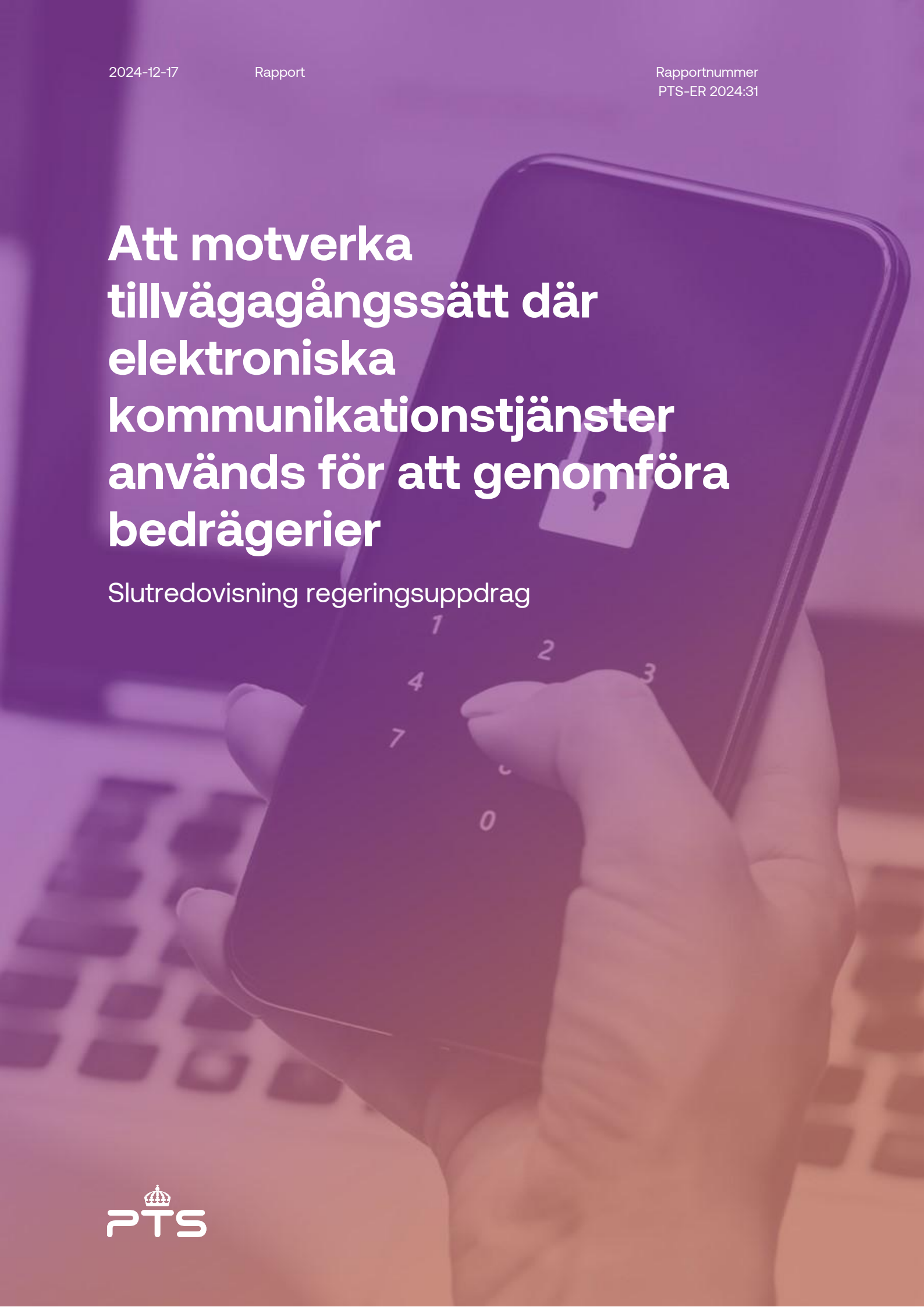
2024-12-17 Rapport

Rapportnummer
PTS-ER 2024:31

Att motverka tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier

Slutredovisning regeringsuppdrag



PTS

Klicka här för att ange text.
Klicka här för att ange text.

Rapportnummer
PTS-ER 2024:31

Diarienummer
23-31716

ISSN
1650-9862

Författare
Post- och telestyrelsen

Post- och telestyrelsen
Box 6101
102 32 Stockholm

08-678 55 00
pts@pts.se
www.pts.se

-

Innehåll

Sammanfattning

Post- och telestyrelsen (PTS) fick i december 2023 ett uppdrag från regeringen att motverka tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier.[1] PTS har kartlagt och motverkat användningen av elektroniska kommunikationstjänster vid bedrägerier, t.ex. i form av spoofing och sms-bedrägerier. Kartläggningen har bestått av informationsinhämtning från ett antal berörda aktörer, både i Sverige och internationellt. En delredovisning överlämnades i maj 2024 där delar av kartläggningen redovisades.[2]

I denna slutredovisning presenteras de åtgärder som PTS genomfört och avser att genomföra samt lämnas förslag till åtgärder för att fortsatt kunna motverka bedrägerier genom elektroniska kommunikationstjänster. Redan vidtagna åtgärder presenteras med fokus på vad PTS, operatörer och andra aktörer har gjort.

Då PTS under året har infört reglering för att motverka s.k. spoofing, som avser bedrägerier via telefonsamtal, fokuserar myndigheten främst på åtgärder som omfattar bedrägerier via sms. De åtgärder och förslag som PTS avser att arbeta vidare med är:

- Införa ett samlat och offentligt register för avsändarnamn[3]
- Etablera branschöverenskommelse alternativt vägledning med regler kring kundkännedom
- Införa samverkansforum med experter inom bedrägerier genom elektroniska kommunikationstjänster
- Analysera eventuella åtgärder beträffande nummertillstånd och s.k. Global Title

PTS analyserar i rapporten de möjliga åtgärder och förslag som myndigheten identifierat i kartläggningen. Möjliga åtgärder för sms delas upp i två områden; avsändare och innehåll.

När det gäller avsändare ser PTS att det finns problem med manipulering av avsändarnamn. Därför föreslår PTS att det inrättas ett samlat register för

[1] Fi2023/03206

[2] Delredovisning - Att motverka tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier

[3] Kallas även alfanumeriska avsändarnamn eller sender ID

avsändarnamn, som är frivilligt att anmäla sig till. I korthet innebär detta att företag m.fl. som vill skicka sms med avsändarnamn kan registrera sig. Operatörer och sms-aggregatörer måste sedan blockera alla sms med ett registrerat avsändarnamn som skickas från fel källa. Registret blir offentligt för allmänheten, som då kan se vilka företag/organisationer som är registrerade. PTS ser att en sådan lösning kan få stor effekt genom att antalet bluff-sms som skickas blir färre.

PTS har också undersökt möjligheterna för operatörer och sms-aggregatörer att filtrera sms baserat på innehållet i meddelandena. De största svenska operatörerna har alla uppgett att de redan idag i viss utsträckning filtrerar bort bedräglig sms-trafik, genom att titta på andra faktorer än just innehållet. Alla operatörer som PTS har pratat med har också framhållit behovet av tydligare reglering på detta område, så att gränserna för vad som är tillåtet tydliggörs. PTS bedömer att det i nuläget inte finns förutsättningar för att filtrera innehåll i sms med hänsyn till gällande bestämmelser om integritet och behandling av personuppgifter.

PTS ser att en branschöverenskommelse där berörda aktörer kommer överens om regler gällande kundkännedom är ett bra komplement till ovan beskrivna åtgärder. Genom kundkännedom kan företagen försvåra att den egna verksamheten utnyttjas för bedrägerier. Ett alternativ till branschöverenskommelse är att PTS ger ut en vägledning till sms-aggregatörer och operatörer gällande kundkännedom.

Utöver dessa åtgärder ser PTS att det finns ett behov av effektiv samverkan mellan myndigheter och andra aktörer som har expertis inom olika områden som rör bedrägerier. Detta är särskilt viktigt eftersom bedragarna är snabbrörliga och ofta tekniskt kunniga och snabbt byter tillvägagångssätt för bedrägeriförsöken. PTS avser därför att införa och driva ett samverkansforum för experter med kunskaper om bedrägerier genom elektroniska kommunikationstjänster. En mer effektiv samverkan kommer att bidra till att bygga upp gemensam kunskap om bedragarens tillvägagångssätt, att snabbare kunna motverka dessa samt att nå ut med samordnad information till allmänheten.

Slutligen utreder PTS vidare möjligheter att vidta åtgärder gällande användning av nummer samt Global Title, vilket har påverkan på förutsättningarna för bedragaren att på olika sätt utnyttja nummer för att genomföra bedrägerier.

PTS har även gjort en översyn av möjligheterna att ställa krav på e-post och andra OTT-tjänster, liknande de krav som föreslås för sms. PTS granskning visar dock att regleringen kring dessa tjänster är svårgenomtränglig och bedragare är svåra att komma åt. Här ser PTS att befintliga regler som t.ex. Digital Services Act, DSA, kan ha effekt. DSA-förordningen har till syfte att motverka olaglig och skadlig verksamhet på internet och att begränsa spridningen av desinformation.

1. Inledning

Regeringen gav i december 2023 PTS i uppdrag att motverka tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier.[4] En delredovisning överlämnades i maj 2024 där valda delar av uppdraget redovisades.[5]

1.1 PTS arbete med regeringsuppdraget

PTS har kartlagt användningen av elektroniska kommunikationstjänster vid bedrägerier, t.ex. i form av spoofing och sms-bedrägerier. Detta har gjorts genom insamling av information från bl.a. Polismyndigheten och BRÅ, genom egna enkätundersökningar och ett stort antal möten med olika aktörer på marknaden och med organisationer som företräder slutanvändare.[6] En genomgång av några utvalda länders erfarenheter av reglering inom området har gjorts genom en mindre komparativ studie av dessa länders sätt att hantera problemen, samt genom frågor till och kontakter med ansvariga regleringsmyndigheter. PTS har även verkat för informationsspridning genom att bl.a. medverka i olika forum som t.ex. Digitala Varningsgruppen och föreläsning via Digitalidag i samarbete med pensionärsföreningar i Tyresö om myndighetens uppdrag och arbete för att motverka bedrägerier.

1.2 Bedrägeriernas omfattning

Den ökade digitaliseringen av samhället och den ökade globaliseringen har bidragit till att bedrägerier där elektroniska kommunikationstjänster används har ökat kraftigt under senare tid. Den ekonomiska brottsligheten är ett allvarligt samhällsproblem och vinsterna från bedrägeribrotten används ofta för att finansiera annan kriminalitet. Enligt Polismyndigheten[7] uppgick brottsvinsterna från vishing-bedrägerier år 2023 till 708 miljoner kronor, vilket var en ökning med 13 procent från året innan. I Polismyndighetens underlag räknas både bedrägerier via samtal och sms in i vishing-

[4] Fi2023/03206.

[5] Delredovisning - Att motverka tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier.

[6] Polismyndigheten, Konsumentverket, Svenska Bankföreningen, Tech Sverige, Brå, Telia Company, Tele2, Telenor, Leissner Data, Hi3G, Internetstiftelsen, Telekområdgivarna, Sinch, SKPF Pensionärerna, Finansinspektionen, Google, Meta, Digitala Varningsgruppen.

[7] Polismyndigheten, *Brottsvinsterna för bedrägeribrottsligheten 2023*, 2024-04-15, Dnr A233.272/2024.

begreppet. Polismyndigheten har publicerat ny statistik för 2024 över brottsvinster från bedrägerier genom vishing. Siffrorna indikerar en starkt nedåtgående trend med en minskning av brottsvinster med 43 procent mellan januari till september, jämfört med samma period förra året.[8]

Det är svårt att exakt utreda vem det är som drabbas av bedrägerier genom t.ex. bedrägliga telefonsamtal eller bluff-sms. PTS har i kartläggningen bl.a. använt Polismyndighetens rapporter gällande brottsvinster[9], Svenskt Näringslivs rapport gällande brottslighetens kostnader för näringslivet[10] och Brottsförebyggande rådets rapport gällande bedrägerier mot privatpersoner[11]. Vishingbedrägerier drabbar både företag och privatpersoner. Svenskt Näringslivs rapport visar att kostnaderna för det svenska näringslivet till följd av alla slags bedrägerier beräknas till 4,5 miljarder SEK. Polismyndighetens siffror gällande brottsvinster baseras på anmälda brott, medan Svenskt Näringslivs siffror baseras på uppskattade kostnader, baserat på anmälda och oanmälda brott. Svenskt näringsliv anger att 41 procent av företagare inte anmäler något brott, medan 22 procent anger att de anmäler vissa brott. Polismyndigheten uppger att bedrägerier genom elektroniska kommunikationstjänster slår hårt framför allt mot äldre personer[12]. Bedrägerierna påverkar brottsoffren både ekonomiskt och psykiskt, oavsett ålder. Många förlorar sparkapital och drabbas av minskad tilltro till den digitala utvecklingen.

Kartläggningen visar avslutningsvis att alla åtgärder som försvårar för bedragaren, både stora och små, är positiva och PTS påbörjar därför arbetet med de åtgärder som är möjliga omgående.

2. PTS förslag och kommande åtgärder

I detta avsnitt presenteras kortfattat de förslag samt kommande åtgärder som PTS avser att eller rekommenderar att gå vidare med i närtid. I avsnitt 5 presenteras en mer ingående analys av de möjliga åtgärder som PTS har undersökt i uppdraget.

[8] https://polisen.se/aktuellt/nyheter/nationell/2024/oktober/bedragerierna-minskar/ [Hämtat 2024-12-06]
[9] Polismyndigheten, *Brottsvinsterna för bedrägeribrottsligheten 2023*, 2024-04-15, Dnr A233.272/2024.
[10] Nitz, Lena. Svenskt Näringsliv (2023). *Brottslighetens kostnader 2023*
[11] Brå, (2023). *Bedrägerier mot privatpersoner De förebyggande åtgärdernas träffsäkerhet*, Rapport 2023:11
[12] Polismyndigheten. (2024). PM 2024-07-03. Svar till PTS.

2.1 Införa ett frivilligt register för avsändarnamn

Åtgärd: PTS anser att det bör införas ett samlat register för avsändarnamn. Registret ska användas för att bolag och organisationer ska kunna skydda sina avsändarnamn från obehörig användning. Registreringen ska vara frivillig. Registret ska vara offentligt så att slutanvändare kan se vilka bolag och organisationer som är anslutna. Operatörer och sms-aggregatörer ska blockera sms med registrerade avsändarnamn som skickas från fel avsändare. Sms från oregistrerade avsändarnamn ska skickas fram utan åtgärd.

Motiv för åtgärden: I dagsläget finns en marknadsdriven lösning för skydd av avsändarnamn. PTS anser att ett offentligt register, administrerat av PTS, är ett effektivt sätt att minska antalet bedrägerier som sker med sms. PTS föreslår att registrering av avsändarnamn ska vara frivilligt för bolag och organisationer. De bolag och organisationer som väljer att registrera sitt avsändarnamn kommer då att kunna skydda det från obehörig användning. En fördel med ett offentligt register är att mottagarna av sms enkelt kan ta reda på vilka bolag som registrerat sig då registret är tillgängligt för alla att ta del av. Enligt PTS uppskattning kan frivillig registrering av avsändarnamn minska förekomsten av sms-bedrägerier i betydande grad. Förslaget kommer sannolikt att leda till att allmänhetens förtroende för sms ökar, vilket även är till nytta för de företag som använder sig av tjänsten.

Förutsättningar: En förutsättning för att ett samlat register för avsändarnamn ska få avsedd effekt är att PTS ges ett utökat bemyndigande. Detta kan göras genom att en ny lagbestämmelse införs i 9 kap lagen (2022:482) om elektronisk kommunikation, LEK, liknande den som idag finns för talkommunikationstjänster i 9 kap. 6 § LEK. Genom den nya bestämmelsen bör PTS ges bemyndigande att utfärda föreskrifter om krav som ska ställas på en *textkommunikationstjänst* som medger identifiering av avsändaren av meddelandet. PTS kan med ett sådant bemyndigande t.ex. föreskriva att operatörer och sms-aggregatörer ska blockera meddelanden från registrerade avsändarnamn som används felaktigt. Föreskrifter kan också innehålla detaljer kring registreringen av avsändarnamn, t.ex. vilka namn som får registreras och utformningen av registrerade namn (tecken som inte får användas etc.). Ett register kan administreras av PTS eller av en av PTS utsedd aktör. I likhet med lösningar i andra EU-länder bör även utländska företag tillåtas att registrera ett avsändarnamn i Sverige.

Ett alternativ till ny bestämmelse i 9 kap. är att nuvarande 4 kap. 11 § LEK ändras till en skrivning som är närmare ordalydelsen i artikel 97.2 i kodexen,[13] samtidigt som PTS ges bemyndigande att utfärda föreskrifter om i vilka fall operatörer får blockera sms utan föregående beslut från myndighet i varje enskilt fall. Detta skulle enligt PTS

[13] Direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation

bedömning göra det tydligare för såväl användare som operatörer i vilka fall det är tillåtet att blockera meddelanden. Oavsett alternativ till ny bestämmelse är tydligare regler på området något som också efterfrågas av operatörerna.

Kostnader: Det kommer att uppstå kostnader för att upprätta och administrera ett samlat register. Om PTS ska hantera ett sådant register kommer en avgift att behöva tas ut av de företag som väljer att registrera sitt avsändarnamn. Kostnader uppstår också för sms-aggregatörer och operatörer, inledningsvis för att implementera en teknisk lösning för kontrollen av avsändarnamn och senare för att upprätthålla denna funktion. Dessa kostnader bör bäras av kunderna. Det kan också bli aktuellt med informationskampanjer till allmänheten kring detta, vilket medför kostnader.

Finansiering: PTS föreslår att kostnaderna för att administrera ett samlat register för avsändarnamn, samt för tillsyn i anslutning till detta, finansieras av avgifter.

2.2 Etablera regler om kundkännedom

Åtgärd: PTS planerar att medverka till att en branschöverenskommelse om kundkännedom skapas, som operatörer och sms-aggregatörer bör använda i sin verksamhet. Ett alternativ är att PTS tar fram en vägledning med motsvarande innehåll.

Motiv för åtgärden: Att känna sina kunder är grundläggande i en affärsrelation. Genom kundkännedom kan företagen försvåra att den egna verksamheten utnyttjas för bedrägerier. A2P-sms kan passera flera olika sms-aggregatörer och därefter en operatör innan de når mottagaren och det är därför viktigt att kundkännedom finns i alla de led som ett sms passerar. Fördelen med en branschöverenskommelse är att de parter som ingår en sådan förbinder sig att följa reglerna och förhoppningsvis kan den utvecklas till att bilda ”praxis” som operatörer och sms-aggregatörer följer. Ytterligare en fördel med en branschöverenskommelse är att riktlinjerna i den kommer att fungera på den aktuella marknaden, eftersom den kommer att ha etablerats av berörda aktörer. Effekten av denna åtgärd förväntas bli ett ökat förtroende för sms med anledning av att bedrägliga verksamheter kan upptäckas och hindras från att skicka A2P-sms i ett tidigt skede. Arbetet med en branschöverenskommelse kommer att påbörjas av PTS snarast.

Förutsättningar: En branschöverenskommelse kräver att operatörer och sms-aggregatörer kommer överens om vilka regler som ska gälla. PTS kan facilitera detta arbete. En vägledning kan PTS ta fram på egen hand efter avstämningar med operatörer och sms-aggregatörer.

Kostnader: Vid både en branschöverenskommelse och en vägledning uppstår kostnader för operatörer och sms-aggregatörer att ta fram, implementera och följa de regler som etableras. Det går inte att uppskatta kostnaderna då PTS inte vet vilka regler som kommer att sättas upp. PTS bedömning är dock att flertalet av aktörerna redan idag arbetar med någon form av kundkännedom. Kostnader uppstår även för PTS om myndigheten ska utarbeta en vägledning.

Finansiering: Kostnader för PTS bedöms rymmas inom befintlig ram. Kostnader för att ta fram och upprätthålla överenskommelsen kommer även att uppstå för deltagande aktörer.

2.3 Införa ett samverkansforum

Åtgärd: PTS avser att införa ett samverkansforum med experter med kunskaper om bedrägerier. PTS leder och samordnar forumet och bjuder in relevanta deltagare.

Motiv till åtgärden: Inom branschen finns specialistkunskap om bedrägerier, men från olika infallsvinklar. PTS bedömer att det kommer att det krävs aktiv samverkan och utbyte av denna kunskap mellan PTS och andra berörda aktörer för att hantera problemet med bedrägerier genom elektroniska kommunikationstjänster effektivt. Samverkan med berörda aktörer kommer att startas upp omgående.

Förutsättningar: Alla förutsättningar finns för att upprätta ett samverkansforum.

Kostnader: Administrativa kostnader uppstår för PTS att driva samverkansforum. Vissa kostnader tillkommer också för de aktörer som deltar i forumet.

Finansiering: PTS bedömer att kostnader för att driva samverkansforum kan finansieras inom befintlig ram.

2.4 Nummertillstånd och Global Title

Åtgärd: PTS avser att se över användning och behov av eventuell reglering av nummertillstånd på grossistnivå och användning av s.k. Global Title. Syftet är att öka myndighetens kunskaper, identifiera och vidta lämpliga åtgärder för att motverka de problem som kan uppstå i dessa sammanhang.

Motiv till åtgärden: PTS har under det senaste året noterat att svenska nummer, i större utsträckning, börjat förekomma i samband med bedrägerier där ovanstående två företeelser utgör en del. Andra länder har också sett liknande problem, och likt Sverige börjat agera i frågan.

Förutsättningar: PTS har redan påbörjat arbetet och det kommer att fortsätta under 2025.

Kostnader: En analys av konsekvenser för genomförande och eventuell påverkan på marknaden har ännu inte gjorts, men kommer göras inom ramen för det fortsatta arbetet.

Finansiering: För 2025 ryms kostnader för åtgärden inom myndighetens befintliga avgiftsram för nummertillstånd.

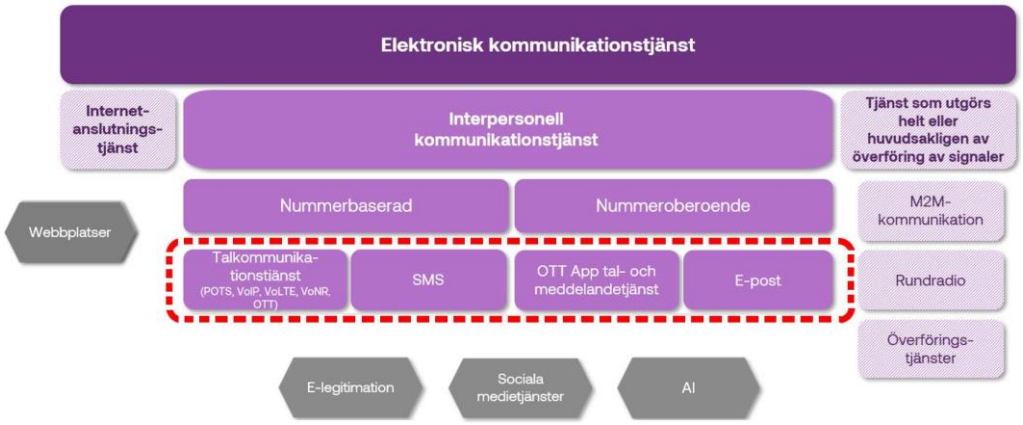
3. Bedrägerier genom elektroniska kommunikationstjänster

Elektronisk kommunikation är ett brett område. Erfarenheter, både från Sverige och andra länder, visar att bedragare ändrar tillvägagångssätt i takt med att åtgärder mot bedrägerierna införs. Flera operatörer uppger att det finns en osäkerhet kring vilka regler som kommer att gälla i de olika länder de verkar i, vilket medför att de i vissa fall inte vet vad de ska eller kan göra för att försöka förhindra bedrägerierna. Hårdare regler i ett land kan också innebära att en del av brottsligheten istället riktar sig mot något annat land. Därför är det viktigt att Sverige vidtar liknande åtgärder som andra EU-länder.

Bedrägerierna leder till att de drabbade skadas både ekonomiskt och psykiskt. Samhällskada består bl.a. i risken för minskad tilltro till samhällets institutioner och system med bl.a. ökat utanförskap som följd men även i stora brottsvinster till de kriminella.[14] I många av fallen riskerar även förtroendet för elektroniska kommunikationstjänster som t.ex. sms att minska. Det är viktigt att dessa tjänster uppfattas och är säkra att använda för att meddela sig med.

I detta avsnitt beskrivs problemen med bedrägerier genom elektroniska kommunikationstjänster samt andra närliggande metoder som bidrar till problemen. I bilden nedan illustreras elektroniska kommunikationstjänster och de avgränsningar som PTS har valt att göra, se streckade rödmarkerade områden i bilden nedan. PTS har fokuserat på de delområden där kartläggningen visat att de största problemen med bedrägerier finns för tillfället, d.v.s. på spoofing och sms-bedrägerier.

[14] BRÅ rapport 2023:11, *Bedrägerier mot privatpersoner*, s. 65



Figur 1 - PTS avgränsning av elektroniska kommunikationstjänster i detta uppdrag inom röd streckad markering. Tjänster som inte utgör elektroniska kommunikationstjänster indikeras genom sexkantiga figurer.

3.1 Talkommunikation

Bedrägeriförsök med hjälp av talkommunikation kan göras på olika sätt. En metod är att använda s.k. spoofing. Vid spoofing manipuleras det nummer som vid inkommande samtal visas i telefonen, så att samtalet ser ut att komma från någon annan än det faktiskt gör, t.ex. från en bank eller annan som den uppringda känner till. Även om samtalet egentligen görs från utlandet kan det genom spoofing se ut som det är ett svenskt telefonnummer som ringer mottagaren. De nummer som används behöver inte nödvändigtvis vara ett svenskt telefonnummer som är tilldelat en operatör. Det förekommer också att bedragare använder telefonnummer som inte är tilldelade en operatör, eller att de lägger till eller tar bort en siffra i ett befintligt telefonnummer (vilket i hastigheten kan se ut att stämma överens med t.ex. din banks nummer).

En annan metod är wangirisamtal[15], som innebär att den som ringer upp lägger på efter bara en signal. Syftet är att få den som blivit uppringd att ringa tillbaka. Numret som ringer är ofta ett högkostnadsnummer (främst internationella telefonnummer) vilket gör det dyrt att ringa tillbaka.

3.2 Sms

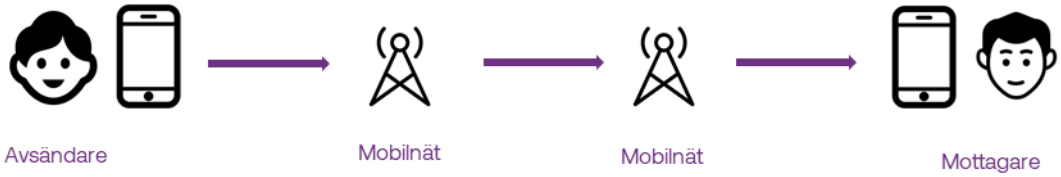
Det finns ett brett användningsområde för sms och många som vill skicka och ta emot denna typ av meddelanden. Det är viktigt för avsändaren och mottagaren, men

[15] Wangiri är ett japanskt uttryck som ungefär innebär “one (ring) and cut.” - https://www.europol.europa.eu/sites/default/files/documents/wangiri_final_2.pdf [Hämtad 2024-11-27]

även för tillhandahållare av tjänsterna och samhället i stort, att kunden har förtroende för tjänsten. Sms är en tjänst som inte går att välja bort om man har en mobiltelefon, vilket medför att höga krav måste ställas på att tjänsten inte används för bedrägerier.

Det finns två olika typer av sms;

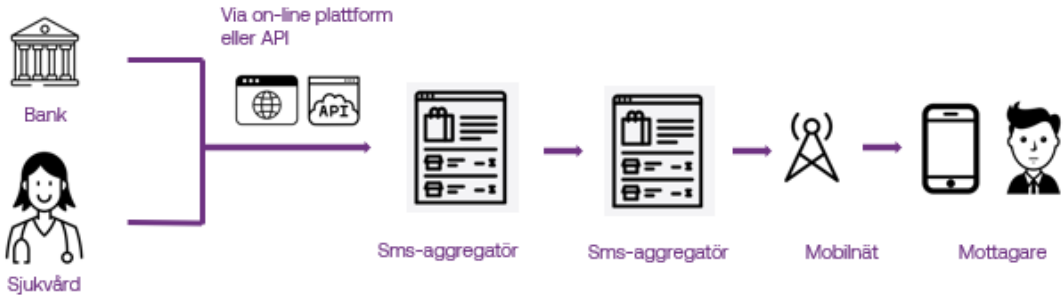
Person-till-person (P2P) sms innebär att meddelandet sänds från en mobiltelefon till en annan inom eller mellan operatörers nät. Detta är meddelanden som vanligen skickas mellan privatpersoner.



Figur 2 - Beskrivning av vägen för P2P-sms från avsändare till mottagare.

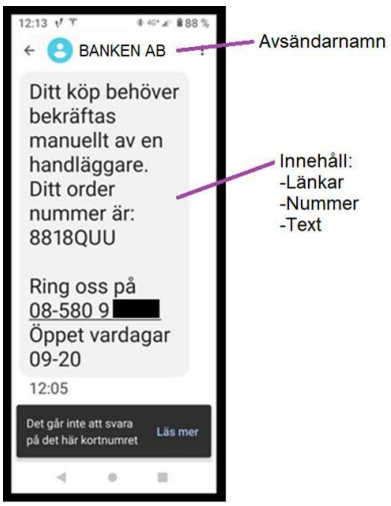
Applikation-till-person (A2P) sms innebär att meddelanden skickas via en online-plattform eller ett API[16] via en eller flera sms-aggregatörer till operatörens mobilnät för att nå en mottagare. En sms-aggregatör är ett företag som agerar mellanhand mellan den som vill skicka ut A2P-sms och mobiloperatören. Det finns olika typer av sms-aggregatörer där några har direkt kontakt med nätägande operatörer och andra inte. Mobiloperatörerna har ofta avtal med flera sms-aggregatörer. A2P-sms gör det möjligt för en avsändare att nå ett stort antal mottagare för t.ex. information eller reklamutskick som t.ex. påminnelser om läkarbesök, kunderbjudanden, information om bokade resor eller tvåfaktorsautenticering vid t.ex. köp och beställningar. För att göra ett sådant utskick krävs att avsändaren förmedlar meddelandena via en sms-aggregatör. PTS har noterat i kartläggningen att möjligheten att skicka stora mängder A2P-sms för att nå många mottagare ofta utnyttjas av bedragare.

[16] Application programming interface - Ett API kan beskrivas som en bro mellan exempelvis två system och är ett kontrollerat sätt att överföra data fram och tillbaka mellan programvaror på ett formaliserat sätt.



Figur 3 - Beskrivning av A2P-sms.

Det skickas årligen drygt 7,6 miljarder P2P-sms och drygt 5,8 miljarder A2P-sms. Av de förstnämnda är drygt 6 miljarder sms mellan privatpersoner och knappt 1,6 miljarder är sms från företag.[17] Både vid skickande av P2P- och A2P-sms består sms:et av två delar, en adressdel och en innehållsdel, se bild nedan. När en eller båda delarna innehåller falsk information kallas sms:en för bluff-sms.



Figur 4 – Exempel på ett bluff-sms. Avsändare kan stå antingen som ett telefonnummer eller som ett avsändarnamn. Innehållet i sms:et kan t.ex. innehålla ett telefonnummer som mottagaren uppmanas att ringa till eller länkar som går till falska webbplatser som kan vara mycket lika de äkta webbplatserna.

[17] https://statistik.pts.se/telekom-och-bredband/svensk-telekommarknad/tabeller/mobila-samtals-och-datatjanster/tabell-16-sms/

3.2.1 **Avsändarnamn**

Ett avsändarnamn är ett annat sätt att ange avsändaren av ett A2P-sms, istället för telefonnummer som används inom P2P-sms. Ett avsändarnamn kan bestå av max 11 tecken. Många företag använder detta vid utskick av A2P-sms, för att kunden lätt ska kunna identifiera avsändaren. En vanlig metod vid sms-bedrägerier är att bedragaren, i likhet med spoofing av telefonnummer, förfalskar avsändarnamnet så att det ser ut som att sms:et kommer från någon annan än det faktiskt gör.

Idag finns ingen reglering i Sverige kring hur avsändarnamn får användas. Detta har lett till att bedragare använder t.ex. bankers och andra kända företagsnamn som avsändare, i syfte att lura mottagaren. Bluff-sms med förfalskade avsändarnamn kan vara extra svåra att särskilja från riktiga sms från samma avsändarnamn, eftersom telefonen ofta sorterar in bluff-sms:et i samma meddelandetråd som tidigare mottagna sms från den riktiga avsändaren. Detta innebär att om mottagaren tidigare har fått ett riktigt sms från avsändarnamn BANKEN AB, så kommer ett bluff-sms från avsändarnamn BANKEN AB hamna i samma meddelandetråd i telefonen.

3.2.2 **Innehåll**

Förfalskade avsändarnamn används ofta tillsammans med länkar i sms:et, vilka leder till bedrägliga webbplatser. Det handlar ofta om att någon t.ex. utger sig för att vara din bank i ett sms, med länk till en bedräglig webbplats. Efter att ett sådant bluff-sms har skickats kan bedragaren ibland även ringa upp mottagaren. Det förekommer även ofta att bluff-sms innehåller ett telefonnummer som mottagaren uppmanas att ringa till. PTS har sett i kartläggningen att operatörerna har tekniska förutsättningar för att filtrera innehåll i sms för att kunna blockera meddelanden med skadligt innehåll.

3.3 Övriga meddelandetjänster

OTT-tjänster[18] har definierats av Berec[19] som ”*content, a service or an application that is provided to the end user over the public Internet*”. Till skillnad från sms som är en nätbaserad tjänst och använder mobilnätet för att skicka meddelanden, så skickar OTT-tjänster meddelanden via internet. Exempel på vanligt förekommande OTT-tjänster är Gmail, Messenger, Linkedin:s chattfunktion och WhatsApp. Dessa tjänster kräver att användaren installerar en specifik app på sin telefon för att kunna använda dem. Apple´s iMessage har liknande funktioner som andra OTT-tjänster men

[18] OTT – Over the top

[19] The Body of European Regulators for Electronic Communications, eller Organet för europeiska regleringsmyndigheter för elektronisk kommunikation. Berecs uppdrag är att bistå kommissionen och de nationella tillsynsmyndigheterna i genomförandet av EU:s telekomregler. Den ger också råd till EU-institutionerna och kompletterar de nationella myndigheternas tillsynsuppgifter på EU-nivå.

fungerar endast mellan Apple-enheter. iMessage kräver dock ingen särskild app utan är ”inbyggd” i telefonens standardapp för meddelanden. Användaren måste dock aktivt aktivera tjänsten i sin telefon och både avsändare och mottagare måste vara anslutna till tjänsten, i annat fall skickas meddelandet som sms eller mms.

RCS (Rich Commuication Services) är en tjänst som började utvecklas redan 2007, som en tänkt ersättare till sms. RCS ger möjlighet till funktioner som gruppchattar och fildelning likt funktioner i OTT-tjänster. Detta skiljer sig från sms som inte har den funktionaliteten. Flera operatörer har stöd för RCS, men slutanvändarens telefon och dess operativsystem måste också ha funktionen implementerad. I likhet med iMessage krävs ingen särskild app för RCS utan funktionen är inbyggd i telefonens standardapp för meddelanden. För att RCS ska kunna användas behöver både avsändare och mottagare vara anslutna till tjänsten, i annat fall skickas meddelandet som sms eller mms. RCS-meddelanden fungerar både på Android- och iOS-enheter.

Bedrägeriförsök är vanligt förekommande även i dessa tjänster och mycket talar för att problemet kommer att öka i takt med hårdare reglering av t.ex. spoofade röstsamtal och bluff-sms. Tillhandahållare av OTT-tjänster gör redan vissa insatser för att motverka bedrägerier. Många har kundtjänstfunktioner där användare kan anmäla misstänkta meddelanden och falsk reklam.

OTT-tjänster är, till skillnad från sms, något som kunden själv väljer att ha. Detta gör att användarna själva kan minska riskerna genom att välja bort användning. I många andra länder är dock användningen av OTT-tjänster vanligare än i Sverige och många företag utomlands nås enklast genom sådana tjänster. I dessa fall blir kunden tvungen att använda tjänsten för att kunna få kontakt med t.ex. företagets kundtjänst.

PTS har i denna rapport inga specifika förslag på hur OTT-tjänster skulle kunna regleras särskilt i Sverige för att minska risken för bedrägerier, men myndigheten följer utvecklingen på området, både nationellt och internationellt och ser över behov att agera i framtiden.

3.3.1 EU:s förordning om en inre marknad för digitala tjänster

Digital Services Act (DSA-förordningen)[20] gäller fullt ut sedan den 17 februari 2024. Den kompletterande nationella lagstiftningen[21] trädde ikraft den 1 december 2024. Huvudsyftet med DSA-förordningen är att motverka olaglig och skadlig verksamhet på internet samt att begränsa spridningen av desinformation. Den ska bidra till att öka säkerheten för användarna, upprätthålla skyddet för grundläggande rättigheter och

[20] Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG

[21] Lagen (2024:954) med kompletterande bestämmelser till EU:s förordning om digitala tjänster

främja rättvisa och transparenta förhållanden för internetplattformar. PTS är nationell samordnare för reglerna och ska tillsammans med Konsumentverket och Mediemyndigheten ansvara för tillsyn och kontroll av efterlevnaden av reglerna i Sverige.[22]

DSA-förordningen reglerar så kallade förmedlingstjänster och internetplattformar, som till exempel marknadsplatser, sociala medier, plattformar för delning av innehåll, app-butiker och plattformar för att boka resor och boende. Mycket stora plattformar eller sökmotorer med mer än 45 miljoner användare i EU kommer att ha striktare regler och särskilda skyldigheter. Det är EU- kommissionen som identifierar vilka plattformar som är mycket stora. Förordningen syftar även till att klargöra processen för överklaganden, främja transparens och underlätta informationsutbyte mellan medlemsstaterna.

För privatpersoner innebär reglerna bl.a. förbättrat skydd av grundläggande rättigheter, ökat utbud och ökad kontroll, förstärkt skydd av barn på internet och minskad risk för exponering för olaglig verksamhet. För leverantörer av digitala tjänster innebär reglerna ökad rättslig trygghet och enhetliga regler inom hela EU. För samhället som helhet innebär reglerna bl.a. ökad demokratisk kontroll och överblick över systemviktiga plattformar samt färre systemrisker som manipulation och desinformation. Även om DSA inte är specifikt avsett för att motverka bedrägerier ser PTS att regleringen kommer att kunna ha inverkan på denna typ av brottslighet.

3.4 E-post

Trots att det idag finns möjligheter att minska problemen genom filtrering förekommer det fortfarande bedrägeriförsök via e-post. Bedragarna använder samma metoder som för bluff-sms; massutskick till ett stort antal mottagare, falska avsändare som ser ut att vara en bank eller annan känd organisation, skadliga länkar i meddelandet o.s.v. Genom att öppna filer som bifogas ett meddelande kan du luras att ladda ner kod och programvara som skadar din dator eller smarttelefon. Den ger angriparen möjlighet att ta kontroll över din dator eller smarttelefon, logga dina tangenttryckningar eller få tillgång till känslig information som dina kortuppgifter, lösenord eller annan personlig information.[23]

[22] Se t.ex. på PTS webbplats https://pts.se/internet-och-telefoni/dsa-forordningen---regler-om-digitala-tjanster-for-en-sakrare-onlinemiljo/ [Hämtad 2024-12-06] och hos Mediemyndigheten: https://mediemyndigheten.se/ansokan-och-registrering/regelverk/dsa--eus-forordning-om-en-inre-marknad-for-digitala-tjanster/ [Hämtad 2024-12-06].

[23] Se t.ex. https://www.msb.se/sv/rad-till-privatpersoner/digital-sakerhet/natfiske-och-skadlig-kod/ [Hämtad 2024-12-06].

Metoden ovan kan även användas i kombination med s.k. teknisk support-bedrägeri. I dessa fall utger sig bedragaren för att vara en expert som kan hjälpa kunden med diverse problem med dator eller telefon, t.ex. virus.

De flesta e-postprogram som förekommer på marknaden tillåter idag någon form av kontroll och filtrering av meddelanden. Genom att kunden godkänner användarvillkoren för tjänsten kan tillhandahållaren filtrera meddelanden och markera meddelanden med misstänkt skadligt innehåll som ”skräppost”. I detta syfte använder tillhandahållarna av tjänsten redan idag artificiell intelligens (AI). Systemen lär sig känna igen t.ex. avsändare och skadliga länkar bl.a. genom vad användarna själva markerar som skräp.

PTS ser att det finns ett visst skydd idag för att motverka bedrägerier genom e-post och har därför valt att fokusera på andra områden. Myndigheten följer utvecklingen på området, både nationellt och internationellt och ser över behov att agera i framtiden.

3.5 Andra metoder som används vid bedrägerier genom elektroniska kommunikationstjänster

3.5.1 Bedrägliga webbplatser och säker surf

Många bedrägerier sker genom att användare själva, aktivt eller av misstag, söker upp webbplatser som utger sig för att vara t.ex. en webbutik men som i själva verket är uppbyggda för att lura användare. Falska webbplatser används främst för att lura användare på personliga uppgifter som lösenord, koder och kortuppgifter. De kan också användas för att få användare att ladda hem spionprogram och annan skadlig kod. Bedrägerier via falska webbplatser omsätter miljontals svenska kronor varje år.[24] Många aktörer i samhället gör insatser för att utbilda användare om hur de undviker falska annonser och falska webbplatser. Det finns även tjänster på marknaden som tillhandahålls av operatörer för att skydda sina kunder.

3.5.2 Artificiell intelligens i samband med bedrägerier

Intresset för AI har ökat kraftigt under de senaste åren och den kan användas både för att bekämpa och genomföra bedrägerier. Till exempel finns s.k. deepfakes, där AI genererar realistiska falska bilder, ljud och videor. De kan användas vid bedrägeriförsök för att komma över koder och pengar. AI kan även användas för att genomföra s.k. phishing-attacker, där bedragaren försöker lura personer att avslöja

[24] Se Internetstiftelsen: https://internetkunskap.se/snabbkurser/falska-sajter-och-annonser/skydda-dig-mot-falska-webbsidor/ [Hämtad 2024-12-06].

känslig information genom att imitera pålitliga källor. Utöver detta kan algoritmer analyseras och optimeras för att förenkla bedrägerier och förfalskningar på ett sätt som gör dem svåra att upptäcka. I PTS kartläggning har det framkommit att bedrägeriförsök där AI används förekommer i Sverige.

AI kan även användas som ett verktyg för att motverka bedrägerier. Genom att analysera stora mängder data kan AI-system identifiera mönster som tyder på bedrägeri, till exempel genom att spåra ovanliga finansiella transaktioner eller upptäcka avvikelser i användarbeteende vid elektronisk kommunikation. Tekniken kan även användas för att upptäcka och verifiera identiteter, t.ex. genom ansiktsigenkänning och biometriska data, vilket gör det svårare för bedragaren att använda stulna identiteter och genomföra bedrägerier.

För att effektivt motverka AI-baserade bedrägerier krävs en balanserad strategi som kombinerar tekniska lösningar, dataskydd samt informationsinsatser med juridiska och etiska ramverk, t.ex. AI-förordningen[25], Dataförvaltningsförordningen[26] och Dataakten[27]. Samarbete mellan myndigheter, industri och forskningsinstitutioner är avgörande för att utveckla hållbara lösningar som skyddar samhället utan att kompromissa med individens rättigheter.

[25] Europaparlamentets och Rådets förordning (EU) 2024/1689 av den 13 juni 2024 om harmoniserade regler för artificiell intelligens.
[26] Europaparlamentets och Rådets förordning (EU) 2022/868 av den 30 maj 2022 om europeisk dataförvaltning.
[27] Europaparlamentets och Rådets förordning (EU) 2023/2854 av den 13 december 2023 om harmoniserade regler för skälig åtkomst till och användning av data.

4. Genomförda åtgärder och initiativ

Flera åtgärder har redan vidtagits av både myndigheter och privata aktörer under de senaste åren inom området elektronisk kommunikation för att motverka bedrägerier. Utöver de nedan beskriva åtgärderna finns också en rad initiativ från marknaden som t.ex. erbjuder skydd via applikationer i telefonen genom att visa vem som ringer. I detta avsnitt presenteras de åtgärder som PTS och andra aktörer redan har genomfört.

Åtgärd	Genomförd av	Effekt
Spoofing – föreskrifter och allmänna råd	PTS	Blockerade samtal (ca 40-50 000 per dygn)
Kontantkortsregistrering	PTS genomför tillsyn	Går inte längre att använda oregistrerade kontantkort
Internationella samarbeten	PTS	Avgörande för att kunna påverka där besluten fattas
Digital inkludering	PTS	Ökad kunskap om digitalisering hos slutanvändare
Registrering av avsändarnamn	Sms-aggregatörer och operatörer	Skyddar registrerade avsändarnamn
7726	Operatörer	Används för statistik
Blockering av Wangirisamtal	Operatörer	Blockerar stor andel av Wangirisamtal
Blockerande filter för webbplatser	Operatörer	Bedrägliga webbplatser blockeras alternativt får användaren en varning
Blockerande för sms och andra meddelandetjänster	Operatörer, sms-aggregatörer och OTT-leverantörer	Bluff-sms och andra typer av meddelanden blockeras eller flyttas till skräppost
Blockeringsverktyg med hjälp av spärrlista	Operatörer	Operatörer blockerar samtal som kommer från nummer som finns med på spärrlistan

Tabell 1 – Sammanställning av genomförda åtgärder

4.1 Genomförda åtgärder av PTS

4.1.1 Talkommunikation – föreskrifter och allmänna råd

En stor del av bedrägeriförsöken genomförs med hjälp av telefonsamtal med spoofade nummer. Den allra största delen av sådana samtal kommer, enligt uppgifter från de svenska operatörerna, från utlandet. PTS publicerade i november 2023 en vägledning, som togs fram i samarbete med operatörer och Telekområdgivarna.

Vägledningen innehåller rekommendationer om hantering av samtal med svenska telefonnummer som kommer in till Sverige från utlandet via ett internationellt samtrafikgränssnitt.

Flera operatörer följer rekommendationerna och spärrar nu en stor mängd samtal med svenska fasta nummer som kommer in till Sverige från utlandet. Någon operatör har också börjat göra s.k. roamingkontroller av samtal från operatörens egna mobiltelefonikunder och spärrar samtal som kommer in från utlandet om kunden inte befinner sig utomlands. Inledningsvis blockerades upp till 50 000 samtal per dag. Telia uppskattar att åtgärden leder till att de blockerar ca tre miljoner samtal per månad.

I september 2024 beslutade PTS om föreskrifter och allmänna råd för att förhindra samtal med manipulerade anropande telefonnummer (PTSFS 2024:2). Föreskrifterna bygger i stor utsträckning på vägledningen. Huvudprincipen för föreskrifterna är att svenska telefonnummer ska användas i Sverige. Det innebär att samtal med svenska telefonnummer som kommer in till Sverige via ett internationellt samtrafikgränssnitt ska spärras, så att de inte kopplas fram. Vid samtal inom Sverige ska dessutom den tillhandahållaren där samtalet startar (originerande tillhandahållaren) kontrollera att det uppringande numret är tilldelat någon tillhandahållare för användning innan samtalet kopplas fram. När det gäller telefonnummer för mobiltelefonitjänster, mobila telematiktjänster[28] och mobila bredbandstjänster ska en kontroll först ske för att se om den svenska abonnenten roamar i ett annat land, och om så är fallet kan samtalet kopplas fram.

Föreskrifterna trädde i kraft den 4 november 2024 för fasta nummer. Den del av föreskrifterna och det allmänna råd som gäller kontroll av mobilsamtal som roamar från en utländsk operatörs nät träder i kraft den 3 mars 2025. Det senare datumet beror på att operatörerna behöver tid för att implementera en teknisk lösning. Först efter att alla delar av föreskrifterna har trätt i kraft kan vi se full effekt av åtgärden. PTS utgår ifrån att ännu fler samtal kommer att stoppas när föreskrifterna och allmänna råd har trätt i kraft fullt ut.

4.1.2 **Kontantkortsregistrering**

Den 1 augusti 2022 trädde reglerna om registrering av abonnentuppgifter vid tillhandahållande av förbetalda allmänt tillgängliga nummerbaserade interpersonella kommunikationstjänster eller förbetalda internetanslutningstjänster (kontantkort) i kraft. Reglerna innebär att det inte längre är möjligt att ringa eller surfa med oregistrerade och anonyma kontantkort. Den som tillhandahåller en förbetald tjänst

[28] Nummer för mobila telematiktjänster används för t.ex. maskin-till-maskinkommunikation (även kallat M2M).

ska enligt reglerna registrera uppgifter om abonnenten och kontrollera abonnentens identitet innan tjänsten aktiveras.

Reglerna infördes eftersom det innan augusti 2022 var vanligt förekommande att oregistrerade och anonyma kontantkort till mobiltelefoner användes i samband med brottslig verksamhet. Kommunikation genom anonyma kontantkort innebär att brottsbekämpande myndigheter går miste om viktig och ibland avgörande information i sin brottsutredande verksamhet. I syfte att underlätta för brottsbekämpande myndigheter och försvåra för kriminella infördes därför reglerna om registrering av kontantkort i 9 kap. 24 – 26 §§ LEK.

Ett annat tillvägagångssätt för bedragare är att använda sig av s.k. sim-farmar för att kunna skicka ut bluff-sms till ett stort antal slutanvändare genom att använda många sim-kort. Det har i dessa sammanhang varit vanligt förekommande att bedragarna använt oregistrerade sim-kort. Genom de nya reglerna om registrering av kontantkort har detta förfarande försvårats.

PTS har tillsynsansvar för efterlevnaden av bestämmelserna om registrering av kontantkort. PTS har genomfört en tillsyn av samtliga operatörer som tillhandahåller kontantkort på den svenska marknaden. Alla tillsynsärenden förutom ett är nu avslutade. Det är dock för tidigt att uttala sig om vilka eventuella effekter tillsynen kan haft.

4.1.3 PTS deltagande i internationella samarbeten

Inom CEPT ECC WG NaN[29] pågår arbete med att ta fram en rekommendation med syfte att ge vägledning till medlemsstaterna kring hantering av avsändarnamn för att förhindra att avsändarnamnen förfalskas. Innehållet i rekommendationen kommer bland annat beröra upprättande av ett register för avsändarnamn, kriterier för vilka tecken ett avsändarnamn bör/inte bör innehålla och hur operatören ska hantera dessa vid framkoppling. Rekommendationen beräknas bli klar under första kvartalet 2025. Gruppen har tidigare tagit fram rekommendationer bl.a. kring åtgärder för att motverka bedrägerier med manipulerade telefonnummer[30].

Nyligen bildades den globala arbetsgruppen Global Informal Regulatory Antifraud Forum (GIRAF) som har initierats av i3Forum[31]. GIRAF är öppet för alla nationella

[29] CEPT (European Conference of Postal and Telecommunications Administrations) är en organisation som samlar regleringsmyndigheter inom post- och telekomsektorn I Europa. Inom CEPT finns ECC (Electronic Communication Committee), som i sin tur är indelat i ett antal arbetsgrupper, bl.a. Working Group NaN2

[30] ECC Recommendation (23)03 - Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers; https://docdb.cept.org/document/28602 [Hämtad 2024-12-04].

[31] i3Forum är en ideell branschorganisation som jobbar med att möjliggöra och påskynda förändringar över det internationella kommunikationsekosystemet

tillsynsmyndigheter och arbetar för att underlätta globalt samarbete och gemensamma lösningar för att bekämpa oönskade/bedrägliga samtal och meddelanden på en global nivå. Vid en förfrågan till 24 europeiska länder om de vidtagit åtgärder mot spoofade telefonnummer svarade 17 länder att de hade implementerat någon typ av åtgärd.

EU:s cybersäkerhetsbyrå ENISA har angett att de har för avsikt att utforma en övergripande teknisk kartläggning över t.ex. åtgärder mot bluff-sms, åtgärder för ökad säkerhet i signalering, åtgärder för ökad säkerhet i informationsteknologisystem, mjukvara och paket. ENISA har inte tidigare genomfört en sådan studie. ENISA:s expertgrupp inom elektronisk kommunikation ECASEC[32] har som första steg skickat några inledande frågor till medlemsstaterna för en sådan smishingstudie.

I förslaget till BERECs Work Programme 2025[33] planeras en workshop[34] om bedrägerier genom felaktigt användande av telefonnummer att hållas. Här nämns även att det finns planer på att i samarbete med ECASEC, ta fram riktlinjer för att motverka smishing.

4.1.4 **Digital inkludering**

PTS har genom sitt arbete med digitalisering sett vilka utmaningar vissa användare möter när de ska använda digitala tjänster och arbetar för att minska dessa. Utmaningarna för både äldre och de med funktionsnedsättningar är många gånger delvis desamma. Trots att skydd mot bedrägerier implementeras på teknisk väg är det mycket viktigt att öka den digitala kunskapsnivån. Myndigheten arbetar med ett antal olika uppdrag och initiativ inom detta område.

4.1.4.1 PTS regeringsuppdrag om att öka förutsättningarna för digital inkludering

I PTS uppdrag om att öka förutsättningarna för digital inkludering (Fi2024/00172) har behovet av bättre information om cybersäkerhet för allmänheten identifierats. Den utbredda oron för bedrägerier dämpar viljan att använda digitala tjänster, vilket riskerar att minska tilliten och därmed hämma de samhällsvinster som digitaliseringen

[32] The European Competent Authorities for Secure Electronic Communications (ECASEC) group fungerar som en plattform inom ENISA för samarbete och utbyte av information mellan de nationella myndigheter som övervakar telekomsäkerheten i Europa

[33] https://www.berec.europa.eu/system/files/2024-10/BoR%20%2824%29%20148%20Draft%20BEREC%20Work%20Programme%202025.pdf [Hämtad 2024-12-06].

[34] BEREC external Workshop & Summary Report on practical issues preventing number misuse and possible fraudulent activities as a result of impact of new technologies.

kan erbjuda. Genom att öka kunskapen om trygg och säker internetanvändning kan förtroendet för digitala tjänster stärkas.

I uppdraget, som ska slutredovisas senast den 21 december, ingår att lämna förslag för att öka den digitala inkluderingen och användningen av digitala tjänster.

4.1.4.2 Digitalidag

Digitalidag är en samverkansplattform där aktörer från privat- och offentlig sektor samt företrädare för civilsamhället samarbetar. Från och med januari 2024 är samverkansplattformen Digitalidag en del av PTS. Tillsammans arbetar aktörerna för att alla ska kunna ta del av digitaliseringens möjligheter, oavsett förmåga eller förutsättningar. Bred samverkan är nyckeln för att Sverige ska lyckas inspirera fler människor till att vilja och kunna vara en del av den digitala utvecklingen.

En gång om året arrangeras temadagen Digitalidag, då görs en stor gemensam kraftsamling där digitaliseringens möjligheter och utmaningar sätts högst upp på agendan. Aktiviteter sker runt om i hela landet. Temadagen 2023 bjöd på ett rekordstort engagemang och totalt deltog 375 aktörer som tillsammans arrangerade 1 000 aktiviteter i 216 kommuner. Över 10 000 personer engagerade sig för att inspirera fler människor till att vilja och kunna vara en del av den digitala utvecklingen. Under temadagen i november 2024 deltog 385 aktörer som tillsammans arrangerade över 500 aktiviteter runt om i landet. Uppskattningsvis har 978 511 personer fått någon form av kompetensutvecklingsinsats.

4.1.4.3 Kartläggning svenskarna med funktionsnedsättning och internet

PTS arbetar för att tjänster, teknik och kommunikation ska vara inkluderande och bidra till att alla ska kunna vara delaktiga i det digitala samhället, oavsett förmågor och förutsättningar. PTS bidrar till exempel med finansiering till arbetet med att ta fram rapporten *Svenskarna med funktionsnedsättning och internet*[35] som tas fram vartannat år av Begripsam[36] i samarbete med Centrum för klinisk forskning Region Dalarna[37]

Ett genomgående drag i resultatet av undersökningen 2023 är att deltagarna är oroade över hur användningen av nätet har starkt negativa sidor. Det finns en ökad risk att råka ut för brottsliga handlingar och att skydda sig från dessa upplevs som svårt. Att hela tiden behöva oroa sig för det ständiga bakgrundsbruset av en pågående och ökande kriminalitet skapar negativa känslor som rädsla, oro, trötthet,

[35] https://www.begripsam.se/forskning/internet/2023-rapporter-och-resultat [Hämtad 2024-12-06].
[36] https://www.begripsam.se/.
[37] Svenskarna med funktionsnedsättning och internet 2023, s 8 och 9.

uppgivenhet. Det leder också till konkreta förändringar i beteende. Man kanske drar ner på sin närvaro i sociala medier, avstår från att exponera sina kontaktuppgifter eller avstår från att använda olika tjänster.[38] Undersökningen 2023 var första gången det ställdes specifika frågor om trygghet och säkerhet på nätet. Resultatet indikerar att personer med funktionsnedsättning i högre grad verkar vara mer utsatta för allvarlig brottslighet på nätet jämfört med personer utan funktionsnedsättning. Som exempel på allvarlig brottslighet har det i undersökningen ställts frågor om att ha blivit lurad på pengar, och blivit vilseledd att göra saker. Fler personer med funktionsnedsättning uppger till exempel att de fått sina lösenord kapade jämfört med personer som inte har någon funktionsnedsättning.[39]

Att personer med funktionsnedsättning i högre grad verkar riskera att bli utsatta för allvarlig brottslighet på nätet blottlägger ett allvarligt samhällsproblem. Nätets skyddsmekanismer förefaller för dåligt utformade och för personer med funktionsnedsättning är skyddet inte tillräckligt. Det kan bero på att ansvaret för att skydda sig för brottslighet i för hög utsträckning har blivit ett individuellt ansvar och att de tekniska och strukturella skydden inte i sig är tillgängliga och användbara för den som har en funktionsnedsättning. Störst risk för att råka ut för brottslighet och övergrepp på nätet finns hos personer med intellektuella svårigheter och hos personer som har svårt med språket men det tycks finnas en förhöjd risk hos alla grupper, utom hos personer som är blinda och som har grav synnedsättning. Det kommer att ges ut en separat rapport med en fördjupad analys som handlar om trygghet och säkerhet.[40]

4.1.4.4 PTS webbplats

För att nå ut till allmänheten och till aktörerna på marknaden har PTS information om telefonbedrägerier på myndighetens webbplats www.pts.se, som riktar sig till både allmänheten och berörda aktörer.[41] Där förklaras vad telefonbedrägerier innebär, men allmänheten kan också ta del av information om tillvägagångssättet för de vanligast förekommande telefonbedrägerierna samt information om hur man som slutanvändare kan skydda sig. För operatörerna finns även information om föreskrifter och vad som är på gång inom PTS.

[38] Svenskarna med funktionsnedsättning och internet s 8
[39] Svenskarna med funktionsnedsättning och internet s 9
[40] Svenskarna med funktionsnedsättning och internet s 9
[41] https://pts.se/internet-och-telefoni/sakerhet-och-skydd-av-uppgifter/telefonbedragerier/ [Hämtad 2024-12-06].

4.2 Genomförda åtgärder av operatörer och andra aktörer

4.2.1 Registrering av avsändarnamn

Ett antal aktörer på marknaden, däribland de nätägande mobiloperatörerna och ett antal sms-aggregatörer, har tagit fram en lösning som kallas *SMS Sender ID protection*. Lösningen lanserades i slutet av 2023 och går ut på att företag som använder sms-utskick till sina kunder, kan registrera sitt avsändarnamn hos den eller de sms-aggregatörer som hanterar sms-utskick åt företaget. Efter denna registrering underrättas operatörerna som därefter kan spärra sms med detta avsändarnamn om det inte kommer från rätt avsändare.

Denna åtgärd har haft inverkan på antalet bedrägerier med falska avsändarnamn och visar på marknadens potential att identifiera och lösa problem som drabbar slutkunderna. Hittills är det är ett fåtal företag, främst banker och logistikföretag, som har registrerat sitt användarnamn. En nackdel med denna lösning är att det inte finns någon möjlighet för slutkunderna att kontrollera om ett sms kommer från ett anslutet företag. Eftersom de företag som använder möjligheten att registrera sitt användarnamn är stora aktörer med många kunder har det dock sannolikt fört med sig väldigt stor samhällsnytta, då bedrägerier som involverar dem kan resultera i stora summor som förloras för privatpersoner eller företag. PTS har gjort bedömningen att ca tre procent av företagen som använder A2P-sms har registrerat sitt användarnamn.

4.2.2 Sms-kortnummer 7726

Sedan ungefär ett år tillbaka finns det möjlighet att anmäla misstänkta bluff-sms genom att vidarebefordra dem till numret 7726. Numret bildar ordet SPAM på knappsatsen och liknande lösningar finns också i bl.a. Storbritannien och i USA. Tanken med initiativet är att enkelt kunna ta emot anmälningar om misstänkta bluff-sms och på så sätt motverka förekomsten av dessa. Genom 7726 kan mottagaren av ett misstänkt bluff-sms vidarebefordra det till sin mobiloperatör. Operatörerna kan därefter dela informationen med varandra och agera samtidigt på misstänkta bluff-sms. Tidigare har operatörerna haft egna sms-kortnummer dit kunderna har kunnat göra anmälningar men den nya lösningen ger operatörerna bättre information och möjlighet att agera snabbare.

4.2.3 Spärr mot Wangirisamtal

Förekomsten av wangirisamtal till slutanvändare har minskat kraftigt under senare tid, eftersom operatörerna har tagit fram egna lösningar för att motverka problemet. Genom att operatörerna analyserar trafiken och identifierar de telefonnummer

(främst internationella) som används vid wangirisamtal kan trafik till och från dessa nummer automatiskt blockeras under en tid.

4.2.4 Blockerande filter för webbplatser

På marknaden finns tjänster som innebär att misstänkta webbplatser blockeras eller förses med en varningstext om att webbplatsen man vill besöka kan innehålla virus, bedrägeriförsök eller andra skadliga programvaror som kan försöka stjäla personlig information. Flera operatörer erbjuder t.ex. den här typen av tjänster till sina kunder.

4.2.5 Blockerande filter för sms och andra meddelandetjänster

Både operatörer, sms-aggregatörer och tillhandahållare av OTT-tjänster använder idag olika blockerande filter. Både iMessage och RCS-meddelanden har en skräppost i likhet med e-post. Filtreringen kan baseras på t.ex. trafikmönster och avsändare.

4.2.6 Blockeringsverktyg med hjälp av en spärrlista

Under 2018 inleddes ett arbete i regi av Telekområdgivarna, där även PTS deltog, som ledde fram till ett ”blockeringsverktyg”. Blockeringsverktyget är en form av spärrlista[42] över telefonnummer som aldrig används för att ringa ifrån. Blockeringsverktyget har främst använts av banker som har kunnat anmäla telefonnummer (t.ex. deras kundtjänstnummer) som de aldrig använder för att ringa ifrån. Om operatörerna får in ett samtal från ett nummer som är listat på spärrlistan så blockerar de det samtalet.

[42] Spärrlista (eng. deny list) kallas ibland också för DNO-lista. (Do Not Originate). Motsatsen till en spärrlista är en frilista (eng. allow list). Nummer som finns i en frilista släpps igenom utan kontroll.

5. Analys av möjliga åtgärder

I detta avsnitt presenteras och analyseras de möjliga åtgärder som PTS har undersökt i uppdraget.

5.1 Sms

PTS har identifierat två områden där åtgärder kan vidtas för att motverka sms-bedrägerier; avsändare och innehåll. Nedan beskrivs olika möjliga åtgärder samt vilka förutsättningar som finns och vilka konsekvenser som genomförande av åtgärderna medför.

5.1.1 **Avsändare**

Merparten av de bluff-sms som skickas idag är A2P-sms. Användningen av A2P-sms gör det möjligt för en avsändare att nå ett stort antal mottagare för t.ex. information eller reklamutskick. För att göra ett sådant utskick krävs att avsändaren förmedlar meddelandena via en sms-aggregatör. PTS har undersökt hur andra länder, inom och utanför EU, har hanterat problemet med bluff-sms.

De åtgärder avseende kontroll av avsändare som PTS har övervägt listas nedan.

5.1.1.1 *Obligatorisk registrering av avsändarnamn*

Ett sätt att stoppa bluff-sms är att ställa krav på att avsändarnamn ska registreras för att få användas. Detta skulle innebära att ett registrerat avsändarnamn bara kan användas av den registrerade användaren och ett förbud mot att använda ett avsändarnamn som inte är registrerat. Registreringen kombineras med information om vilken sms-aggregatör som avsändaren ifråga använder sig av. Ett meddelande som skickas på ett annat sätt än via registrerad sms-aggregatör ska blockeras och inte skickas fram till mottagaren. Registret skulle kunna administreras av PTS eller en av PTS utpekad administratör.

Oregistrerade avsändarnamn skulle kunna hanteras på olika sätt,

a) genom att helt blockera meddelandet,
b) genom att anonymisera (ta bort avsändarnamnet i rubriken) eller
c) genom att skicka fram sms:et till slutkunden med någon form av varning.

Med lösning b eller c får mottagaren själv göra bedömningen om meddelandet är säkert eller ej. PTS anser att alternativ c är tryggare för mottagaren jämfört med alternativ b, eftersom meddelandet då kommer med en uttalad varning. Som exempel på alternativ c kan nämnas Singapore, som har infört en form av obligatorisk registrering av avsändarnamn. Där krävs inte att meddelanden från oregistrerade avsändare stoppas, men sådana meddelanden måste markeras med texten ”Likely SCAM” som avsändare.[43]

I valet av hur sms från oregistrerade avsändare ska hanteras vid obligatorisk registrering finns flera aspekter att ta hänsyn till. En regel om att oregistrerade avsändare ska blockeras kan få konsekvenser t.ex. för turister i Sverige som inte skulle kunna ta emot sms från utlandet (t.ex. från ett utländskt flygbolag som inte är registrerat i Sverige och som skickar sms om t.ex. uppdaterade flygtider). Obligatorisk registrering är något som de flesta aktörer på marknaden avråder från. Deras kunder efterfrågar enklare lösningar och risken finns att dessa kunder börjar använda sig av s.k. sim-farmar för att skicka P2P-sms istället för A2P-sms.

PTS ser att en lösning med obligatorisk registrering av användarnamn skulle kunna bidra till stor samhällsekonomisk nytta. I Storbritannien, där frågan utreds, uppges att åtgärden kan stoppa 25 procent av sms-bedrägerier, och i Singapore, där en variant av obligatorisk registrering införts, uppges att åtgärden stoppar ca 70 procent av bedrägerier med bluff-sms. Vid införande av en liknande åtgärd i Sverige bedömer PTS att ca 100 miljoner SEK av brottsvinsterna från vishing-bedrägerier skulle kunna stoppas, baserat på Polismyndighetens statistik om brottsvinster för 2023. Därtill stoppas även en stor mängd lidande för brottsoffren som utsätts för den här typen av bedrägerier som troligtvis är större än enbart värdet av de stoppade brottsvinsterna.

Obligatorisk registrering skulle medföra kostnader för administration för företagen som tvingas registrera sig, för sms-aggregatörer och för operatörer, samt för den som ska sätta upp och förvalta registret. Som jämförelse kan nämnas Singapore, där en engångskostnad tas ut för registreringen om S$ 500 och en årlig avgift om S$ 200. Under antagande att kostnader är liknande i Sverige kan vi se en engångskostnad på ca 4 000 SEK per företag och en årlig kostnad på ca 1 600 SEK.

[43] https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/regulations/consultations/2022/proposals-to-strengthen-safeguards-for-sms-messages-to-singapore-users/full-ssir-regime/imda-decision-on-full-ssir-regime.pdf [Hämtad 2024-12-06].

5.1.1.2 *Frivillig registrering av avsändarnamn*

Ett alternativ till kravet att alla användare av avsändarnamn måste registrera sig är en frivillig lösning, liknande den som tillämpas i Finland.[44] En frivillig registrering bygger på samma slags registrering som i alternativet obligatorisk registrering. En lista över registrerade avsändare hålls publicerad av den som administrerar registret så att alla som vill kan ta del av den. För att få effekt bör alla företag som förmedlar sms-trafik få meddelande från registret när en registrering har gjorts.

Skillnaden jämfört med obligatorisk registrering är att avsändare som valt att inte registrera sitt avsändarnamn kan fortsätta skicka sms utan att det kontrolleras om avsändaren är den rätta. Registrerade användarnamn från fel avsändare blockeras helt medan meddelanden från oregistrerade användarnamn skickas till mottagaren. Jämfört med alternativet obligatorisk registrering kommer frivillig registrering alltså endast att skydda registrerade användarnamn.

En fördel med frivillig registrering är att många små aktörer, enligt uppgifter från bl.a. operatörerna, anser att registrering är krångligt och dyrt. Obligatorisk registrering skulle kunna innebära att företag söker sig till andra kanaler för information till sina kunder. En nackdel med frivillig registrering är dock att mottagare av sms måste göra en egen kontroll av om avsändaren är registrerad eller ej.

Kostnaden för frivillig registrering skulle sannolikt vara lägre än för obligatorisk. Företagen skulle själva kunna välja registrering om de anser att fördelarna överväger kostnaderna.

I Finland rekommenderar Traficom (PTS motsvarighet) alla som skickar sms med avsändarnamn till medborgare att skydda sina avsändarnamn genom att anmäla sig till ett nationellt register som administreras av Traficom. Registrerade avsändarnamn publiceras i en lista som finns tillgänglig på Traficoms webbplats. Alla företag som förmedlar sms-trafik i Finland får meddelande när en registrering har gjorts. Antalet frivilligt registrerade företag och organisationer i Finland uppgår i november 2024 till 211 stycken. För registreringen av avsändarnamn tar Traficom ut en ansökningsavgift om 60 euro och en årlig avgift om 200 euro. Traficom har noterat att det skett en minskning av de ekonomiska förlusterna till följd av bedrägerier sedan registreringen infördes.

På Irland har ComReg (PTS motsvarighet) infört möjlighet för företag att registrera sitt avsändarnamn hos ComReg. Registreringen kombineras med information om vilken sms-aggregatör som avsändaren ifråga använder sig av. Operatörerna kan därefter

[44] https://www.traficom.fi/sv/vara-tjanster/ansok-om-sms-sender-id-kortmeddelande-tjanster [Hämtad 2024-12-06]

blockera sms som skickas med ett registrerat avsändarnamn från fel sms-aggregatör.

5.1.1.3 *Förbjuda användning av avsändarnamn*

Det mest drastiska sättet att förhindra falska avsändarnamn är att helt förbjuda att avsändarnamn används. Det skulle rent praktiskt innebära att inga sådana sms får levereras till slutanvändarna/mottagarna av sms:et. I stort sett alla länder inom EU tillåter användning av avsändarnamn och det är positivt för mottagarna att direkt kunna se vem som är avsändaren. För företag och organisationer är det mycket värdefullt att på detta sätt snabbt och enkelt kunna nå sina kunder. Enligt uppgifter från branschen läses 90 procent av alla mottagna sms inom 3 minuter.

5.1.1.4 Bedömning och val av åtgärd

PTS bedömning är att stor del av de effekter som kan uppstå med en obligatorisk registrering av avsändarnamn även kan realiseras med en registrering på frivillig basis till ett samlat register. Åtgärden är genomförbar och PTS avser att påbörja arbetet med implementering av åtgärden så snart de rättsliga förutsättningarna finns på plats. I avsnittet nedan presenteras de rättsliga förutsättningar som finns för att genomföra åtgärden. PTS kommer även fortsättningsvis att bevaka frågan inom arbetsgruppen CEPT ECC WG NaN.

5.1.1.5 Rättsligt stöd för reglering av avsändarnamn

(a) 4 kap. LEK: Hantera avsändarnamn med stöd av bestämmelser om nummer

I prop. 2002/03:110 s. 157 anför regeringen bl.a. att ett nummer kan vara ett namn eller en adress, men det utmärkande är att det utgörs av siffror. Detta talar, enligt PTS mening, för att avsändarnamn inte är avsedda att omfattas. Å andra sidan för regeringen också ett resonemang kring att kännetecknande för ett namn är att det används för att identifiera en slutanvändare eller en tjänst, t.ex. en webbadress eller en e-postadress, men det kan alltså även vara ett vanligt telefonnummer. Regeringen uttalar i propositionen att Sverige inte ensidigt bör låsa sig vid definitioner som kan komma att förändras med kort varsel.

Givet den utveckling som har skett inom området för elektroniska kommunikationer, och regeringens resonemang ovan, gör PTS bedömningen att även avsändarnamn för sms ryms inom begreppet nummer i LEK:s mening. En sådan tolkning medför dock andra problem då bestämmelserna om nummer i 4:e kapitlet LEK i övrigt är dåligt anpassade för avsändarnamn och den lösning kring frivillig registrering som PTS föreslår ovan. Enligt 4 kap. 3 § LEK får ett nummer inte användas utan tillstånd. Om den bestämmelsen, utan några förändringar, skulle utökas till att omfatta

avsändarnamn skulle det krävas obligatorisk registrering för användning av avsändarnamn, samt att meddelanden med oregistrerade avsändarnamn måste blockeras.

Ett alternativ till att söka stöd i befintliga bestämmelser om nummer är att en ändring görs i 4 kap. 11 § LEK så att den bättre överensstämmer med artikel 97.2 i kodexen. 4 kap. 11 § infördes i gamla LEK genom prop. 2010/11:115 (dåvarande 7 kap. 9 a §) och fördes över oförändrad till nya LEK. PTS skulle samtidigt kunna ges bemyndigande att utfärda föreskrifter om i vilka fall operatörer får blockera sms utan föregående beslut från myndighet i varje enskilt fall. Detta skulle t.ex. kunna gälla för sms med användarnamn som skickas från någon annan än den registrerade avsändaren.

(b) 9 kap. LEK: Krav på identifiering av avsändare

PTS har i delredovisningen av uppdraget gjort bedömningen att det idag saknas stöd i 9 kap. LEK för att ställa samma krav på sms som på röstsamtal vad gäller identifiering av avsändare. Bestämmelsen i 9 kap. 6 § LEK grundas på artikel 8 i e-Privacydirektivet[45]. Ett sätt att lösa problemet med bedrägliga avsändare är att ändra i 9 kap. LEK.

Genom att en ny lagbestämmelse införs i 9 kap LEK, liknande den som idag finns för talkommunikationstjänster i 9 kap. 6 § LEK, kan PTS ges bemyndigande att utfärda föreskrifter om krav som ska ställas på en *textkommunikationstjänst* som medger identifiering av avsändaren av meddelandet. PTS kan med ett sådant bemyndigande t.ex. föreskriva att operatörerna ska blockera meddelanden från registrerade avsändarnamn som används felaktigt. Föreskrifter kan också innehålla detaljer kring registreringen av avsändarnamn, t.ex. vilka namn som får registreras och utformningen av registrerade namn (tecken som inte får användas etc.).

5.1.1.6 Rättsligt stöd för att blockera meddelanden

En förutsättning för att ett samlat register för avsändarnamn ska få avsedd effekt är att det är tydligt att operatörerna får och ska blockera meddelanden från felaktiga avsändare. PTS anser att det behöver förtydligas att operatörerna har möjlighet, eller skyldighet, att blockera bedrägliga meddelanden. PTS vill att hanteringen ska kunna ske proaktivt och direkt av operatör eller sms-aggregatör, utan föregående beslut från KO eller PTS.

Ett alternativ till ny bestämmelse i 9 kap. är att, som noterats ovan, nuvarande 4 kap. 11 § LEK ändras till en skrivning som är närmare ordalydelsen i artikel 97.2 i kodexen. PTS bör då ges bemyndigande att utfärda föreskrifter om i vilka fall operatörer får

[45] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation.

blockera sms utan föregående beslut från myndighet i varje enskilt fall. Detta skulle enligt PTS bedömning göra det tydligare för såväl användare som operatörer i vilka fall det är tillåtet att blockera meddelanden.

Enligt 4 kap. 11 § LEK kan ett nummer blockeras endast efter ett beslut från Konsumentombudsmannen (KO). Möjligheten att blockera är begränsad till fall av otillbörlig marknadsföring. Det finns inga möjligheter att blockera i fråga om rena bedrägerier. Innan numret blockeras ska ”den som har vidtagit marknadsåtgärden” få tillfälle att yttra sig, vilket inte är möjligt för okända bedragare.

Artikel 97.2 i kodexen innehåller dock en skarpare skrivning beträffande bedrägeri eller missbruk av tjänsten. Även denna bestämmelse bygger på ”från fall till fall”, men ger ändå mer utrymme att agera snabbare på misstänkta bedrägeriförsök.

PTS ser att en ändring av 4 kap. 11 § till en lydelse som bättre motsvarar artikel 97.2 i kodexen, skulle kunna göra det tydligare för såväl användare som operatörer i vilka fall det är tillåtet att blockera meddelanden.

PTS anser att KO även fortsättningsvis bör ha möjlighet att fatta beslut i frågor som rör otillbörlig marknadsföring och liknande. PTS bör dock ges rätt att meddela föreskrifter som ger operatörer möjlighet att under vissa angivna förutsättningar stänga av användare (”blockera”) utan föregående beslut från KO. Det kan i sammanhanget nämnas att KO, enligt uppgift till PTS, inte har haft några ärenden enligt LEK.

Ett alternativt sätt att klargöra att operatörerna har möjlighet att blockera bluff-sms är att koppla hanteringen till säkerhetsbegreppet i 1 kap. 7 § och 8 kap. 1 § LEK. Genom att ställa krav på att säkerställa autenticiteten hos meddelandet genom registrerade avsändarnamn höjs säkerheten och möjligheterna för sms-bedrägerier begränsas. PTS anser att 8 kap kan användas som lagstöd för att blockera meddelanden från avsändarnamn som finns på listan men skickas från fel avsändare. För att säkerställa autenticiteten behöver det däremot finnas ytterligare åtgärder, förslagsvis ett register. Finland har i samband med regler kring registrering av avsändarnamn angett bestämmelser i den finska motsvarigheten till LEK som lagstöd för att blockera bluff-sms[46].

PTS slutsats är att oavsett vilka förtydliganden som regeringen väljer behöver regleringen utformas så att PTS genom föreskrifter kan bestämma bl.a. hur

46 https://traficom.fi/sites/default/files/media/file/Skydd%20av%20avs%C3%A4ndaruppgifterna%20i%20textmeddelanden.pdf [Hämtad 2024-12-06].

avsändarnamn ska kunna registreras och hur sms med respektive utan registrerade avsändarnamn ska hanteras av operatörer och sms-aggregatörer.

5.1.2 **Innehåll**

En ytterligare åtgärd som skulle kunna utgöra ett komplement till ovan beskrivna register för avsändarnamn är att tillåta operatörer att filtrera innehåll i sms för att identifiera och blockera bluff-sms. Den svenska marknaden, och även regleringsmyndigheter i andra europeiska länder, har dragit slutsatsen att åtgärder där slutanvändarna själva väljer att installera mobilappar som kan filtrera sms för bedräglig text och länkar är förenligt med gällande bestämmelser.

Grundprinciperna för kommunikation är skydd för privatlivet enligt artikel 8 Europakonventionen och artikel 7 EU-stadgan samt enligt 2 kap. 6 § RF. Vissa undantag från denna grundprincip är dock tillåtna. Vissa tänkbara åtgärder för att förhindra bedrägerier innebär att en avvägning måste göras mellan skyddet av den personliga integriteten och möjligheten att förhindra allvarlig brottslighet. Brottsbekämpning är i första hand en fråga för de brottsbekämpande myndigheterna och inte för PTS. Däremot kan PTS och andra myndigheter bidra till att göra det svårare att genomföra bedrägerierna genom t.ex. föreskrifter, allmänna råd och utgivande av vägledningar.

PTS ser två olika alternativ i fråga om filtrering av sms, obligatorisk eller frivillig lösning.

5.1.2.1 Krav på att filtrera innehåll i sms innan de förmedlas till mottagaren

Något som efterfrågas både i Sverige och andra EU-länder är tydligare regler kring vad som är tillåtet i form av filtrering och skanning av innehåll i meddelanden. PTS har undersökt möjligheterna för operatörerna att filtrera sms baserat på innehållet i meddelandena. Samtliga svenska operatörer har uppgett att de redan idag i viss utsträckning filtrerar bort bedräglig sms-trafik genom att titta på andra faktorer än just innehållet. Andra länder har infört möjligheter för operatörer att på olika sätt filtrera på innehåll.

Filtreringen bör utgå från att t.ex. leta upp kända och uppenbart bedrägliga mönster i innehåll eller länkar. Det handlar inte om att granska sakinnehållet, vilket minimerar eventuella integritetsinskränkningar. Operatörer i andra länder, t.ex. Finland och Belgien, filtrerar redan bort skadlig sms-trafik. Vidare har branschorganisationen GSMA[47] ett projekt för att harmonisera metodik och samverkan bland världens mobiloperatörer för att uppnå tekniska lösningar för att förhindra skadlig sms-trafik och sms-bedrägerier.

[47] GSMA (GSM Association) är en internationell organisation för mobiloperatörer. https://www.gsma.com/.

Ett vägval vid införande av krav på åtgärder som filtrerar länkar och text i sms är om kraven ska ställas på sms-aggregatörer eller operatörer. Skillnaden är att operatörer kan ha möjlighet att filtrera alla typer av sms för bedrägligt innehåll, medan en sms-aggregatör enbart kan filtrera A2P.

5.1.2.2 Frivillig filtrering av innehåll

Ett alternativ till tvingande bestämmelser är att överväga frivilliga möjligheter att filtrera innehållet i sms innan det skickas till mottagaren. Såvitt PTS har kunnat utröna har t.ex. Danmark genom en branschöverenskommelse tydliggjort möjligheten för operatörerna att frivilligt införa filtrering av innehåll i sms. Det är då valfritt för operatörerna att införa en sådan lösning, som då kommer att gälla för alla operatörens kunder. Om en kund inte vill att innehållet i sms:en filtreras får kunden välja en operatör som inte tillämpar den lösningen.

5.1.2.3 Rättsligt stöd och möjliga tillvägagångssätt

Grundprincipen för kommunikation är skydd för privatlivet (artikel 8 Europakonventionen och artikel 7 EU-stadgan samt enligt 2 kap. 6 § RF). Vissa undantag från denna grundprincip är dock tillåtna. Det saknas tydliga lagbestämmelser som kan tillämpas för att stoppa skadligt innehåll i sms.

Enligt dataskyddförordningens[48] artikel 6 är behandling av personuppgifter endast laglig om och i den mån som åtminstone en av följande grunder finns: samtycke, avtal, rättslig förpliktelse, nödvändigt för att skydda grundläggande intresse, myndighetsutövning samt s.k. berättigat intresse. När det gäller filtrering av innehåll i sms, såväl obligatorisk som frivillig genom avtal med slutkunden, är det viktigt att detta sker i enlighet med dataskyddsförordningen. Det är operatörerna själva som är ansvariga för personuppgiftsbehandlingar. PTS har undersökt möjligheterna att tillämpa 8 kap. LEK med utgångspunkt i kravet på autenticitet, som enligt definitionen i 1 kap 7 § LEK innefattas i begreppet ”säkerhet i nät och tjänster”.

I 8 kap. LEK anges att tillhandahållare ska vidta lämpliga organisatoriska och tekniska åtgärder för att upprätthålla säkerhet i nät och tjänster. Av definitionen till ”säkerhet i nät och tjänster” i 1 kap. 7 § LEK framgår att bl.a. säkerhetsbegreppet autenticitet innefattas. Autenticitet eller äkthet, är nära relaterat till riktighet, men tar snarast sikte på informationens ursprung. Kravet på autenticitet innebär bl.a. att uppgifter om varifrån information kommer ska skyddas mot förfalskning eller förvanskning.[49]

[48] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

[49] Prop. 2021/22:136 s. 324

Ett sätt att reglera filtrering av innehåll är att med utgångspunkt i 8 kap. 1 § LEK utforma mer detaljerade krav för att uppnå autenticitet för sms-tjänster. För sms innebär det att avsändaren är den som den framstår att vara och att innehållet är det som det framstår att vara.

PTS gör bedömningen att brottsvinsterna från sms-bedrägerier kan minskas med upp till 408 miljoner SEK genom att införa åtgärder. Bedömningen har gjorts utifrån antagande baserat på den kvarvarande andelen av brottsvinsterna från vishing (både telefoni och sms) år 2023 på 708 miljoner SEK, som inte redan har åtgärdats eller kan åtgärdas med exempelvis den föreskrift som stoppar samtal vid det internationella gränssnittet.

5.1.2.4 Jämförelse med andra länder

I Belgien ges operatörerna möjlighet att välja om de vill filtrera innehåll i sms. En annan variant som t.ex. Norge valt är att man från lagstiftarens sida accepterar att sms:en filtreras för att hitta länkar. Om operatörerna får möjlighet att filtrera sms skulle de kunna erbjuda sina kunder att i avtalet med operatören välja om de vill få sina sms filtrerade eller inte.

I Finland trädde Traficoms föreskrift om televerksamhetens informationssäkerhet i kraft den 1 september 2024. Den innehåller bl.a. krav på att teleföretag ska filtrera både sms och mms. I Finlands motsvarighet till LEK föreskrivs bl.a. krav på att trygga kommunikationsmöjligheter för den som sänder eller tar emot meddelanden avseende åtgärder för informationssäkerhet.

Irländska ComReg har också tittat på lösningar för att filtrera bluff-sms. Ett sådant filter fungerar enligt ComReg på samma sätt som ett spamfilter som används för e-post. Inkommande meddelanden dirigeras genom en brandvägg för att upptäcka och blockera skadliga länkar eller innehåll. För att kunna implementera sådana lösningar behövs nya mandat och regeländringar. Att operatörerna erbjuder sina kunder att frivilligt ansluta sig till en skanningstjänst kan vara en potentiell väg att gå.

5.1.2.5 Bedömning

De flesta operatörer som PTS har pratat med har framhållit behovet av tydligare reglering av möjligheterna att filtrera innehåll i sms, så att gränserna för vad som är tillåtet tydliggörs.

PTS har bemyndigande att ta fram ytterligare föreskrifter beträffande säkerhetsåtgärder enligt 8 kap. 1 § LEK. Emellertid ska en ny cybersäkerhetslag

implementeras i Sverige med anledning av det så kallade NIS2-direktivet.[50] PTS mandat och föreskriftsrätt enligt 8 kap. LEK kan därför komma att ändras. PTS konstaterar det råder stor osäkerhet kring vilka bestämmelser i LEK som kommer att falla inom PTS ansvarsområde.

PTS bedömer att det i nuläget inte finns förutsättningar för att filtrera innehåll i sms eftersom rättsläget är svårbedömt med hänsyn till gällande bestämmelser om integritet och behandling av uppgifter enligt 9 kap. LEK och e-Privacy-direktivet[51]. Det nu gällande e-Privacydirektivet kan komma att upphävas eller ändras inom en inte alltför avlägsen framtid. Det i kombination med det osäkra rättsläget kring den nya cybersäkerhetslagen gör att PTS i nuläget inte rekommenderar några åtgärder gällande filtrering av innehåll i sms.

Myndigheten fortsätter dock att bevaka frågan och rättsutvecklingen i övriga länder, då detta kan komma att påverka förutsättningarna för eventuella vidare åtgärder.

5.2 Kundkännedom

Kundkännedom i det här sammanhanget handlar om att operatören eller sms-aggregatören ska ha tillräckligt god kännedom om sin kund för att försvåra och förhindra att operatörens eller sms-aggregatörens verksamhet utnyttjas för att genomföra bedrägerier. I detta fall handlar det främst om att lära känna de kunder som skickar A2P-sms där sms-aggregatörer behöver ha kännedom om de företag som använder deras tjänster och operatörer i sin tur behöver ha kännedom om de sms-aggregatörer som de samarbetar med.

Att lära känna sina kunder är ett första steg för att kunna genomföra en riskbedömning avseende aktuella och blivande kunder så att operatören eller sms-aggregatören ska kunna vidta lämpliga åtgärder för att förhindra att deras verksamhet utnyttjas för bedrägerier, dvs att A2P-sms endast skickas från betrodda källor, samt för att kunna rapportera misstänkta aktiveter till polisen.

Ett första steg för att lära känna sin kund är att identifiera kunden och göra en identitetskontroll av de som vill skicka A2P-sms. Ett andra steg i att lära känna sin kund är att begära information om vad kunden vill få ut av affärsförbindelsen och

[50] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS2-direktivet).

[51] Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation)

vilka tjänster kunden kommer att utnyttja och i vilken omfattning. Ett tredje steg är att inte tillåta kunder som inte kan styrka sin identitet eller på ett tydligt sätt kan beskriva sina avsikter att använda operatörens eller sms-aggregatörens tjänster. Vidare bör operatören eller sms-aggregatören fortlöpande följa upp pågående affärsförbindelser för att på så sätt säkerställa att kundkännedomen är aktuell. Sms-aggregatörer och operatörer ska genomföra en riskbedömning för att undersöka om och hur deras tjänster eller produkter kan utnyttjas för bedrägerier.[52] Riskbedömningen bör sedan ligga till grund för att utveckla rutiner. Dessa rutiner ska sedan tillämpas av sms-aggregatörerna och operatörerna för att minimera riskerna för att deras verksamhet utnyttjas av bedragare.

PTS bedömning är att en branschöverenskommelse för att etablera regler för kundkännedom är en genomförbar åtgärd. Ett andra alternativ, om en branschöverenskommelse inte är möjlig, är att PTS tar fram en vägledning gällande kundkännedom till sms-aggregatörer och operatörer. Fördelen med en branschöverenskommelse är att den etableras av berörda aktörer varför PTS kommer påbörja arbetet med att driva frågan om att en branschöverenskommelse.

5.3 Förbjuda sim-farmar

Ett tillvägagångssätt för bedragare är att använda sig av s.k. sim-farmar för att kunna skicka ut bluff-sms till ett stort antal slutanvändare genom att använda många sim-kort. Det har i dessa sammanhang varit vanligt förekommande att bedragarna använt oregistrerade sim-kort. Genom reglerna om registrering av kontantkort har detta förfarande försvårats. I kartläggningen har det har dock framförts av någon aktör att bedragare i vissa fall kringgår kraven om registrering genom att låta s.k. målvakter registrera sig på ett eller flera kontantkort. I bland annat Storbritannien är det förbjudet att tillhandahålla eller inneha sim-farmar för vissa utpekade syften men eftersom det kan föreligga bevissvårigheter utreder Ofcom (PTS motsvarighet i Storbritannien) frågan vidare.[53] PTS har i kartläggningen inte fått information om att sim-farmar skulle vara ett stort problem i Sverige och har därför valt att inte gå vidare med förslag på reglering. Givet uppgifterna om utnyttjande av målvakter kommer dock PTS fortsatt följa utvecklingen och samarbeta med andra länder.

[52] Jfr. Riskanalys som ska genomföras enligt 8 kap. LEK och PTS föreskrifter och allmänna råd (PTSFS 2022:11) om säkerhet i nät och tjänster

[53] https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/call-for-input-reducing-mobile-messaging-scams/main-documents/cfi-reducing-mobile-messaging-scams.pdf?v=373465 [Hämtad 2024-12-06].

5.4 Samverkan och informationsspridning kring bedrägerier

Idag saknas en formaliserad samverkan mellan sms-aggregatörer, operatörer, myndigheter och andra berörda aktörer. Detta medför troligen att viktig information rörande bedrägerier som sker med stöd av elektroniska kommunikationstjänster inte sprids eller sprids långsamt mellan de som på olika sätt kan bidra till att minska bedrägerierna. Dessutom saknas en gemensam informationskanal genom vilken information om t.ex. pågående bedrägeriförsök kan spridas eller om hur man som kund bäst skyddar sig.

Många myndigheter och andra organisationer arbetar på olika sätt för att motverka bedrägerier. Exempelvis arbetar Polismyndigheten förebyggande mot vishing och andra bedrägerier bl.a. genom dialoger med banker, mobiloperatörer och webbutiker för att stödja dem i arbetet med att göra plattformar svårare för bedragarna att angripa. Ett annat exempel är Finansinspektionen som under året också haft ett regeringsuppdrag för att motverka bedrägerier[54], som redovisades i maj 2024[55].

PTS anser att en mer formaliserad samverkan krävs för att motverka bedrägerier genom elektroniska kommunikationstjänster på ett ännu mer effektivt sätt. I Norge har man utsett en nationell expertgrupp mot digitala bedrägerier bestående av representanter både från myndigheter och berörda branscher i syfte att hitta gemensamma åtgärder för att motverka bedrägerier samt att samordna informationsspridning.[56]

PTS föreslår att en motsvarande expertgrupp genom ett samverkansforum etableras i Sverige för att på så sätt bl.a. kunna dela erfarenheter och kunskaper kring bedrägerierna. I nuläget finns viss samverkan mellan berörda parter, men det finns inget strukturerat forum avsett specifikt för den här typen av frågor. En önskad effekt av samverkan är att bygga upp en gemensam kunskap om bedragarnas tillvägagångssätt, att snabbare kunna motverka dessa samt att nå ut med samordnad information till allmänheten, bolag och organisationer. PTS föreslår i ett första steg att PTS sammankallar och leder samverkansforumet och bjuder in relevanta deltagare som kan bestå av branschrepresentanter och andra myndigheter.

PTS bedömer att kostnader för att driva detta samverkansforum ryms inom befintlig ram. Inga betydande kostnader förväntas uppstå för deltagare i forumet.

[54] https://www.regeringen.se/contentassets/6dd1b8b156ae4e3dbe7ccd0d23faf5f1/uppdrag-om-motverkande-av-bedragerier.pdf [Hämtad 2024-12-06].
[55] https://www.fi.se/contentassets/80ee86ed2cd34676849dbeb89f204ee9/rapport-motverkande-av-bedragerier-i-betaltjanster.pdf [Hämtad 2024-12-06].
[56] https://nkom.no/aktuelt/norge-skal-lede-global-kamp-mot-digital-svindel [Hämtad 2024-12-06]

5.5 Övriga åtgärder

Nedan listas några övriga åtgärder inom PTS ordinarie verksamhet som PTS har noterat under arbetet med uppdraget och som bidra till att motverka bedrägerier.

5.5.1 Nummertillstånd

Nummer ur telefoninummerplanen som PTS förvaltar tilldelas operatörer och tillhandahållare genom beslut om nummertillstånd. Utvecklingen på marknaden har lett till att tjänster med tillgång till nummer säljs mellan olika tillhandahållare. T.ex. finns det MVNE:er[57] som tillhandahåller tjänster på grossistnivå, ibland i flera led. En MVNE har inte egen infrastruktur utan hyr det från en tillhandahållare som har det. I dessa sammanhang försvåras möjligheten att kontrollera vem som slutligen är användaren av ett telefonnummer. Detta är särskilt besvärligt då telefonnummer används i bedrägerisammanhang.

5.5.2 Global Title

Global Title[58] är en adress som används för att kommunicera mellan elektroniska kommunikationsnätverk och dess nätverkspunkter. En Global Title adress ser normalt ut som ett vanligt mobilnummer då det har blivit industripraxis att man omvandlar mobilnummer för detta syfte. PTS har under det senaste året noterat att allt fler svenska nummer förekommer i samband med Global Title-baserade bedrägerier där man exempelvis skickar stora mängder signaleringstrafik i olika slags belastningsattacker, olovligt får tag på känslig information om enstaka individer som exempelvis platsinformation eller för att kringgå befintliga brandväggar genom att maskera sig som en trovärdig operatör och på så sätt kunna skicka bedrägliga meddelanden till företag och privatpersoner.

Branschorganisationen GSMA har uppmärksammat fenomenet i rapporten *Global Title Leasing Code of Conduct*[59] där det konstateras att uthyrning av dessa nummerresurser gjorts med bristfälliga kontroller av lämpligheten hos den som hyr, och att detta har introducerat säkerhetsrisker i kommunikationsnäten både för operatörer och slutanvändare.

PTS har under hösten 2024 påbörjat ett arbete kring både nummertillstånd och Global Title för att få en större förståelse och för att kunna identifiera och vidta lämpliga åtgärder för att motverka de problem som kan uppstå med dessa

[57] MVNE; Mobile Virtual Network Enabler

[58] Global Title är en adress som används i SCCP-protokollet för att dirigera signaleringsmeddelanden inom elektroniska kommunikationsnät

[59] https://www.gsma.com/solutions-and-impact/technologies/security/gtleasing/ [Hämtad 2024-12-06]

företeelser. Andra länder har också sett liknande problem, och likt Sverige börjat agera i frågan.

5.5.3 **Anmälningsplikten**

Den som ska erbjuda elektroniska kommunikationsnät och kommunikationstjänster till allmänheten måste först göra en anmälan till PTS. Anmälan ska vara gjord innan verksamheten påbörjas. I 2 kap. 1 § LEK framgår att allmänna elektroniska kommunikationsnät som vanligen tillhandahålls mot ersättning eller allmänt tillgängliga elektroniska kommunikationstjänster får tillhandahållas endast efter anmälan till tillsynsmyndigheten. Anmälningsplikten gäller t.ex. inte nummeroberoende interpersonella kommunikationstjänster (t.ex. WhatsApp och Messenger).

Artikel 12 i kodexen innehåller grundläggande bestämmelser om marknadsinträde för den som tillhandahåller elektroniska kommunikationsnät och kommunikationstjänster till allmänheten. I enlighet med artikel 12.3 får det krävas att företag som omfattas av allmän auktorisation ska göra en anmälan. Däremot får det inte krävas något beslut eller någon annan administrativ handling från en myndighet innan ett företag börjar utöva de rättigheter som följer av att en anmälan har gjorts. Det finns alltså ingen möjlighet att inom anmälningsförfarandet initialt granska dem som står bakom verksamheten. Däremot finns möjligheten att inom ramen för tillsynen besluta att den som åsidosatt en skyldighet som följer av lagen ska upphöra med verksamheten. Syftet med regleringen är att det ska vara lätt för aktörer att starta upp verksamheter och vara delaktiga i att det skapas ett stort utbud av nät och tjänster för slutanvändarna på marknaden för elektroniska kommunikationer.

På den svenska marknaden för elektroniska kommunikationer finns det idag många verksamma aktörer. Vissa av dessa har inte hemvist i Sverige, istället är hemvisten antingen inom EU, övriga Europa eller utanför Europa. En del av de som inte har hemvist i Sverige har en adress i Sverige men flera av dem har inte det, vilket försvårar PTS tillsynsmöjligheter. Det kan också försvåra utredningar för brottsbekämpande myndigheter. När tröskeln för inträdet på en marknad är låg finns alltid en risk att även oseriösa aktörer söker sig dit om den är lukrativ eller om möjligheter finns att genomföra bedrägerier i någon form för att på så sätt skapa ekonomisk vinning.

I den eskalering som nu skett gällande bedrägerier, och andra angrepp mot elektroniska kommunikationer i samhället både från illasinnade stater och av kriminella, finns det anledning att utvärdera om detta enkla marknadsinträde fortfarande är lämpligt. Förfarandet för anmälningsplikten är styrt av kodexen. Vid den översyn som planeras till 2025 bör för- och nackdelar med det enkla marknadsinträdet analyseras.

5.6 Effekter på samhället om inga åtgärder vidtas

Avslutningsvis kan PTS konstatera att det inte råder någon tvekan om att sms-bedrägerier genererar stora brottsvinster. Brottsvinsterna från vishing år 2023 låg på 708 miljoner SEK. Mer än hälften av beloppet kan kopplas till bluff-sms. PTS uppskattar att sms-bedrägerier till ett värde av maximalt 408 miljoner SEK per år skulle kunna förhindras om samhället lyckades stoppa alla bluff-sms. Det finns därmed ett stort ekonomiskt incitament för samhället att agera. Dessutom kan potentiella brottsoffer komma att besparas onödigt lidande. Eftersom möjliga åtgärder är beroende av t.ex. frågor om personlig integritet är det befogat att ställa frågan vad som händer om samhället väljer att *inte* vidta några åtgärder för att motverka bluff-sms. Intressant i sammanhanget är att utgå från *externaliteter*[60].

Om vi utgår ifrån att Sverige skulle välja att vara passiva i bekämpningen av bluff-sms blir frågan hur andra länders behandling av frågan skulle kunna påverka Sverige. De ekonomiska incitamenten bland brottslingarna är stora. Om ett land lyckas förhindra sms-bedrägerier genom reglering är sannolikheten stor att de brottsliga aktiviteterna flyttas till ett annat land med svagare skydd. Detta är möjligt eftersom den kriminella aktiviteten utförs globalt. Allt fler länder har på senare tid infört skyddsåtgärder. Irland, Polen och Storbritannien är tre exempel på detta[61]. Finland och Singapore är ytterligare två länder som har vidtagit åtgärder. Skulle ännu fler länder öka sitt skydd, finns risk att nationer som väljer att avstå från åtgärder betraktas som ”fristäder” bland brottslingarna. Bluff-sms kan därför komma att öka i Sverige i framtiden om åtgärder inte vidtas, detta enbart till följd av andras åtgärder.

Ytterligare ett problem med externaliteter är att brott i någon mening följer ”marknadslogik”. Om sms-kriminalitet visar sig lönsam, kommer omfattningen av denna oönskade verksamhet att öka av rent logiska skäl. Människor tenderar att satsa mer på det som fungerat hittills, det gäller även kriminella. Om detta fortgår utan åtgärder så är risken även stor att förtroendet försvagas eller helt upphör hos slutanvändarna för denna idag mycket viktiga kpeommunikationstjänst.

[60] En extern effekt uppstår när de samhällsekonomiska kostnaderna för en vara eller en transaktion underskattas eller överskattas i förhållande till dess marknadspris. Det uppstår då produktion eller konsumtion av en vara orsakar välfärdsförändringar för andra än producent eller konsument. I detta fall orsakar ökade åtgärder mot sms-bedrägerier i andra länder negativ påverkan i Sverige då de bedragare som verkat på den berörda utländska marknaden rör sig mot den svenska marknaden om vi inte infört liknande åtgärder.

[61] Nivot, Laurence. (2024). *National measures against spoofing practices*. CTTEEU20240059. 15 July.

Litteratur och referenser

Förarbeten

Prop. 2002/03:110 (Lag om elektronisk kommunikation, m.m.)

Prop. 2010/11:115 (Bättre regler för elektroniska kommunikationer)

Prop. 2021/22:136 (genomförande av direktivet om inrättande av en europeisk kodex för elektronisk kommunikation)

Rapporter m.m.

Begripsam, *Svenskarna med funktionsnedsättning och internet 2023*, 2024.

Brå, rapport 2023:11. *Bedrägerier mot privatpersoner De förebyggande åtgärdernas träffsäkerhet*.

Berec, *Draft Berec work programme 2025*, december 2024, BoR (24) 148.

Infocomm Media Development Authority (IMDA), 14 oktober 2022, *Decision issued by the Info-communications Media Development Authority on proposals to strengthen safeguards for sms messages to Singapore users: full sms sender id registry regime*, https://www.imda.gov.sg/-/media/imda/files/regulations-and-licensing/regulations/consultations/2022/proposals-to-strengthen-safeguards-for-sms-messages-to-singapore-users/full-ssir-regime/imda-decision-on-full-ssir-regime.pdf

ECC Recommendation (23)03 - Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers.

Finansinspektionens rapport, *Motverkande av bedrägerier i betaltjänster*, 31 maj 2024, Dnr 24–14480.

Nitz, Lena. Svenskt Näringsliv (2023). *Brottslighetens kostnader 2023*

Nivot, Laurence. (2024). *National measures against spoofing practices*. CTTEEU20240059. 15 July.

Ofcom, 29 juli 2024, *Reducing mobile messaging scams - Evidence and options for addressing consumer harm,* https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-

1-10-weeks/call-for-input-reducing-mobile-messaging-scams/main-documents/cfi-reducing-mobile-messaging-scams.pdf?v=373465.

Polismyndigheten, *Brottsvinsterna för bedrägeribrottsligheten 2023*, 2024-04-15, Dnr A233.272/2024

Post- och telestyrelsen, PTS-ER-2024:18, *Svensk telekommarknad 2023*.

Traficom, 19 april 2024, *Skydd av avsändaruppgifterna i textmeddelanden*, https://www.traficom.fi/sites/default/files/media/file/Skydd%20av%20avs%C3%A4ndaruppgifterna%20i%20textmeddelanden.pdf

Internetadresser

https://www.europol.europa.eu/sites/default/files/documents/wangiri_final_2.pdf

https://www.gsma.com/solutions-and-impact/technologies/security/gtleasing/

https://internetkunskap.se/snabbkurser/falska-sajter-och-annonser/skydda-dig-mot-falska-webbsidor/

https://mediemyndigheten.se/ansokan-och-registrering/regelverk/dsa--eus-forordning-om-en-inre-marknad-for-digitala-tjanster/

https://www.msb.se/sv/rad-till-privatpersoner/digital-sakerhet/natfiske-och-skadlig-kod/

https://nkom.no/aktuelt/norge-skal-lede-global-kamp-mot-digital-svindel

https://pts.se/internet-och-telefoni/dsa-forordningen---regler-om-digitala-tjanster-for-en-sakrare-onlinemiljo/

https://pts.se/internet-och-telefoni/sakerhet-och-skydd-av-uppgifter/telefonbedragerier/

https://statistik.pts.se/telekom-och-bredband/svensk-telekommarknad/tabeller/mobila-samtals-och-datatjanster/tabell-16-sms/

https://www.traficom.fi/sv/vara-tjanster/ansok-om-sms-sender-id-kortmeddelande-tjanster