) och en unik egenskap (t.ex. fingeravtryck, ansikte). Ett annat ord som används är **tvåfaktorsautentisering**.

Virtuella plånböcker, digitala plånböcker eller e-plånböcker är online-tjänster eller applikationer för att lagra eller koppla uppgifter om pengar, medlemskort och identifikationsuppgifter. Plånboken används vid internetbaserade köp och andra digitala transaktioner.

Vishing kommer från voice phishing (röstfiske) och innebär bedrägeri som sker över telefon. I rapporten benämns det **telefonbedrägeri**.

Bilaga 3 Tabeller

I den här bilagan finns en förteckning över de åtgärder för att förebygga bedrägerier mot privatpersoner som har framkommit i den här rapporten. Förteckningen är uppdelad på åtgärder mot tekniska och strukturella sårbarheter (tabell 2) och på åtgärder med syfte att stärka potentiella brottsoffers motståndskraft (tabell 3). I tabell 4 och tabell 5 beskrivs de bedrägeriförebyggande åtgärderna kortfattat utifrån identifierade sårbarheter. Tabellerna innehåller även en bedömning av i vilken mån de förebyggande åtgärderna täcker de identifierade sårbarheterna. Samtliga tabeller bygger på de intervjuer och dokument som Brå har gått igenom och gör inte anspråk på att vara heltäckande.

Tabell 2 Förteckning över brottsförebyggande åtgärder med syfte att minska tekniska och strukturella sårbarheter.

Typ av åtgärd	Exempel på konkret åtgärd
Åtgärder mot målvakter (t.ex. som representanter för företag)	- Ekobrottsmyndighetens arbete för att det ska bli svårare att använda målvakter, inklusive samverkan med Bolagsverket angående deras kontrollmöjligheter samt utredning av missbrukade identiteter - förslag om att Bolagsverket ska få en tydligare kontrollerande roll av företrädare för företag (SOU 2023:34).
Åtgärder mot bedräglig användning av domäner och webbplatser (inklusive falska företagsannonser)	- Internetstiftelsens arbete med identifiering vid registrering av domäner, kontroll av domäner och påverkansarbete mot myndigheter att göra skyddsregistreringar - Konsumentverkets arbete mot annonser och webbutiker som inte följer gällande regler - Finansinspektionens företagsregister med företag och personer med tillstånd att erbjuda finansiella tjänster - onlineplattformarnas granskning av annonser (t.ex. Meta) - påverkansarbete (bl.a. polisens och Internetstiftelsens) gentemot centrala aktörer att inte bifoga länkar i e-post- eller sms-utskick till medborgare eller användare - påverkansarbete (bl.a. polisen) mot stora onlineplattformar och onlinesökmotorer som Meta och Google för att få dem att ta ett större ansvar mot exempelvis oseriösa annonser - införandet av EU-förordningen om en inre marknad för digitala tjänster (EU 2022/2065).
Åtgärder mot forum på darkweb	- svenska polisens deltagande i europeiska och internationella insatser mot forum på darkweb som bl.a. säljer kriminella tjänster samt stulna kort- och användaruppgifter.
Åtgärder mot falska konton, annonser och vilseledanden på digitala andrahandsmarknadsplatser	- identitetsverifiering av användarkonton (t.ex. Blocket. Tradera, Meta) - granskning av annonser (t.ex. Blocket, Tradera) - verifierade meddelandetjänster (t.ex. Blocket, Tradera) - varningar till användare när de flyttar kontakten utanför plattformen (t.ex. Blocket).
Åtgärder mot kartläggning av potentiella brottsoffer	- påverkansarbete för att det ska bli svårare att komma åt personuppgifter (bl.a. seniororganisationer).
Åtgärder mot dataintrång	- offentliga och privata aktörers arbete med att förbättra den tekniska säkerheten i sina system och tjänster

Typ av åtgärd	Exempel på konkret åtgärd
	- Microsofts arbete med att ta ner webbplatser med virus - åtgärder mot social manipulation genom sms, e-post eller sociala medier.
Åtgärder mot bedräglig användning av manipulerade telefonnummer (s.k. spoofing)	- Post- och telestyrelsen, Telekområdgivarna och telefonoperatörernas arbete med att ta fram föreskrifter, vägledningar och tekniska lösningar för att motverka bedräglig användning av manipulerade telefonnummer - manuell spärrlista med utvalda nummer som skyddas mot manipulerade telefonnummer genom att de spärras från samtal ut från numren (t.ex. bankers och vissa myndigheters växelnummer) - separata överenskommelser mellan banker och sms-tjänster för att bankernas namn inte ska kunna missbrukas.
Åtgärder mot bedrägliga banktransaktioner	- Bank-id:s lösningspaket *Säker Start* som förhindrar inloggning i internetbank på distans - Bank-id:s regler och villkor vid utfärdande av ett nytt bank-id, samt vid transaktioner i internetbanken som signeras med bank-id - förslag på en statlig e-legitimation - bankernas övervakning av banktransaktioner i syfte att identifiera misstänkta bedrägliga transaktioner - bankernas villkor och begränsningar i produktegenskaper - samverkan mellan polisen, Bankföreningen och storbankerna i syfte att förebygga bedrägerier - påverkansarbete (t.ex. polisen, Konsumentverket och seniororganisationer) mot banker i syfte att få dem att fokusera mer på säkra system och produkter - Konsumentombudsmannens arbete med att driva ärenden om bankernas ersättningsskyldighet.
Åtgärder mot bedrägliga korttransaktioner	- införandet av betaltjänstdirektivet (EU 2015/2366) som medför stark kundautentisering vid kortbetalningar inom EU - kortföretagens övervakning av korttransaktioner - påverkansarbete (t.ex. polisen) mot e-handelsaktörer för att de ska utveckla sina kontroller vid kortköp.
Åtgärder mot bedrägliga betalningar med faktura och betaltjänster	- införandet av stark kundautentisering för fakturabetalningar online (Prop.2022(23:9) - Blocket och Traderas integrerade betallösningar.
Åtgärder för att försvåra hanteringen av brottsvinster	- Polismyndighetens informationsinsatser mot potentiella möjliggörare för penningtvätt (t.ex. bil- och klockhandlare samt ungdomar) - indirekta åtgärder mot penningtvätt inklusive: - utredning och lagföring av penningmålvakter - bankernas övervakning av banktransaktioner i syfte att identifiera misstänkt penningtvätt samt åtgärder mot penningtvättare (t.ex. spärrning av konton och bank-id) - bankernas och andra verksamhetsutövares rapportering av misstänkta transaktioner till Finanspolisen - Finanspolisens arbete mot misstänkta transaktioner och penningtvätt (t.ex. sammanställning och analyser av penningtvättsregistret och stöd till verksamhetsutövare) - Polismyndighetens deltagande i europeiska insatser mot penningmålvakter - nationell samordningsfunktion mot penningtvätt och finansiering av terrorism som leds av Polismyndigheten och inkluderar sexton myndigheter och en organisation.

Tabell 3 Förteckning över brottsförebyggande åtgärder med syfte att stärka potentiella brottsoffers motståndskraft.

Typ av åtgärd	Exempel på konkret åtgärd
Medvetandehöjande åtgärder med inriktning på digital kompetens	- kampanjen *Tänk säkert* (Myndigheten för samhällsskydd och beredskap (MSB), Internetstiftelsen, Polismyndigheten (PMY), Stöldskyddsföreningen (SSF) m.fl. med artiklar, guider, webbinarier m.m.) - webbsidor med information med syfte att stärka den digitala kompetensen, bl.a. hur man kan handla säkert (t.ex. Hallå konsument, Blocket), hur man kan investera säkert (t.ex. Finansinspektionen) och hur bank-id används (t.ex. Finansiell Id-teknik, banker) - utbildningar och föreläsningar för unga (t.ex. MSB, SSF och Internetstiftelsen).
Medvetandehöjande åtgärder med inriktning på bedrägerier	- utbildningen *Försök inte lura mig* (PMY, seniororganisationer, Brottsofferjouren, UR) - Polismyndighetens lokala och regionala informationsarbete (föreläsningar för äldre, informationsblad, sociala medier m.m.) - Polismyndighetens vykort till äldre - Polismyndighetens samtalsstöd till anhöriga, *Prata med nära och kära om bedrägerier* - Sveriges bankers kampanj *Svårlurad!* - Stöldskyddsföreningens klisterlapp - seniororganisationers informationsarbete (möten, medlemstidningar, nyhetsbrev, sociala medier m.m.) - webbsidor med information om hur bedrägerier kan gå till, hur de kan förebyggas och vad man kan göra om man har utsatts (t.ex. Finansinspektionen, Konsumenternas, Microsoft).
Varningar	- varningslistor (t.ex. SSF, Finansinspektionen och Svensk Handel) - varningar för bl.a. tillvägagångssätt vid bedrägerier eller bedrägliga företag i media och sociala medier, nyhetsbrev, medlemstidningar m.m. - varningar för osäkra digitala lösningar (t.ex. webbplatser, betalningslösningar, tjänster).
Rådgivning och praktisk hjälp	- konsumentvägledningar (t.ex. Hallå konsument, kommunala konsumentvägledningar) - fysiska platser som erbjuder hjälp med digitala tjänster (t.ex. Digidelcenter) - personliga samtal (t.ex. Brottsofferjourer, privatpersoners samtal till myndigheter).

Tabell 4 Bedrägeriförebyggande åtgärder utifrån identifierade tekniska och strukturella sårbarheter, inklusive en bedömning av åtgärderna.

Sårbarheter	Pågående och planerade åtgärder	Bedömning
Öppna källor möjliggör kartläggning av potentiella brottsoffer.	påverkansarbete	Åtgärder för att begränsa publiceringen av personuppgifter behövs.
Informationsosäkerhet möjliggör dataintrång.	informationen i studiens material är	Säkerhetsarbetet för skydd mot dataintrång behöver fortsätta.

Sårbarheter	Pågående och planerade åtgärder	Bedömning
	begränsad[40], åtgärder mot manipulering av avsändare liksom mot oseriösa webbplatser och företagsmålvakter är även indirekta åtgärder mot dataintrång	
Manipulering av telefonnummer för att skapa trovärdighet.	insatser mot bedräglig manipulering av telefonnummer, s.k. ”spoofing”	Arbetet behöver tas vidare och utvecklas.
Registrering av domäner för att skapa oseriösa webbplatser och e-postkonton.	kontroll av domäner	Kontrollen behöver förbättras.
Möjligheter att publicera oseriösa privat- liksom företagsannonser.	påverkansarbete mot onlineplattformar och onlinesökmotorer, EU-förordning med högre kontrollkrav, vissa onlineplattformars kontroller av annonser, Konsumentverkets arbete mot annonser och webbutiker som inte följer regler	Kontrollen behöver utökas och förbättras.
Bedrägliga transaktioner stoppas inte.	bankernas övervakning av misstänkta transaktioner, påverkansarbete mot bankerna	Övervakningen behöver förbättras.
Snabba och ospårbara betallösningar och transaktioner.	beloppsgränser på Swish, integrerade betallösningar på digitala marknadsplatser som alternativ till Swish	Åtgärder behövs, t.ex. i form av frivilliga begränsningar, pushnotiser och varningar samt integrerade betallösningar på fler digitala marknadsplatser.
Missbruk av digital identifikation.	övervakning sker, Bank-id inför löpande nya säkerhetslösningar, förslag om en statlig e-legitimation	Förslaget om den statliga e-legitimationen behöver tas vidare och utvecklas, användningen av push-notiser och varningar kan förfinas.
Undantag från krav på stark kundautentisering.	övervakning av korttransaktioner sker, påverkansarbete mot e-handelsaktörer	Internationell samverkan behövs.
Bristande identitetskontroller på onlineplattformar m.m.	påverkansarbete mot onlineplattformar och onlinesökmotorer, EU-förordning med högre kontrollkrav, vissa onlineplattformars verifiering av användarkonton och meddelandetjänster	Kontrollen behöver förbättras.
Bristande identitetskontroller vid fysisk identifiering.	studiens material saknar information om aktuella åtgärder	Kvaliteten på identitetskontroller behöver bli bättre.
Tillgång till kompetens och utförare.	arbete med att ta bort forum på "darkweb"	Arbetet behöver fortsätta.
Tillgång till målvakter på företag, abonnemang m.m.	förslag om utökade kontroller av företag, påverkansarbete för att det ska bli svårare att använda målvakter, samverkansarbete kring missbruk av identiteter	Kontrollen av företagsföreträdare behöver utökas.

[40] Det bör dock inte tolkas som att åtgärder helt saknas utan att aktuella åtgärder bedrivs i det bredare säkerhetsarbetet och inte specifikt relaterat till bedrägerier och därför inte påtalats av studiens intervjupersoner. Se även Brå 2022b.

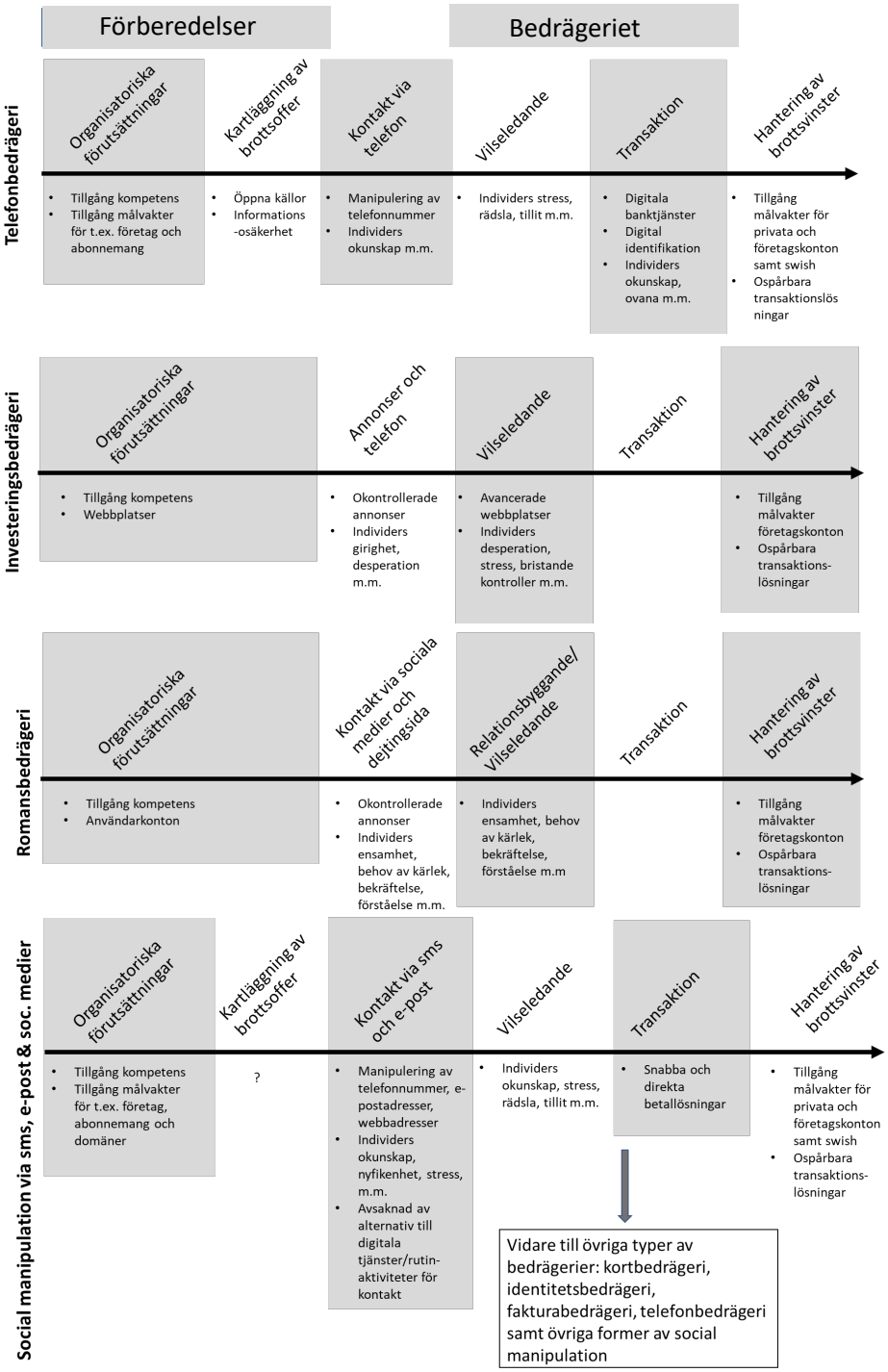
Sårbarheter	Pågående och planerade åtgärder	Bedömning
Tillgång till penningmålvakter.	sporadiska informationsinsatser, polisens, bankers och andras arbete mot penningtvätt är även indirekta åtgärder mot bedrägerier	Mer systematiska informationsinsatser behövs.
Avsaknad av alternativ till digitala tjänster.	vägledning och råd, t.ex. konsumentrådgivningar, förslag om en statlig e-legitimation	Utökat stöd vid användningen av digitala tjänster m.m. behövs.

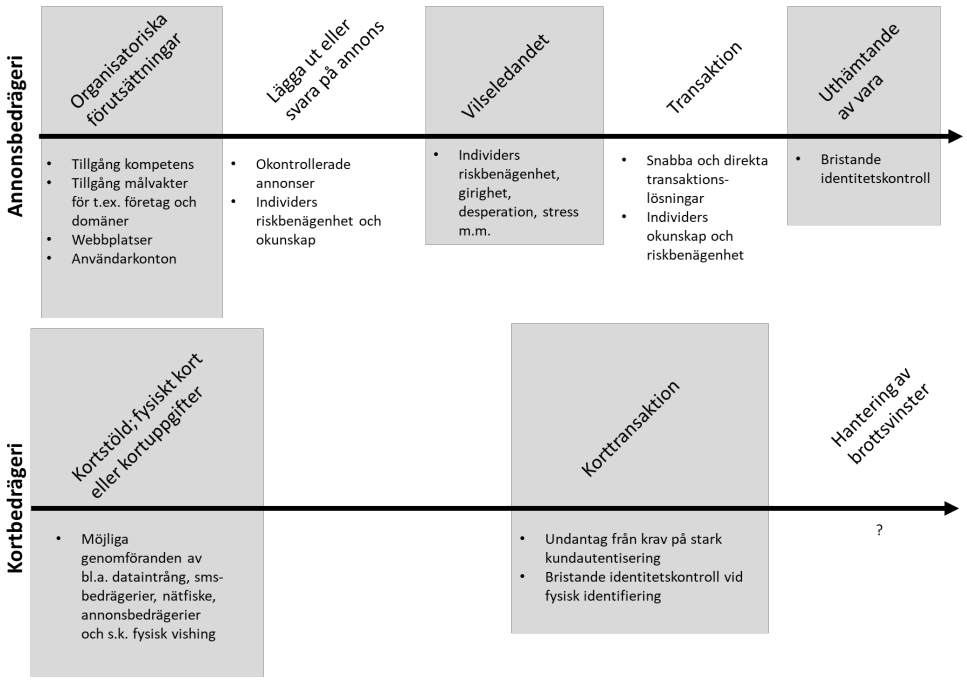
Tabell 5 Bedrägeriförebyggande åtgärder utifrån identifierade sårbarheter hos potentiella brottsoffer, inklusive en bedömning av åtgärderna.

Sårbarheter	Pågående och planerade åtgärder	Bedömning
Digital ovana och okunskap.	informationsinsatser, kampanjer och varningar med syfte att öka människors digitala kunskap och förståelse	Behov finns av mer anpassade informationsinsatser och fler praktiska inslag, liksom av utökat stöd vid användningen av digitala tjänster, förfinade pushnotiser och varningar, samt av fler uppföljningar och utvärderingar av insatser.
Okunskap om bedrägliga tillvägagångssätt.	informationsinsatser, kampanjer och varningar med syfte att göra människor mer svårlurade	Behov finns av mer anpassad information, liksom av fler uppföljningar och utvärderingar av informationsinsatser
Stress och rädsla.	indirekt medvetandehöjande åtgärder, genom att göra människor bättre rustade att hantera stressiga situationer	Behov finns av mer anpassad information med särskilt fokus på praktiska inslag, samt av fler uppföljningar och utvärderingar av informationsinsatser.
Osund tillit.	medvetandehöjande åtgärder i syfte att få människor att bli sunt kritiska	Behov finns av mer anpassad information, liksom av förfinade pushnotiser och varningar, samt av fler uppföljningar och utvärderingar av informationsinsatser.
Girighet, risktagande, nyfikenhet, bristande kontroller.	informationsinsatser och kampanjer med syfte att öka människors digitala kunskap och förståelse, vissa online-plattformars pågående åtgärder	Användningen av nudging för att puffa mot säkrare alternativ kan utökas. Användningen av pushnotiser och varningar kan utökas och förfinas. Behov finns också av mer anpassad information, samt fler uppföljningar och utvärderingar av informationsinsatser.
Ensamhet, längtan efter kärlek och förståelse.	informationsinsatser om romansbedrägerier.	Andra typer av åtgärder behövs.

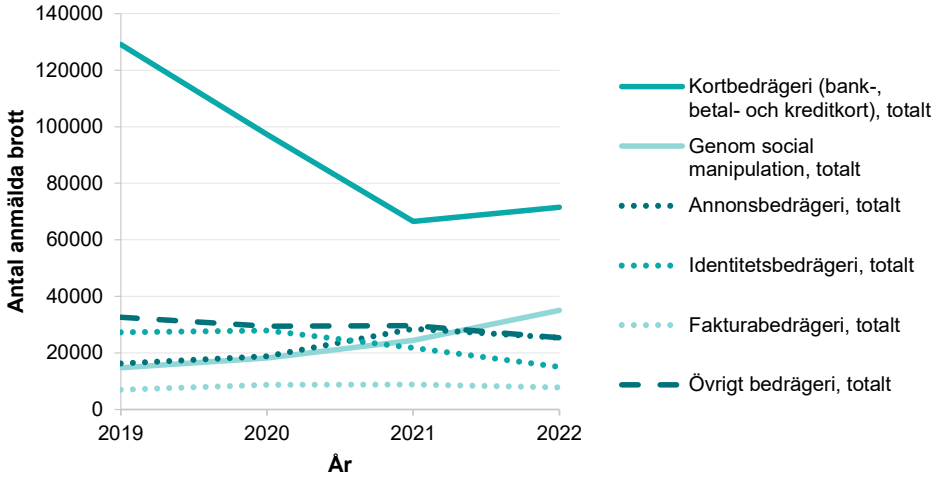
Bilaga 4 Figurer

Figur 6 Sårbarheter utifrån bedrägeriets händelsekedja uppdelat på bedrägerityp.





Figur 7 Antal anmälda bedrägeribrott uppdelat på bedrägerityp 2019–2022. Källa: Brå 2023.



Bedrägerier är ett av de vanligaste brotten, och de drabbar såväl individ som samhälle. Den omfattande och över tid ökande brottsligheten i kombination med att brotten i regel är svåra att utreda kräver att det brottsförebyggande arbetet prioriteras. Hittills har det dock inte funnits någon sammanställning av det brottsförebyggande arbetet eller vilka bedrägerier och sårbarheter åtgärderna riktar sig mot.

I den här rapporten undersöker Brå därför träffsäkerheten i de bedrägeriförebyggande åtgärderna. Rapporten bygger i första hand på intervjuer och redogör för olika tillvägagångssätt vid bedrägerier mot privatpersoner, vilka omständigheter och situationer som möjliggör brott och vilka åtgärder som görs för att förebygga bedrägerier. Brå gör även en analys av hur träffsäkra de förebyggande åtgärderna är och presenterar utvecklingsområden och rekommendationer till olika brottsförebyggande aktörer.

Rapporten vänder sig till regeringen liksom till olika aktörer som arbetar förebyggande mot bedrägerier mot privatpersoner, såsom Polismyndigheten, andra myndigheter, intresseorganisationer och företag.

Brottsförebyggande rådet/National Council for Crime Prevention

Box 1386/Tegnérgatan 23, SE-111 93 STOCKHOLM
Tel +46 (0) 8 527 58 400, info@bra.se, www.bra.se

urn:nbn:se:bra-1137