

TELEFONBEDRÄGERIER

-hur kan det stoppas?

Förord

Telefonbedrägerier har funnits mycket länge och fick extra stor uppmärksamhet efter Uppdrag gransknings program. Det var först efter det som statsministern kallad till möte med bankerna för att höra hur man kan få ett stopp på det.

Telefonbedrägerier anses nu vara så allvarlig att den av många anses som system- och samhällshotande.

Men ingen ifrågasätter varför de svenska telekombolagen inte stoppar manipulerade telefonnummer när t.ex. Finland redan gjort det. Hur kan de klara sig undan kritiken? Varför är det ingen som ifrågasätter deras verksamhet, som möjliggör telefonbedrägerier?

Jag har själv en anhörig som varit drabbad i över 20 år och 2018 fick jag nog och tog över ansvaret för att försöka få stopp på det. Det jag då upptäckte var att inget telekombolag ville ta ansvar för bedrägerier och penningtvätt som pågick via telefonnummer med förhöjd samtalstaxa, något som även är anmält till PTS utan någon reaktion. I stället hänvisade telekombolagen till andra eller svarade med oriktiga uppgifter, till både till mig och myndigheter, ARN. Min uppfattning är att telekombolagen helt enkelt försökte mörka det inträffade.

När jag sedan 25 maj 2023 träffade Gitte och Åsa, initiativtagare och grundarna till Föreningen mot Nätbedrägerier, på en manifestation på Mynttorget mot bankbedrägerier så insåg jag att det var ett större samhällsproblem än jag tidigare förstått och att jag inte var ensam om att undra hur de ens kan vara möjligt att ingen försöker stoppa det.

Vid ett riksdagsseminarium 21 november om bankbedrägerier krävde vi därför att tjänsten som möjliggör manipulerade samtal skulle stoppas helt.

Detta är första utgåvan av granskningen och tips och synpunkter tas gärna emot om det saknas något eller om det finns otydligheter eller faktafel, så rättar jag gärna upp det i framtida utgåvor.

Tyresö april 2024
Mikael Förborgen
Styrelseledamot, Föreningen mot Nätbedrägerier

Innehåll

1.	Inledning.....	4
	Bakgrund	4
	Brottsstatistik	4
	Skadestånd till brottsoffer	4
	Hur går telefonbedrägerier till	5
	Digitala spår på nätet.....	6
	Olika typer av begrepp.....	6
	Vad är social manipulation.....	7
2.	Sammanfattning	7
3.	PTS vägledning.....	8
	Inledning.....	8
	PTS remiss.....	8
	Remissvar Föreningen mot Nätbedrägerier	8
	Remissvar sammanfattning övriga.....	8
	Regeringsuppdrag från Finansdepartementet.....	9
4.	PTS föreskrifter	9
	Inledning.....	9
	Förslag på föreskrifter.....	9
	Konsekvensutredning	10
5.	Bluff-SMS 7726	10
6.	Globalt problem.....	11
	CEPT och ECC.....	11
	Finland	11
	Norge	11
	Storbritannien	12
	Australien	12
	Malta	12
7.	Alternativa lösningar	12
	Inledning.....	12
	PTS förslag.....	12
	STIR/SHAKEN.....	12
	Säkra samtal	13
8.	Slutord.....	13
9.	Bilaga 1	14
10.	Bilaga 2	15

1. Inledning

Bakgrund

Telefonbedrägerier har funnits mycket länge utan att någon på allvar har försökt stoppa det.

Denna granskning försöker svara på varför det är så och om det är möjligt att stoppa telefonbedrägerier och varför ingen har gjort det tidigare.

Telefonbedrägerier är inget nytt, det berättar Marcus Nohlberg på Högskolan i Skövde om i Vetenskapsradions två program "Lurad via luren".¹ Marcus gjorde en avhandling om telefonbedrägerier redan 2008.²

Telefonbedrägerier är ett problem som sedan 2018 har eskalerat och alltså nu anses som systemhotande av polisen med flera.

Brottsstatistik

Ett tag såg det först ut som att antal bedrägerier började minska 2018, framför allt kortbedrägerier, men på senare år har både telefonbedrägerier genom social manipulation och kortbedrägerier ökat kraftig och effekten av tidigare försök att minska bedrägerier har försvunnit helt.

Vid Bankföreningens digitala seminarium³ 26 januari berättar Johan Sekora, Global Head of Financial Crime Prevention på SEB, om utvecklingen av telefonbedrägerier. Presentationen visar Sveriges lägesbild över bedrägerier där man ser att ökningen börjar redan 2005 fram till första toppen 2018.

Han visar också en trendförändringen för bedrägerier genom social manipulation från 2019 till 2022. Från att majoriteten var obehörig transaktion till att i stället vare en behörig transaktion, dvs när man inte får någon ersättning från bank. Någon förklaring på den lite märkliga trendförändringen till behörig transaktion, som uppskattas ligga på 70 - 90% beroende på bank, ges inte.

2023 var antalet bedrägerianmälningar klassade som social manipulation totalt 47 526.⁴ Notera att allt inte är telefonbedrägerier utan är uppdelat på fyra olika kategorier och Vishing ingår i kategorin befogenhetsbedrägerier som var 12 312, men lite oklart vad som är korrekt siffra. Mer om senaste statistiken från Brå i bilaga 1.

Skadestånd till brottsoffer

Orsaken till att fler har drabbats på senare tid, ekonomiskt, kan bero på den lagändring 2018 av betaltjänstlagen⁵ och där ARN:s ändring av praxis av vad som anses som en obehörig transaktion, 2018-06551,⁶ som gjorde att banker bara i undantagsfall blev skadeståndsskyldiga vid bedrägerier. Svenska bankföreningen menade då att lagförändringen skulle förbättrat konsumentskyddet,⁷ det blev precis tvärtom.

Uppgifter om hur många som fick ersättning direkt från sin bank är oklart, men uppskattningsvis maximalt 10%, dvs bara om det är en obehörig transaktion och om man inte anses vara särskilt klandervärd av banken. Det ger ca 2 312 som kan ha fått ersättning.

2023 gjordes det 2 780 anmälningar till ARN⁸ som berörde bank, men bara 1 599 avgjordes i sak och det var bara 128 som fick bifall i ARN 2023. Det är långt ifrån de tiotusentals bedragna som media rapporterade om skulle få rätt 2022 efter den omtalade HD-domen.⁹

¹ [Lurad via luren – här är fällorna telefonbedragarna utnyttjar 10 mars 2024 - Vetenskapsradion På djupet | Sveriges Radio](#)

² [Så blir du lurad att lämna i från dig hemlig information - forskning.se](#)

³ [Samverkan för att motverka bedrägerier | Swedishbankers](#)

⁴ [Bedrägerier och ekobrott - Brottsförebyggande rådet \(bra.se\)](#)

⁵ [Betaltjänstlagen och PSD2 \(Payment Services Directive 2\) | Swedishbankers](#)

⁶ [referat-anr-2018-06551.pdf \(arn.se\)](#)

⁷ [Vad innebär den nya betaltjänstlagen och PSD2? | Swedishbankers](#)

⁸ [Årsredovisningar | Allmänna reklamationsnämnden \(arn.se\)](#)

⁹ [Efter HD-dom: Tiotusentals bedragna kan få tillbaka pengar | SVT Nyheter](#)

Skadeståndskravet för brottsoffer vid telefonbedrägerier fastställs i domstol och hamnar hos penningtvättsmålvakten som inte har några pengar.¹⁰ Det finns därför ingen möjlighet för brottsoffer att få hjälp av kronofogden eller brottsoffermyndigheten för att få ut skadeståndet. Brottskadeersättning för ren förmögenhetsskada ges nämligen bara i undantagsfall och inte vid telefonbedrägerier.¹¹

Hur går telefonbedrägerier till

I Vetenskapsradions På djupet får vi i två avsnitt ta del av både den tekniska och den psykologiska delen av telefonbedrägerierna. Gitte, initiativtagare och ordförande i Föreningen mot Nätbedrägerier, berättar genom en rekonstruktion hur hon blev utsatt för telefonbedrägeri. Retorikexperten vid Uppsala universitet berättar om den mänskliga svaghet som gör bedrägerierna möjliga. Gittes berättelse finns i sin helhet att läsa på Internetstiftelsen¹² samt att lyssna till på Internetpodden.¹³

Inte förrän Uppdrag granskings reportage har problemet med telefonbedrägerier blivit mer allmänt känt. I tre olika program har UG granskat bedrägerier. Först i serien om Marbella från juli 2023 där del 4, Bedragarna i paradiset, tar upp telefonbedrägerier. Sedan kom Bedragarna i februari 2024 där vi fick följa ligan från insidan och senast i programmet om Hackaren från mars 2024.

Inget av dessa program är egentligen några nyheter. Det har brottsoffer berättat om länge utan att någon har lyssnat på dem. Till exempel i ett inslag från SVT Nyheter i januari 2019:¹⁴ *”De utger sig för att komma från Elgiganten, Postnord eller din bank. Sen skrämmar de dig med att du blivit ID-kapad eller att ditt bankkort använts för att köpa varor du aldrig beställt.”*

Efter programmet från SVT Nyheter finns en flera sidor lång chatt där utsatta berättar vad de blivit utsatta för. SVT Nyheter berättar om många reaktioner de fått efter berättelse om telefonbedragare¹⁵ och de beskriver exakt samma sak som händer idag. En bank uttalar sig till SVT Nyheter, SEB, och berättar: *”Vi ser att de till exempel får tillgång till 010-nummer som vanligtvis bara myndigheter eller andra betrodda organisationer har.”*

Exempel på hur telefonbedrägeri kan gå till:

1. Först samlar bedragarna in personuppgifter, till exempel sådant som går att hitta på nätet genom olika informationstjänster eller genom phishing eller smishing.
2. Sedan skickar de ut ett bluff-SMS som massutskick till en grupp lämpliga brottsoffer, som man redan samlat in personuppgifter om. Man sitter inte och ringer upp en och en, det skulle ta alldeles för lång tid och med okänt resultat.
3. De personer som sedan ringer upp det nummer som står i bluff-SMS är de som snarare beroende på under vilka omständigheter de just för tillfället befinner sig i, stress eller annat, än att de skulle vara särskilt lättlurade. Det kan räcka med en sekunds ouppmärksamhet eller att man bara vill ringa för att rätta till något som är felaktigt och snabbt få det ur världen.
4. Eftersom man redan läst och vet att det som står i bluff-SMS är felaktigt, det är ju därför man ringer upp, så är man redan upprörd och fastnar direkt i bedragarna nät genom social manipulation. Detta eftersom man är helt övertygad om att det manipulerad SMS:et verkligen kommer från det företaget som de utger sig för att vara.

Ett riktigt exempel från SEB idag visar också Johan Sekora, som nämndes tidigare, i sin presentation om söktjänster och SMS spoofing och påpekar att det saknas lagstiftning för att stoppa dessa.

¹⁰ [Två döms efter bedrägeri mot äldre - chans till ersättning - DN.se](#)

¹¹ [Sak- och rena förmögenhetsskador \(Brottsoffermyndighetens referatsamling 2020\)](#)

¹² [Telefonbedragare stal Gittes livsbesparingar \(internetkunskap.se\)](#)

¹³ [Så lurade telefonbedragare Gitte på hennes livsbesparingar | Internetstiftelsen](#)

¹⁴ [Polisen varnar för nya bedrägerimetoden: ”Extremt manipulerande” | SVT Nyheter](#)

¹⁵ [Många reaktioner efter berättelse om telefonbedragare | SVT Nyheter](#)



Bild från SEB presentation

Digitala spår på nätet

Alla vet om att allt man gör på nätet lämnar digitala spår efter sig som för alltid kommer att finnas kvar. Hur kan det då komma sig att just telefonbedragare kan använda sig av telefonnätet och andra legala tjänster som manipulerade nummer, spoofing, helt anonymt utan att polisen får hjälp av telefonbolagen med att spåra upp vem som ringde och utförde bedrägeriet?

Detsamma gäller för bankerna. Första överföringen går till en penningtvättmålsvakt. Efter det verkar det omöjligt för banken att hjälpa polisen med information om vart eller till vem pengarna egentligen tog vägen?

Digitala spår från bedragare verkar helt försvinna hos telekombolag och banker, hur är det ens möjligt 2024?

Vad är det som lagstiftaren missar när man inför förbud mot anonyma kontantkort för mobilen men inte mot manipulerade telefonnummer?¹⁶

Vilken effekt förbudet mot anonyma kontantkort för mobilen fått är lite oklart, enligt polisen finns mobil-målvakter.¹⁷ PTS ska göra en prioriterad tillsyn av kontantkort under 2024 för att ta reda på det.¹⁸

Olika typer av begrepp

Vad betyder Vishing, Spoofing, Phishing, Smishing och Wangiri?

Spoofing¹⁹ är manipulerade telefonnummer som ska lura dig att tro att det verkligen kommer från det företaget som de utger sig för att vara.

Manipulerade telefonnummer kan sedan används för att genomföra telefonbedrägerier s.k. **Vishing**. Ordet är en sammanslagning av voice (röst) och phishing (fiske).²⁰

Phishing och **Smishing** är s.k. nätfiske för att komma åt personliga uppgifter via mejl eller SMS²¹

Wangiri (ping-samtal) innebär att den som ringer upp lägger på efter bara en signal. Syftet är att få dig att ringa tillbaka. Numret som ringer är ofta ett högkostnadsnummer (betal-samtal- eller utlandsnummer).

¹⁶ [Nya regler förbjuder anonyma kontantkort \(telekomradgivarna.se\)](https://www.telekomradgivarna.se/nyheter/nya-regler-forbjuder-anonyma-kontantkort)

¹⁷ [Kriminellas nya kryphål: "Mobil-målvakter" - P4 Skaraborg | Sveriges Radio](https://www.sverigesradio.se/artiklar/kriminellas-nya-kryphal-mobil-malvakter-p4-skaraborg)

¹⁸ [Avtalsinformation och kontantkort prioriterad tillsyn under 2024 | PTS](https://www.pts.se/nyheter/avtalsinformation-och-kontantkort-prioriterad-tillsyn-under-2024)

¹⁹ [Telefonbedrägerier | PTS](https://www.pts.se/nyheter/telefonbedrageri)

²⁰ [Polis: Banker måste ta mer ansvar för att stoppa bedrägerier - DN.se](https://www.dn.se/nyheter/polis-banker-masta-ta-mer-ansvar-for-att-stoppa-bedrageri)

²¹ [Nätfiske, phishing | Polismyndigheten \(polisen.se\)](https://www.polisen.se/nyheter/natfiske-phishing)

Vad är social manipulation

Bedrägerier där gärningspersonen tar kontakt med person för att luras och komma åt dennes pengar och det är absolut inte bara äldre som kan drabbas.

Telefonbedrägerier genom social manipulation kommer aldrig att kunna stoppas med bara information på det sättet som banker, PTS och Telekområdgivarna försöker göra.²² Det förklarar Lars-Olof Johansson, professor i psykologi från Göteborgs universitet, mycket tydligt och bra på Riksdagsseminariet 21 november och som är publicerat på föreningens sida.²³

Att informera om riskerna för att bli utsatt för telefonbedrägeri är bra men att det skulle vara lätt att bli svårlurad²⁴ stämmer inte riktigt, tvärtom, vem som helst kan bli lurad även om många inte tror det förrän det händer. Bankernas kampanj har även fått kritik av forskaren Marcus Nohlberg²⁵ för att ytterligare skambelägga brottsoffer och riskerar att många, på grund av skuld och skamkänslor, inte anmäler till bank och polis när de blivit utsatta. Det finns troligen därför ett stort mörkertal när det gäller telefonbedrägerier.

2. Sammanfattning

En sammanfattning av efterföljande kapitel där PTS vägledning och förslag på föreskrifter granskas och hur telekombolagen ser på saken om sitt ansvar.

Vad är det för verksamhet som skulle vara så samhällsviktig att man måste behålla möjligheten för legalt spoofade samtal? Telekombolagen skriver inte att det t.ex. bara skulle gälla telemarketing via call-center från utlandet. Det är därför lite oklart vad det är för verksamhet som telekombolagen vill skydda.

PTS kan ställa tuffare krav på telekombolagen. Det övergripande kravet ska vara att stoppa illegalt spoofade samtal och SMS. Det är helt ointressant, ur ett samhällsperspektiv, hur legala spoofade samtal påverkas eller vad det skulle kosta för telekombolagen att ha tjänsten kvar.

Om en tillhandahållare inte lyckas med det så ska förslagsvis både skadestånd och sanktionsavgift kunna utkrävas, precis som vid penningtvätt.

Den vägledning för tillhandahållare²⁶ som PTS har publicerat eller de nya föreskrifterna kommer inte att lösa problemet med telefonbedrägerier. Det är tydligt att det är de globala multinationella telekomföretagen som påverkar marknaden och de slutliga godkända ECC rekommendationer som PTS följer. Det ska mycket till för att regeringsuppdraget ska kunna ändra på det även om andra länder redan gjort mer.

Föreningen mot Nätbedrägerier är därför mycket kritisk till hur PTS hanterar problemet och inte stoppar det vanligaste sättet av telefonbedrägerier via SMS.²⁷ Vi kräver att PTS lyssnar på oss brottsoffer och om det är svårt att tekniskt säkerställa att telefonnummer inte utnyttjas för telefonbedrägerier så bör PTS överväga att förbjuda tjänsten. Kravet, så att polisen kan lösa telefonbedrägerier, är att samtliga telefonnummer och SMS som har ett svenskt nummer ska vara kopplade och spårbara till en svensk person eller svenskt bolag med adress i Sverige och med en seriös huvudman.

Och vi är inte ensamma om att vilja stoppa spoofing för samtal och SMS. Även Svenska Bankföreningen har 2023 skickat en hemställan till regeringen och vill se ett stopp för spoofing.²⁸ Men det är många som ser en lagändring som enda lösning för att få banker att börja ta sitt ansvar.²⁹

Skadeståndskravet för brottsoffer vid telefonbedrägerier skulle kunna betalas ut av de inblandade bankerna och telekombolagen tillsammans.

²² [Nu stoppar telekomoperatörerna miljontals bedrägeriförsök genom "spoofing"! \(telekomradgivarna.se\)](https://www.telekomradgivarna.se/nyheter/nu-stoppa-telekomoperatorerna-miljontals-bedraegeriforsok-genom-spoofing/)

²³ [Riksdagsseminarium \(motnatbedraegerier.org\)](https://motnatbedraegerier.org/riksdagsseminarium)

²⁴ [Bankgemensamt initiativ för att förhindra telefonbedrägerier | Swedishbankers](https://www.svebank.se/nyheter/bankgemensamt-initiativ-for-att-forhindra-telefonbedraegerier)

²⁵ [Bankernas satsning mot bedrägerier sågas av expert - DN.se](https://www.dn.se/nyheter/ekonomi/bankernas-satsning-mot-bedraegerier-sagas-av-expert)

²⁶ [Vägledning för tillhandahållare \(pts.se\)](https://pts.se/tydning-och-forslag-2023-01-21)

²⁷ [Varning för telefonbedrägeri | Polismyndigheten \(polisen.se\)](https://www.polisen.se/nyheter/varning-for-telefonbedraegeri)

²⁸ [Försvåra manipulering av telefonnummer | Swedishbankers](https://www.svebank.se/nyheter/forsvara-manipulering-av-telefonnummer)

²⁹ ["Gångkriminella tillåts stjäla miljarder från bankernas kunder" - DN.se](https://www.dn.se/nyheter/ekonomi/gangkriminella-tillats-stjala-miljarder-fran-bankernas-kunder)

3. PTS vägledning

Inledning

Det är inte första gången PTS försöker stoppa manipulerade nummer som används vid telefonbedrägerier. 2019 gjordes ett pilotprojekt som inte gav någon effekt, läs mer om det i slutord.

PTS remiss

Post och telestyrelsen (PTS) skickade i september 2023 ut ett pressmeddelande,³⁰ om vägledning för tillhandahållare, rekommenderade åtgärder mot manipulering av nummer (s.k. spoofing). Som handlar om hur telefonbedrägerier skulle kunna minskas och som nu var ute på remiss.³¹ Något som flera media har rapporterat om t.ex. TV4³² och DN³³.

PTS menar att vägledningen skulle kunna minska telefonbedrägerier via spoofing påtagligt.

PTS menar också att flera andra länder infört åtgärder på liknade sätt som denna vägledning gör, utan ett ge några exempel.

Remissvar Föreningen mot Nätbedrägerier

Det var med stor förväntning som vi började granska förslaget, men som snabbt byttes ut mot stor besvikelse.

Man kan lätt få uppfattningen att PTS tillsammans med Telekområdgivarna³⁴ hade tagit fram en ny teknisk lösning som ska lösa problemet med spoofing när man läser om nyheten i media. Vilket är helt felaktigt och som vi har granskat.

Att problemet med spoofing finns överhuvudtaget beror på att det är en tjänst som telekombolagen har för företag som använder t.ex. call-center från utlandet.

Vi ansåg att förslaget riskera att vara helt verkningslöst och inte ha någon effekt alls på telefonbedrägerier och såg stora brister. Något som vi också påpekade i vårt remissvar till PTS.³⁵

PTS vägledning innehåller inget förslag för att stoppa telefonbedrägerier som genomförs så som beskrivs i inledningen.

Vi ansåg också att det var oklart vilka typer av verksamheter som berörs och vem som hade tagit fram förslaget eller på vems uppdrag, så vi bad även om ett förtydligande om det och en uppdragsbeskrivning.

Svaret vi fick var att det är PTS som tagit fram vägledningen i ordinarie linjeverksamhet och att man fört en dialog med ett antal olika operatörer, Telekområdgivarna samt Polismyndigheten. Och att för vem vägledningen gäller har förtydligats efter remissvaren.

När man läser pressnyheter från Telekområdgivarna så är det lätt att få en annan uppfattning om vem som varit drivande och tagit fram vägledningen.

Remissvar sammanfattning övriga

Föreningen mot Nätbedrägerier begärde ut alla remissvar på PTS Dnr 23-11697.

Totalt lämnades bara 15st remissvar in. En sammanställning med en kort översiktlig summering av alla remissvar finns i bilaga 2.

³⁰ [Vägledning på gång för att minska antalet telefonbedrägerier | PTS](#)

³¹ [Remiss av vägledning för tillhandahållare om skydd mot manipulering av nummerinformation \(pts.se\)](#)

³² [Nu ska spoofing stoppas \(tv4.se\)](#)

³³ [Hårdare tag mot spoofade samtal - DN.se](#)

³⁴ [Samarbete för att stoppa bedrägerier \(telekomradgivarna.se\)](#)

³⁵ [Remissvar \(motnatbedragerier.org\)](#)

Det är förvånade lite intresse, för att vara ett sådant stort samhällsproblem, och merparten vill bara skydda egen verksamhet och slippa undan kostnader och ansvar.

Av 15 svar är 4 från globala stora telekomtjänsteföretag som bara ser risker med att legalt spoofade samtal stoppas.

Det är bara 3 av de svenska operatörerna som svarar, Tre (Hi3G) saknas, och samtliga påpekar att vägledningen måste också gälla för tillhandahållare av mobiltelefonitjänster för att bli effektiv och fungera. Något som var otydligt i förslaget och även vi påpekade, som PTS också rättat till i slutliga versionen.

Telenor och Tele2 hade synpunkter på att PTS menar att de inte kunde finansiera en lösning. Framför allt Telenor påpekar att kostnader för att stoppa telefonbedrägerier framför allt kommer att gynna samhället som helhet och att det därför är rimligt att staten/PTS står för finansieringen av delar eller hela lösningen.

Bankföreningen som vill förbjuda spoofing lämnade inte in något remissvar, läs mer om det i inledningen bakgrund.

Regeringsuppdrag från Finansdepartementet

PTS får ett nytt regeringsuppdrag från finansdepartementet i december 2023 för att motverka bedrägerier genom manipulering av telefonnummer och SMS.³⁶

Att det kommer så snabbt efter att PTS precis släppt en vägledning kan inte tolkas på annat sätt än som kritik mot att PTS inte gjort tillräckligt tidigare.

4. PTS föreskrifter

Inledning

Eftersom den vägledning som PTS tog fram 2023 inte är bindande så görs de nu om till föreskrifter som föreslås träda i kraft i november 2024.³⁷ Skillnaden är att undantag för telematiktjänster tas bort, något som Tele2 påpekade i sitt remissvar på vägledningen.

Förslag på föreskrifter

Föreningen kommer att svara på PTS:s remissförslag senare, men gör några noteringar.³⁸

4 § är intressant eftersom det gäller och blockerar alla svenska telefonnummer som inte är korrekt tilldelat, oavsett om man ringer från utlandet eller inom Sverige. Något som Telenor påpekade i sitt remissvar på vägledningen.

6 § gäller bara hantering av inkommande samtal och liknar det förslag från vägledningen.

8 § För samtal inom Sverige från telefonnummer med förhöjd samtalstaxa ska det anropande numret döljas är nytt och fanns inte med tidigare i vägledningen.

Fortfarande nämns inte SMS och när man ringer upp det nummer som står angivet. Alltså det vanligaste sättet som bedragare använder. Föreskrifterna är bara utformade för att följa de nya ECC rekommendationerna och inget ytterligare.

³⁶ [Uppdrag till Post- och telestyrelsen att motverka tillvägagångssätt där elektroniska kommunikationstjänster används för att genomföra bedrägerier. - Regeringen.se](#)

³⁷ [Remiss av regler mot telefonbedrägerier | PTS](#)

³⁸ [Remiss av PTS föreskrifter och allmänna råd om användning av nummer ur den svenska telefonnummerplanen samt krav på nummerpresentation | PTS](#)

Konsekvensutredning

Till remissförslaget på föreskrifter finns och en konsekvensutredning bifogad, något som saknades när vägledningen togs fram.

Under kapitel 4 förklarar PTS vilka aktörer som kan beröras av föreskrifterna, något som saknades när vägledningen togs fram och som vi frågade efter. Det finns över 600st tillhandahållare, hur ska PTS kunna ha kontroll över att alla dessa är seriösa företag? När PTS listan av operatörer³⁹ dessutom innehåller företag med namn som kan förknippas med ett av de vanligaste sätten av telefonbedrägerier och finns med på Svensk Handels varningslista?⁴⁰

PTS anser att svenskt nummer bara ska användas i Sverige med två undantag varav ett är mobilabonnemang som fortfarande ska få användas via roaming. Men är det inte exakt det vi ser i Uppdrag gransknings reportage, killar som ringer med mobiler från Spanien? Detta undantag kräver också kontroll av vem som äger abonnemanget så det inte tillhör en mobil-målvakt, se inledning.

PTS ser risker med att vara sist om Sverige inte inför begränsningar och att telefonbedrägerier kan öka allt eftersom andra länder inför begränsningar.

Att PTS anser sig vara proaktiv för att man nu äntligen börja införa någon typ av åtgärd med nummer med förhöjd samtalstaxa är något anmärkningsvärd. Tidigare fanns samtal med taxa på 100 kr/min som sedan begränsades till 20kr/min. Att man inte ser några större problem kan beror på att man inte agera när man får in anmälan om hur det används, se förord. Varför ska det ens finnas kvar möjlighet att lura folk på pengar genom dyra samtal 2024?

PTS:s frågor till olika operatörer om konsekvensen och kostnader för spärr av fastanätsnummer visar på att det egentligen inte är svårt, kostar något eller att det ens behövs denna typ av tjänster. Att en stor aktör redan infört åtgärderna visar på andra telekombolags ovilja att lösa problemet utan bindande föreskrifter.

Att en teknisk lösning skulle vara att telefonnummer valideras genom att se på maximal eller minimal nummerlängd för Sverige, låter lite för enkelt för en bedragare att komma runt.

5. Bluff-SMS 7726

Är "nya" kortnummer 7726 för bluff-SMS en bluff eller hur är tanken att det ska lösa problemet?

Telekområdgivarna skickade ut pressmeddelande, bara någon vecka efter PTS nya vägledning, som plötsligt ska lösa bluff-SMS problemet med en helt ny metod.⁴¹

Men varför kom inte det med från början under det året som samarbetet med PTS pågick för att ta fram vägledningen och där SMS inte ens nämns? Metoden är inte heller ny, har funnits i Storbritannien under 10 år utan att ge någon större effekt.

Till att börja med så försvinner informationen om vem som har skickat bluff-SMS när man vidarebefordrar ett meddelande till 7726, bara innehållet skickas vidare. Om det inte är ett för långt meddelande med länkar dvs ett MMS, för då går det inte ens att vidarebefordra meddelandet utan att först ta bort text och länkar så att det blir ett SMS (Tele2).

Vi har provat att skickat ett bluff-SMS från BankID till 7726 (Telenor) där man skulle ringa ett 08 nummer om något var fel. Det liknar många av de exempel som finns på Råd & Röns hemsida under Bluffvarningar/Falska SMS, till och med samma nummer som visas. Se även exempel från SEB i inledningen.

Genom att söka på numret i meddelandet så hittar man även företaget som ligger bakom och på tidningen PC för alla:s eforum från 2021 kan man läsa i en chatt som handlar om dem och hur de håller på med telefonbedrägerier och flera som gjort polisanmälan utan att något händer.

Företaget bedriver call-centerverksamhet men har också kopplingar till andra företag med säkerhetssystemtjänster som larm och ID-skydd.

³⁹ [Operatörer | PTS](#)

⁴⁰ [Tre nya bolag åkte upp på Varningslistan under januari - Svensk Handel](#)

⁴¹ [Tillsammans bekämpar vi sms-bedrägerier med ny metod! \(telekomradgivarna.se\)](#)

Så vad tillför bluff-SMS 7726 informationen när alla företag och myndigheter redan varnar för bluff-SMS, oftast det första man ser när man går till deras hemsida?

Enda sättet att stoppa telefonbedrägerier är att blockera massutskicka av illegala spoofade bluff-SMS, något som Finland har infört.

6. Globalt problem

CEPT och ECC

Problemet med spoofing är globalt och finns i hela världen.

CEPT (European Conference of Postal and Telecommunications Administrations) är en organisation som samlar regleringsmyndigheter inom post- och telekomsektorn i Europa och som givit ECC (Electronic Communication Committee) i uppdrag att ta fram rekommendationer.

Problemet med en allt för flexibel möjlighet att visa annat telefonnummer den s.k. Calling Line Identification (CLI) uppmärksammades redan 2016 i ECC report 248⁴² och 2022 i ECC report 338⁴³ där man kan läsa följande:

*ECC Report 248 "Evolution in CLI usage – decoupling of rights of use of numbers from service provision" [2] contains further information on flexible CLI usage, **which has advantages for end-users when it is not used with malicious intent**. This Report recommends that CLI validation techniques should be made mandatory. The alternative operator should provide validation measures ensuring that the end-user has the right to use the number presented as CLI.*

Den vägledning som PTS tog fram utgår från de nya ECC rekommendationer⁴⁴ (Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers) som nu är fastställda för inkommande telefonsamtal, några meningar under punkt 1a, 1b och 1c. Resten av dokumentet är egentligen bara information och beskriver 6 olika scenarier som behöver kunna hanteras för att inte stoppa legala samtal.

En intressant hänvisning är även till ECC rekommendationer⁴⁵ från 2019 (Measures for increasing Trust in Calling Line Identification and Originating Identification) dvs att användare ska ha tillit att använda telefoni. Oklart om PTS gjorde någon åtgärd när dessa kom?

Det pågår nu ett arbete inom ECC med rekommendationer för SMS Sender ID (ECC Recommendation on SMS SenderID)⁴⁶, något som Finland redan infört åtgärder för.

Finland

PTS nämner Finland i konsekvensanalys men har ingen hänvisning, den hittar man i Bankföreningens hemställan.

Finland har redan infört föreskrifter, november 2023,⁴⁷ för att stoppa spoofing och använder proxyserver som lösning för roamingkontroll av mobilsamtal. PTS nämner inte att Finland även infört lösning för SMS.⁴⁸

Norge

PTS nämner Norge i sin konsekvensanalys men har ingen hänvisning till vad och det går inte att hitta någon information om vad de gjort, förutom från Telenor.

⁴² [ECC Report 248 \(cept.org\)](#)

⁴³ [ECC Report 338 \(cept.org\)](#)

⁴⁴ [ECC Recommendation \(23\)03 \(cept.org\)](#)

⁴⁵ [ECO Recommendation \(19\)03 \(cept.org\)](#)

⁴⁶ [ECC WorkProgram Database \(cept.org\)](#)

⁴⁷ [Sökresultat | Traficom](#)

⁴⁸ [Skydd av avsändaruppgifterna i textmeddelanden.pdf \(traficom.fi\)](#)

Storbritannien

PTS nämner Storbritannien i sin konsekvensanalys men har ingen hänvisning. Går att tolka som att de infört liknande lösning som Finland.

Det var redan 2014 som Storbritannien införde möjligheten att skicka bluff-SMS till 7726.⁴⁹

Ändå rapporteras att 8 av 10 är omedvetna om att numret finns enligt Ofcom:s undersökning och det är tveksamt om det alls gjorts någon skillnad i en artikel från 2022.⁵⁰

Eftersom alla försök att stoppa spoofing i Storbritannien hittills varit verkningslösa så ändra man nu lagen så att banken blir ersättningsskyldig.⁵¹

Australien

PTS nämner Australien i sin konsekvensanalys men har ingen hänvisning. Går att tolka som att de infört liknande lösning som Finland.

Malta

Fler frågor uppstår när man läser ett liknade förslag för att stoppa telefonbedrägerier från Malta,⁵² jämfört med den vägledning som PTS tagit fram för att försöka stoppa spoofing. Ett mycket mer detaljerat förslag där man tar problemet på ett större allvar och visar på de tekniska svårigheterna med att stoppa bedrägerierna via både samtal och SMS.

Att kunna skilja på legala eller illegalt spoofade telefonnummer.

It is recognised, however, that the task of distinguishing between legitimate and illegitimate calls is challenging, particularly given that malicious actors use the same, or very similar, tools that facilitate legitimate calls.

7. Alternativa lösningar

Inledning

Denna rapport innehåller ett stort antal källor utan att det direkt finns några bra förslag på lösningar som skulle kunna skilja på legala och illegala spoofade samtal. Bara exempel på försök och åtgärder som hittills inte haft så stor effekt. När är det dags att inse att förbjuda alla manipulerade nummer är enda lösningen?

PTS förslag

PTS:s konsekvensanalys har ett kapitel 3.3 Alternativa lösningar och effekter om någon reglering inte kommer till stånd, som märkligt nog inte innehåller några alternativa lösningar?

Så slutsatsen är att proxyserver, som flera länder redan infört, är enda realistiska förslaget och gäller då bara för mobilsamtal och inte SMS.

STIR/SHAKEN

Det som nämns som en framtida teknisk lösning i flera remissvar är att använda STIR/SHAKEN-skydd.⁵³

⁴⁹ [Reporting Spam Text Messages to the 7726 short code. \(youtube.com\)](https://www.youtube.com/watch?v=7726)

⁵⁰ [Don't delete scam texts - send them to 7726 and become a scambuster | This is Money](#)

⁵¹ [I Storbritannien kommer banker stå för bedrägerinotan - DN.se](#)

⁵² [Malta: MCA publishes consultation paper for preventative measures for CIL spoofing and vishing scams | News post | DataGuidance](#)

⁵³ [Combating Spoofed Robocalls with Caller ID Authentication | Federal Communications Commission \(fcc.gov\)](#)

Ett regelverk som håller på att tas fram av amerikanska FCC. Förkortningarna betyder på engelska "Secure Telephone Identity Revisited (STIR)" och "Signature-based Handling of Asserted Information Using toKENS (SHAKEN)".

Säkra samtal

PTS:s konsekvensanalys nämner alla fördelar för kommuner och samhälle i kapitel 6.9 och 6.10 och hur viktigt det är att ha tillit för telekommunikation. Man ger exempel på hur kommuner och regioner redan gynnas positivt eftersom deras fasta telefonnummer inte längre kan spoofas från utlandet.

Men för övrigt nämner man inte riktigt hur tilliten skulle kunna bli bättre i praktiken för företag som behöver ringa upp personer i tjänsten eller för personer som inte har någon tillit kvar efter att varit utsatt för bedrägerier.

En lösning på det skulle kunna vara att båda parter får legitimera sig på ett säkert sätt dvs även banken eller t.ex. telekombolagens kundtjänst eller annan kundservice. Något som branschorganisationen Kontakta nu kräver i ett eget regelverk som etniska regler.⁵⁴

Säkra Samtal by twopart ID⁵⁵ är en teknisk lösningen som kontakta rekommenderar.

8. Slutord

Störst möjlighet för att stoppa bedrägerier har bankerna genom att införa några dagars fördröjning på allt man idag snabbt kan ändra via sin mobil med BankID, t.ex. beloppsgränser, nya mottagare och större transaktioner.

Men telekombolagen har också ett stort ansvar eftersom deras tjänster gör det så enkelt för bedragaren att komma i kontakt med lämpliga brottsoffer.

Ingen skulle bli gladare än vi i Föreningen mot Nätbedrägerier om alla åtgärder som Banker, BankID, PTS och telekombolagen infört under 2023 hade någon effekt så att antal bedrägerier minskar och att PTS:s vägledning⁵⁶ och 7726⁵⁷ för bluff-SMS fungerar på riktigt.

Men tyvärr är risken stor att det blir som senast PTS försökte stoppa spoofing med en spärrlista,⁵⁸ som infördes 2019 och hanteras av SNPAC (Swedish Number Portability Administrative Centre), dvs helt verkningslöst.

Något som visar sig från statistiken från Brå och Polisen som kom 18 april. För antal telefonbedrägerier för kvartal 1 2024 har inte minskat jämfört med kvartal 1 2023! Efter alla åtgärder och den uppmärksamhet som telefonbedrägerier har fått i media efter Uppdrag granskningens program så är det nu dags för svenska myndigheter att ta problemet på ett större allvar och lyssna på oss brottsoffer.

⁵⁴ [Etiska regler - praxis för trygga kundkontakter - Kontakta](#)

⁵⁵ [Företag - Säkra Samtal DEV \(sakrasamtal.se\)](#)

⁵⁶ [Bakslag för telefonbedragarna – ny metod stoppar 50 000 bedrägeriförsök varje dag - P4 Jönköping | Sveriges Radio](#)

⁵⁷ [Hit skickar du dina bluff-sms – nytt nummer ska stoppa bedrägerier - P4 Jönköping | Sveriges Radio](#)

⁵⁸ [Spärrlista PowerPoint-presentation \(pts.se\)](#)

Bilagor

9. Bilaga 1

Brå statistik anmällda brott Social manipulation.⁵⁹

Anmällda brott	Brottsförebyggande rådet								
	2022	2022	2022	2022	2023	2023	2023	2023	2024 prel.
	Kvartal 1	Kvartal 2	Kvartal 3	Kvartal 4	Kvartal 1	Kvartal 2	Kvartal 3	Kvartal 4	Kvartal 1
	Antal	Antal	Antal	Antal	Antal	Antal	Antal	Antal	Antal
Hela landet									
8-12 kap. Brott mot förmögenhet									
9 kap. Bedrägeri och annan oredlighet									
Bedrägeri inkl. grovt, bedrägligt beteende (1-3 §)									
Bedrägeri genom social manipulation (fr. o. m. 2019)	7712	8091	8939	10315	11693	11015	12776	12042	12605
Romansbedrägeri	304	338	367	303	335	302	351	330	320
Investeringsbedrägeri	494	485	715	872	1154	889	977	941	875
Befogenhetsbedrägeri	2444	2705	2685	2888	2944	2673	3571	3124	3529
Social manipulation av annan typ	4470	4563	5172	6252	7260	7151	7877	7647	7881

Anmällda brott	Brottsförebyggande rådet						
	2017	2018	2019	2020	2021	2022	2023
	Helår	Helår	Helår	Helår	Helår	Helår	Helår
	Antal	Antal	Antal	Antal	Antal	Antal	Antal
Hela landet							
8-12 kap. Brott mot förmögenhet							
9 kap. Bedrägeri och annan oredlighet							
Bedrägeri inkl. grovt, bedrägligt beteende (1-3 §)							
Bedrägeri genom social manipulation (fr. o. m. 2019)	..	126	14760	18219	24446	35057	47526
Romansbedrägeri	..	1	993	1058	1162	1312	1318
Investeringsbedrägeri	..	8	1642	1643	1899	2566	3961
Befogenhetsbedrägeri	..	21	3600	4676	6282	10722	12312
Social manipulation av annan typ	..	96	8525	10842	15103	20457	29935

⁵⁹ [Gör din egen sökning \(bra.se\)](#)

10. Bilaga 2

Kort summering av alla remissvar på PTS Dnr 23-11697. Endast 15 inlämnade remissvar av mer än 600 tillhandahållare, även om inte alla berörs enligt PTS.

Colt Technology Services, Globalt telekommunikationsföretag med huvudkontor i London. Ett engelskt dokument på 4 sidor och bifogar gemensamma synpunkter, från en grupp som kallas "Business Carrier Coalition" (BCC) som består av Colt, Lumen, Orange Business och Verizon, på det utkast från ECC på rekommendationer om hur spoofing kan stoppas. Som Colt rekommenderar PTS att läsa noga. Colt ser risker med att legalt spoofade samtal blockeras redan från 5 december av fyra svenska telekomföretag. Påpekar att mobilnummer används oftare för bedrägerier.

Konsumentverket, två meningar i ett mejl. Välkomnar PTS insatser men har svårt att bedöma undantagen. Hoppas att spoofade samtal hindras så långt det är möjligt.

Microsoft Ireland Operation Limited, 6 sidor. Ser problem för sin tjänst Microsoft Teams Meetings, för de som ringer in, och Skype VoIP-till-PSTN samtalstjänst. Att förslaget riskerar "oavsiktligt skada svenska användare genom att störa legitima affärsmodeller". Föreslår som en framtida teknisk lösning att använda STIR/SHAKEN-skydd.

Polismyndigheten NOA, svara med ett mejl på 1 sida. Ett steg i rätt riktning men påpekar att det skulle vara önskvärt att SMS omfattades eftersom det är ett större problem. NOA ifrågasätter att spoofing skulle minska påtagligt enligt förslaget, men saknar tillräckliga kunskap för att bedöma effekten för spoofade röstsamtal. NOA har inga belägg för att inhemska aktörer ringer från utlandet. NOA vill gärna veta hur arbetet med SMS Sender ID går.

Polismyndigheten Rättsavdelningen, har inga invändningar mot förslaget.

Privatperson 1, uppfattar förslaget som bra och ger tummen upp. Ger förslag på en tjänst "vit-lista" för mobilen att kunna blockera landsnummer själv.

Privatperson 2, påpekar att lösningar sedan länge finns i andra länder och att förslaget bara stoppar spoofade svenska nummer från utlandet, inte utländska spoofade nummer. Ger förslag på Call filter app. Nämner exempel Wangiri samtal. Nämner även att USA infört STIR/SHAKEN och en app från Vimla.

Teknikföretagen, 1 sida. Nämner att cyberkriminalitet och spoofing en utmaning för Teknikföretagens medlemmar. Spoofing används av kriminella i kombination med andra digitala verktyg för att störa verksamheter eller stjäla tillgångar. Har inga invändningar mot förslaget som ett första steg att komma till rätta med brottslig verksamhet genom digital teknik.

Tele2, 2 sidor med 6 synpunkter. Vill bland annat tydliggöra att det även måste gälla för alla mobiloperatörer, inte bara "tillhandahållare", om det ska fungera för mobiltelefonitrafikfall. Ta bort undantag för telematiktjänster. Delar inte PTS:s bedömning att PTS inte skulle kunna finansiera en lösning som ska motverka spoofing.

Telenor, 4 sidor. Anser att vägledningen och kommande föreskrifter även ska gälla för mobiloperatörer. Påpekar att ett av undantagen, för call-center utomlands, snarare är en lösning för kunder som har en "felaktig" lösning utomlands. Anser att det är rimligt att staten/PTS är med och finansierar lösningar, till exempel proxyserver, då det framträdande intresset är att skydda svenska konsument, företag och myndigheter. Uppmärksammar PTS på att spoofing även förekommer inom Sverige och menar att det inte ska få förekomma oannonserad manipulering av nummer och adresser mellan svenska operatörer.

Telia, en halv sida och i huvudsak inga synpunkter. Påpekar att det kan finnas mobiloperatörer som också måste vara reglerade för att det ska fungera. Påpekar att PTS förslag på undantag är inget undantag utan en beskrivning på hur man kan undgå blockering.

Trafikverket, en halv sida och i huvudsak inga synpunkter.

Twilio Ireland, 6 sidor på engelska. Tillhandahåller molnbaserade kommunikationstjänster i Sverige. Ser en risk med att legala spoofade samtal blockeras. Vill se undantag för legala spoofade användningsområden. Hänvisar till andra pågående regleringsförslag som Ofcom, ComReg och CEPT tar fram.

Verizon, 3 sidor på engelska. Amerikanskt globalt kommunikationsföretag med svensk VD. Vill ha förtydligande på definition av "fixed number" och tolkning hur "2 CLI functionality" ska hanteras. Anser att det är viktigt att deras kunder får visa att svenskt nummer även om man ringer från utlandet.

Rekommenderar en gemensam proxy-server för att lösa mobilnummer. Ser risker med att legalt spoofade nummer blockeras. Vill se en flexibel och gradvis gemensam implementering i hela EU. Mycket gemensamt med bilagan som Colt lämnade in.

Föreningen mot Nätbedrägerier, 5 sidor och remissvaret går att ladda ner från föreningens hemsida. Vi är kritiska till hela förslaget och ser inte att det kommer att ha någon effekt på telefonbedrägerier.