

2026-05-21

Sveriges riksdag  
*Trafikutskottet*

## Framställning om försvårande av bedrägeri-SMS och bedrägliga webbplatser

Svenska Bankföreningen hemställer om att riksdagen vidtar åtgärder för att stoppa bedrägeri-SMS. Detta genom inrättande av ett centralt register för avsändarinformation och en infrastruktur inspirerad av den finska lösningen, som på ett effektivt sätt identifierar och blockerar bedrägeri-SMS.

Förslagen enligt denna hemställan är att

Riksdagen tillkännager att regeringen bör utreda ärendet på nytt i syfte att

1. Inrätta ett obligatoriskt register för avsändarinformation avseende SMS (SMS Sender ID). Registret ska föras av Post- och telestyrelsen.
2. Teleoperatörerna ska säkerställa att avsändaruppgifterna i SMS från företag och organisationer till konsumenter är korrekta.
3. Teleoperatörerna ska identifiera avsändaren på ett tillförlitligt sätt.
4. Teleoperatörerna ska blockera SMS i vissa fall.
5. Teleoperatörerna ska blockera bedrägliga bankwebbplatser i vissa fall.
6. Teleoperatörerna ska i annat fall blockera nummerpresentationen och tilldela SMS avsändarnamn "spam".
7. Post- och telestyrelsen ges lagstöd att föreskriva eller genomföra åtgärderna enligt p 1-6.

### Bakgrund

Det har under senare år blivit ett omfattande samhällsproblem att den organiserade brottsligheten använder sig av s.k. spoofing via telefon eller SMS. SMS-spoofing innebär att någon manipulerar avsändaruppgifterna för SMS:et, så att detta verkar ha skickats från en legitim och känd avsändare, som till exempel en bank eller en myndighet. SMS:et ser äkta ut på alla vis.

För den enskilde som tar emot ett SMS som innehåller falska avsändaruppgifter kan det därför vara mycket svårt att inse att meddelandet i själv verket utgör ett led i ett bedrägeri. I vissa fall kan till och med ett enskilt SMS sorteras in i en tidigare SMS-tråd, där den enskilde har haft en verklig kommunikation med till exempel sin bank.

Vikten av en tillförlitlig SMS-trafik kan inte överskattas, vilket gäller både avseende avsändarinformation och innehåll. SMS utgör en grundläggande informationsbärare som används brett i samhället av såväl privata som statliga aktörer, till exempel i samband med krissituationer. SMS är sedan några år den vanligaste första kontaktvägen vid telefonbedrägeri. SMS fungerar ofta som en "trigger" för modus kopplat till social manipulering eftersom sms:et skapar en känsla hos mottagaren att något behöver göras skyndsamt.

Det är rimligt att påstå att all den bedrägliga SMS-trafik som har drabbat den svenska befolkningen under senare år starkt har underminerat förtroendet för telekombranschen. Både banker och myndigheter behöver kontakta sina kunder / medborgare och vi behöver skydda pålitligheten. Denna förtroendebrist drabbar i sin tur alla företag vars varumärke utnyttjats av den organiserade brottsligheten. Slutligen drabbas de enskilda som luras på pengar eller andra tillgångar.

I många fall är det genom utredning och andra åtgärder mycket svårt att identifiera, spåra och lagföra dem som använt spoofing för att begå brott. De befinner sig inte sällan i utlandet och verkar överhuvudtaget i det fördolda. Även om det i många länder ställs krav på att användare av telefonnummer och teletjänster är registrerade, är kraven ofta enkla att frångå genom till exempel använde av målvakter.

Enbart proaktiva åtgärder kan på ett effektivt sätt stoppa SMS-spoofing.

Genom denna framställning vill Svenska Bankföreningen få ett slut på SMS-bedrägerierna samt återställa förtroendet för SMS-trafiken i Sverige. Det ska åter vara möjligt att lita på att SMS verkligen kommer från den avsändare som anges. Är avsändaren okänd ska SMS antingen blockeras eller tilldelas en tydlig varning till konsumenten.

### **Propositionen "Nya regler mot bedrägerier och annat vilseledande genom elektroniska kommunikationer" (2025/26:233)**

Svenska Bankföreningen välkomnar att regeringen genom rubricerad proposition (nedan; propositionen) den 9 april 2026 verkar för att vidta ytterligare åtgärder för att motverka telefonbedrägerier genom SMS-spoofing samt att Post- och telestyrelsen (PTS) ges bemyndigande att meddela korresponderande föreskrifter.

Förslaget enligt propositionen går i huvudsak ut på att det överlämnas åt tillhandahållarna (nedan; operatörerna) på marknaden att själva utforma anpassningen av åtgärder med utgångspunkt i det som bedöms vara mest ändamålsenligt för att uppnå föreskriven effekt. Därutöver ges PTS bemyndigande som ger möjlighet att vidta åtgärder i form av ett frivilligt register för anmälda avsändarnamn för SMS.

Sammanfattningsvis är det svårt att se att dessa åtgärder effektivt kommer att sätta stopp för SMS-spoofing, vilken inte sällan drabbar Sveriges äldre befolkning.

Även om förslagen enligt propositionen har fördelar i form av till exempel flexibilitet genom att lämna till operatörerna att bedöma vilka åtgärder som kan vara effektiva, finns stor risk för att en bristande enhetlighet. Om inte en gemensam standard införs via lag är risken stor att vissa operatörer vidtar mer effektiva åtgärder än andra. Det blir även en fråga om företagets olika prioriteringar och förutsättningar att avdela resurser, vilket typiskt sett ger fördelar för större operatörer och försvårar för de mindre. Det är även rimligt att föreställa sig att det kommer ta avsevärd tid innan någon påtaglig effekt eventuellt kan påvisas.

Vidare bör det inte etableras incitament för enskilda operatörer att konkurrera med argument om snabba och enkla processer på bekostnad av kontroll och säkerhet.

Förslaget enligt propositionen lämnar därmed stort utrymme för variationer och bedömningar i implementeringen och verkställigheten av åtgärder.

Vad som anses utgöra avvikande trafikmönster kommer vidare att bedömas på olika sätt av olika operatörer. Detta gagnar knappast regleringens syften och framstår inte heller som fördelaktigt för telekombranschen. Regleringen blir svårtillämpad och resultatet oförutsebart.

Vidare förefaller det svårt för en operatör att bedöma vad som utgör ett led i ett bedrägeri eller har ett syfte att vilseleda en vidare krets av mottagare. Det är rimligt att föreställa sig att det i många fall saknas konkreta omständigheter som talar tillräckligt starkt i endera riktningen. Detta bland annat mot bakgrund av att informationsmängden eller datapunkterna i teletrafiken (teletrafikuppgifterna) är relativt få<sup>1</sup> för att kunna genomföra en bedömning med tillräcklig precision.

Av relevans är även att operatören inte får granska innehållet i ett meddelande, vilket skapar svåröverskådliga begränsningar av bedömningsunderlaget.

---

<sup>1</sup> I jämförelse med till exempel den informationsmängd som ett kreditinstitut har tillgång till vid sin transaktionsövervakning.



Det finns vidare risk att den föreslagna ordningen öppnar upp för mindre nogräknade operatörer som verkar på den svenska marknaden och som sätter egna affärsintressen framför samhällets intressen av att begränsa spoofing. Om en operatör inte tar tillräckligt ansvar och avsätter tillräckliga resurser skapar detta risker för andra aktörer och konsumenter.

En ytterligare aspekt är att tillsyn är svår att genomföra när det saknas en tydlig kravbild att relatera till. Att operatörerna är skyldiga att anpassa sina åtgärder med utgångspunkt i vad de bedömer som mest ändamålsenligt, utgör komplicerade premisser för en tydlig, förutsebar och effektiv tillsyn.

### **Ett obligatoriskt register**

Regeringen har, såsom det får förstås, valt att i propositionen inkludera frågan om inrättande av ett frivilligt register med avsändarinformation för SMS, genom att ge PTS utökad föreskriftsrätt.

För en effektiv ordning som undanröjer alla oklarheter och risker som angivits i föregående avsnitt, behöver dock tydliga direktiv ges om att ett centralt register ska införas. Farhågor om bland annat oförutsebara och svårimplementerade åtgärder i telesystemen, med sinsemellan skilda förutsättningar mellan operatörer, blir därmed irrelevanta. Spelplanen blir i stället likadan för alla berörda parter och konsumenterna kan lita på att bedrägeri-SMS alltid blockeras eller tydligt markeras.

För att ett centralt register ska vara tillförlitligt och effektivt krävs att registrering av avsändaruppgifter för företag och organisationer är *obligatorisk*. Det innebär att registret<sup>2</sup> kommer att utgöra en förutsättning för att dessa aktörer överhuvudtaget ska ha möjlighet att kommunicera med konsumenter via SMS.

Det obligatoriska registret kan lämpligen föras av PTS som, om kompletterande lagstöd behövs, bör ges sådant.<sup>3</sup>

Den övergripande systematiken, vilken framgår ovan enligt p 1-4 och 6, utgår ifrån skärpta krav på avsändaridentifiering. För det fall registrering inte skett ankommer det på operatören att per automatik vidta åtgärder för blockering av SMS eller annars varna mottagaren genom angivande av "spam" som avsändarnamn. Alfanumeriska

---

<sup>2</sup> Efter en övergångsperiod inom vilken företag och organisationer har möjlighet att anmäla sig till registret vid äventyr av att deras SMS blockeras eller markeras som "spam".

<sup>3</sup> Av propositionen förefaller framgå att krav på åtgärder för blockering i enlighet med denna framställning är så ingripande att dessa ställs genom författning. Denna framställning utgår således från att så är fallet. För det fall PTS med stöd av föreslaget bemyndigande utan uttryckligt författningsstöd kan inrätta ett *obligatoriskt* register och i övrigt föreskriva i enlighet med framställningen välkomnas detta.

Sender ID:s ska fortsatt vara tillåtna, men måste vara tydligt kopplade till avsändarens namn, varumärke, domän eller lagliga verksamhet.

Om så inte bedöms vara fallet ska PTS inte registrera numret. Närliggande namn där man till exempel avsiktligt utlämnat eller ändrat en bokstav (s.k. typosquatting), kommer av naturliga skäl att blockeras. Den föreslagna ordningen innebär att alla operatörer omfattas av samma kravbild och därmed tydligt kan avgöra vilka åtgärder som behöver vidtas för att stoppa SMS-spoofing. Dessa åtgärder kan förväntas vara betydligt enklare och mer kostnadseffektiva i jämförelse med propositionens förslag.

Värt att påtala är även att införande av ett obligatoriskt register medför att det saknas anledning att granska innehåll i SMS<sup>4</sup>, vilket annars hade varit önskvärt för att uppnå tillräcklig effektivitet.

En ordning med ett *frivilligt register* riskerar att lämpa över ansvaret på konsumenten på ett sätt som kan förväntas vara ineffektivt och betungande. Det bygger på konsumentens aktivitet, med kännedom om registret som premiss.

Med en frivillig registrering är det vidare svårt att se vad registret skulle tillföra i de fall en SMS-avsändare inte förekommer, mer än att det i bästa fall innebär någon form av indikation för konsumentens fortsatta egna efterforskningar. Det har inte framkommit något som talar för att PTS kommer att ålägga operatörerna att tilldela samtliga SMS vars avsändarnamn inte förekommer i registret avsändarnamnet "spam" eller motsvarande. Även om så vore fallet skulle det inte ersätta den automatiska blockering som följer av en obligatorisk registrering.

Mot bakgrund av ovanstående och sett i ljuset av vikten av att effektiva åtgärder mot SMS-spoofing vidtas i närtid, bör riksdagen tillkännage att regeringen ånyo bör utreda frågan med utgångspunkt i nu föreslagna åtgärder.

### **Den finska regleringen och den finska blocklistan**

I detta sammanhang är värt att notera att Finland sedan flera år är ett föregångsland inom EU när det gäller att bekämpa telefonbedrägerier, spoofing och phishing från bedrägliga webbplatser med hjälp av telereglering och teletekniska lösningar.

Svenska banker tar idag ned falska hemsidor på löpande band. Det finns ofta en fördröjning i processen innan webbplatsen går ner och kriminella känner till svagheterna i nedtagningsprocessen. Den första dagen av bedrägerivågen är den

---

<sup>4</sup> En sådan granskning kräver samtycke från användaren/konsumenten, och omfattas inte av propositionens förslag, som utgår från att innehåll i SMS inte får granskas i syfte att upptäcka bedrägerier.



mest kritiska och trots att svenska banker använder operatörer som specialiserar sig på nedtagningar kan det dröja 1–3 dagar och ibland kan det ta längre tid.

I Finland genomfördes ett pilotprojekt våren 2025 mellan en av de stora teleoperatörerna och en av de stora bankerna. Syftet var att testa hur en teleoperatör kunde blockerade trafik till bedrägliga bankwebbplatser. Det fungerade så att banken försåg teleoperatören med uppgifter om bedrägliga bankwebbplatser (var 15:e minut) och att teleoperatören därefter blockerade trafik till de webbplatserna.

Under pilotprojektet (en månad) noterade de finska bankerna en minskning av antalet bedrägerioffer på cirka 50 %. Efter en månad avslutades pilotprojektet och då gick antalet offer tillbaka till de tidigare siffrorna. Typiskt antal offer var hundratals personer per vecka i Finland.

Ur ett tekniskt perspektiv var pilotprojektet en succé. När en webbadress fanns med på listorna blockeras trafiken till den snabbt. Under pilotprojektet våren 2025 lades 159 webbplatser till i listan och listans storlek varierade under projektets gång mellan 10 och 37 adresser.

Blocklistor är effektivt mot bedrägliga massutskick som görs via olika kanaler (e-post, SMS, Facebook- och Instagram-annonser etc.). Det stoppar inte alla bedrägerier men minskar avsevärt livslängden för attackerna. Risken för så kallade "false positives" kan minskas genom manuell validering innan de läggs till i blockeringslistan. Under pilotprojektet fanns processer för att säkerställa att inte genuina webbplatser flaggades som bedrägliga.

Efter pilotprojektet fortsatte arbetet med att få lösningen i produktion vilket den gjorde hösten 2025 för banker och teleoperatörer. Idag täcker lösningen cirka 90 % av den finska befolkningen (internetanslutningar). Bedrägliga webbplatser ligger i snitt kvar på blockeringslistan i mellan 12 timmar och 5 dagar.

Bedömningen är att cirka 300 000 anslutningsförsök blockerades (till bedrägliga bankwebbplatser) bara i januari 2026. Bankerna noterade en betydande minskning av antal offer (cirka 50 %) för denna typ av bedrägerimodus. I Finland kan de konstatera att metoden har fungerat väldigt väl och har förebyggt många brott, något likande är önskvärt i Sverige.

Den 4 maj 2026 trädde även en finsk reglering om åtgärder mot SMS-spoofing i kraft.<sup>5</sup> Förslagen enligt denna framställning har den finska regleringen som förebild.

---

<sup>5</sup> Traficom, Order 28 L/2025.



De samlade erfarenheterna är att de åtgärder som hittills vidtagits i Finland inte varit alltför administrativt betungande, kostsamma<sup>6</sup> eller integritetskränkande. Åtgärderna har inte stoppat bedrägerier helt och hållet men förtroendet har stärkts. Fördelarna uppväger med råge eventuella nackdelar. Det saknas anledning att anta att den nya finska regleringen om SMS-spoofing skulle få ett annat utfall, vilket gäller i såväl Finland som Sverige.

SVENSKA BANKFÖRENINGEN

  
Hans Lindberg

  
Peter Göransson

  
Erik Wendeby

---

<sup>6</sup> En premis för ett rimligt kostnadsläge torde vara reglerade avgifter för registrering.