BRANSCH-
ORGANISATIONEN
MORGAN

Branchorganisationen MORGAN

Motverka falska SMS-avsändare

BRANSCH-
ORGANISATIONEN
MORGAN

Versioner

Version	Förändring	Datum
1.0	Morgans förslag för att motverka användningen av falska SMS-avsändare i bedrägligt syfte.	2025-12-18

BRANSCH-
ORGANISATIONEN
MORGAN

Innehåll

BRANSCH-
ORGANISATIONEN
MORGAN

Bakgrund

Branschorganisationen MORGAN representerar Sveriges aggregatörer och operatörer som är verksamma inom den mobila tjänstesektorn. MORGAN tar tillsammans med operatörerna och Telekområdgivarna fram gemensamma regler och riktlinjer för att främja en sund och hållbar marknad.

Som en del i PTS arbete med att stoppa bedrägerier där elektroniska kommunikationstjänster används avser PTS reglera användningen av alfanumeriska avsändare (Sender ID) i trafikfallet A2P (Application-to-Person) SMS. En alfanumerisk avsändare är ett kort namn som visas i stället för ett telefonnummer när företag, myndighet och andra aktörer kommunicerar med exempelvis konsumenter och anställda. Det korta namnet som identifierar en avsändare kan relativt enkelt användas av obehörig i bedrägligt syfte.

A2P SMS används dagligen av tusentals företag och organisationer i Sverige. Till skillnad från P2P (Person-to-Person) SMS, vars volym minskar som en följd av ökad användning av applikationer som WhatsApp, Messenger med flera, ökar användningen av A2P SMS. A2P kommunikation är ofta verksamhetskritiskt och handlar inte sällan om larm, påminnelser om läkarbesök, avisering om försändelser med mera. Användningsområdet är brett.

MORGAN vill med detta dokument föreslå en lösning för att skydda alla legitima avsändare (alfanumerisk och numerisk) som används för A2P SMS. Lösningen har fokus på att förhindra bedrägerier samt att tillgodose marknadens fortsatta behov av A2P SMS och den enkelhet som präglar användningen idag.

Rekommendationer till PTS

MORGAN har tagit del av PTS arbete med att förstå problematiken med alfanumeriska avsändare i A2P SMS samt de influenser man tagit av reglering i andra länder och vill mot denna bakgrund att PTS tar del av följande information och rekommendationer:

- I Sverige skickas cirka 4 miljarder A2P SMS per år, merparten, i stort sett samtliga SMS, är legitima och affärskritiska. Fokus bör därför läggas på att stävja den trafik som inte är legitim, utan påverkan på den legitima trafiken.

- Större fokus bör också riktas mot andra typer av bedrägeri såsom SIM-farmar, GT-spoofing och vishing (röst-smishing/bluff-samtal). Storbritannien har introducerat vidare lagstiftning för att förbjuda SIM-farmar och har ansetts vara mycket effektiv i kampen mot de som genererar bedrägliga SMS.

  Storbritanniens lagstiftning: https://www.gov.uk/government/news/major-step-for-fraud-prevention-with-landmark-ban-on-sim-farms

- Att blockera all A2P SMS-trafik och införa ett krav på vitlistning av avsändare kommer inte att hjälpa mot bedrägerier mer än på mycket kort sikt. En ökad användning av OTT-kanaler riskerar svenska medborgares integritet då utländska nationer får insyn i kommunikationen. Bedrägerierna kommer att flytta till andra kanaler, företrädesvis OTT-kanaler, där insyn och reglering helt saknas. Bedrägeri kommer också att flyttas till andra

operatörskontrollerade kanaler. Ett exempel på det här är på Irland där numeriska avsändare ännu är oreglerade och bedrägeri sker nu via kort- och långnummer. Regulatorn COMREG har nu ansökt om ytterligare lagförändring för att motverka detta genom att inkludera även dessa avsändare i sitt register.

- A2P SMS används professionellt av många seriösa företag och myndigheter. Att blockera A2P SMS och kräva vitlistning blir kostsamt och riskerar att få allvarliga konsekvenser då många befintliga SMS-flöden är svåra att identifiera.

- För att operatörer och aggregatörer lättare ska ha möjlighet att identifiera bedrägerier bör lagstiftningen ändras så att innehållet i SMS kan analyseras för detta syfte. SMS-aggregatörer och operatörer bör ges tillstånd att analysera meddelandeinnehåll för att identifiera vanliga bedrägerimönster (t.ex. falska bankmeddelanden eller paketbedrägerier) samt upptäcka misstänkta formuleringar, såsom bedrägliga URL:er eller suspekta språkliga mönster. Genom att använda AI- och maskininlärningsmodeller kan brandväggar ständigt förbättra identifiering av phishing, smishing och skadliga länkar, vilket möjliggör omedelbar blockering av misstänkta meddelanden innan leverans. Detta bidrar till förbättrad bedrägeriprevention, stärkt regelefterlevnad och ökat förtroende.

- Finland är på väg att införa restriktioner på SMS Sender ID. PTS rekommenderas att invänta resultatet och använda det som underlag till en svensk modell.

BRANSCH-
ORGANISATIONEN
MORGAN

Rekommenderad lösning på den svenska marknaden

Sammanfattning

MORGAN rekommenderar en lösning som bygger på den redan etablerade operatörstjänsten Sender ID Protection i Sverige, en tjänst som skyddar alfanumeriska avsändare från att utnyttjas i bedrägligt syfte. För att förenkla hanteringen av Sender ID Protection införs en central funktion för hantering av tjänsten, avsedd för aggregatörer. Vidare kommer tjänstens kostnadsbild att förändras, tjänsten ska kunna användas av både stora och små organisationer. Ett större ansvar än idag läggs på aggregatörer som har direktavtal med de svenska operatörerna, där aggregatorn aktiverar och levererar Sender ID Protection.

Sender ID Protection

Sender ID Protection är en etablerad tjänst som tillhandahålls gemensamt av de fyra mobiloperatörerna som marknadsför och säljer denna på egen hand samt genom aggregatörer. Sender ID Protection aktiveras på en alfanumerisk avsändare som används för SMS-utskick vilket godkänns genom en fullmakt / ett Letter of Authorization (LoA) undertecknad av företrädare för det aktuella varumärket. Sender ID Protection är idag en etablerad tjänst som ger ett fullgott skydd mot obehörig användning av en specifik avsändare och blockering av snarlika men vilseledande avsändare, s.k. lookalikes. Mot den bakgrunden rekommenderar MORGAN fortsatt användning av Sender ID Protection som grund. Dock krävs förändringar i tjänsten för att den ska användas brett och göra skillnad.

Gemensam funktionalitet

Sender ID Protection’s tekniska implementation och funktionalitet hos operatörerna behöver ensas på ett sätt som innebär att skyddet av en avsändare och blockering av lookalikes fungerar identiskt i samtliga mobiloperatörers nät, förslagsvis genom att samtliga operatörer inför stöd av RegEx (r*eguljära uttryck* för att matcha textmönster).

Kostnadsbild

Kostnaden för Sender ID Protection måste vara rimlig och i paritet med storleken på den organisation som vill skydda en avsändare. Här rekommenderas en kostnadsnivå och en modell som liknar den som finns i Finland.

Varje aggregator som aktiverar Sender ID Protection för ett varumärke borde bära kostnaden för detta och blir därmed likvärdigt debiterad av operatörerna. Begreppet primär och sekundär aggregator försvinner.

Central hantering

För aggregatörer med direktavtal med de svenska operatörerna tas en central webbaserad registreringstjänst fram. Denna tjänst används för att aktivera Sender ID Protection för en avsändare. Webbportalen används för att ladda upp LoA, skydda legitima avsändare, anmäla och blockera lookalikes m.m. Respektive operatör får information skickad till sig och bekräftar även införande genom portalen.

Aktivering av Sender ID Protection påbörjas av operatörerna tidigast två veckor efter det att registrering genomförts. Detta för att varumärken som använder flera olika aggregatörer ska ha möjlighet att succesivt aktivera Sender ID Protection hos dessa.

Aggregatorsspecifik registrering

Varje aggregator aktiverar Sender ID Protection utan inblandning av andra aggregatörer. I det fall ett varumärke legitimt använder flera aggregatörer aktiverar varje aggregator Sender ID Protection för dessa varumärken.

Register för skyddade Sender ID

De avsändare som av en aggregator registreras för aktivering av Sender ID Protection, placeras i ett register som exponeras för samtliga aggregatörer via en webbaserad registreringstjänst, samt via ett API. Respektive aggregator använder informationen för analys av avsändare och för att kunna avgöra om aggregatorn behöver aktivera Sender ID Protection i sina plattformar, samt beställa den av operatörerna. Aggregatorn har två veckor på sig för detta. När två veckor har gått blockeras inom ytterligare två veckor aktuella avsändare av operatörerna.

Tillgång till registret begränsas till direktanslutna aggregatörer och operatörer för att undvika att bedragare utnyttjar registret i bedrägligt syfte.

Hantering av Sender ID

Lookalikes

Alla aggregatörer och operatörer ges möjlighet att anmäla Sender ID som uppenbart används för bedrägeri. Alla aktörer kan ta del av dessa via ett API för att blocka dem i sin egen tjänst.

För generell och enklare hantering av lookalikes föreslås att operatörerna tar bort möjligheten att använda specialtecken i Sender ID. Det innebär att Sender ID bara får innehålla följande tecken: A-Ö, a-ö, 0-9 samt punkt, &, bindestreck och mellanslag. Sådan blockering innebär att färre lookalikes behöver hanteras vid aktivering av Sender ID Protection och minskar även generellt risken för bedrägerier.

För att minska antalet nödvändiga blockeringar av lookalikes föreslås även att alla typer av tecken som förekommer före och efter en avsändare som skyddas av Sender ID Protection blockeras.

Numeriska avsändare och nummeruthyrning

Det finns förutom alfanumeriska avsändare även behov av att skydda trafikfallet då ett telefonnummer (MSISDN, PSTN) används som avsändare. Tjänsten Sender ID Protection behöver kompletteras med denna funktion och att det hanteras på samma sätt som att skydda alfanumeriska avsändare.

Vidare ser Morgan ett behov av skydd för uthyrda lång- och kortnummer i operatörernas i nätverk. Aggregatörer kan idag hyra sådana nummer i syfte att tillhandahålla tvåvägskommunikationstjänster för sina kunder. I dagsläget finns det ingen metod för att hindra en annan aktör från att ta ett uthyrt nummer och begå bedrägeri via andras konnektivitet som inte är den hyrande aggregatorns.

Uthyrda kort- och långnummer bör begränsas så att enbart den som hyr numren har åtkomst. Det innebär bättre kontroll för den hyrande aggregatorn som då kan säkerställa säkerheten i egna plattformar och undvika smishing/spoofing via andra aktörer på marknaden.

Skiftlägeskänslighet

Skyddade avsändare skall registreras skiftlägeskänsliga, medan lookalikes som blockeras helt registreras utan skiftlägeskänslighet. På så sätt kan inte bedragarna kringgå blockeringen av lookalikes genom att blanda stora och små bokstäver.

Trafik

Rapportering

Det är viktigt för en slutkund att förstå effekten av skyddet. Operatörerna bör därför kontinuerligt leverera statistik till aggregatörerna som visar hur mycket trafik som blockerats.

Off-net nationell SMS-trafik

Sender ID Protection måste fungera i samtrafikgränssnittet mellan operatörerna. Off-net trafik med skyddad avsändare ska skickas till nummerägande operatör som ska terminera trafiken. Operatörerna ska därmed lita på varandra och att den trafik som erhålls är legitim.

AIT och “Traffic Pumping”

AIT står för Artificial Inflated Traffic och är en form av SMS fraud som i ekonomiskt syfte används för att generera stora mängder SMS-trafik till många olika telefonnummer. AIT är ett växande problem som aggregatörer och operatörer vill skydda sig och sina kunder ifrån.

För att ge aggregatörer och operatörer möjlighet att snabbt agera och stävja AIT föreslås att operatörerna inför felhantering som tydligt visar att ett adresserat telefonnummer saknar abonnent. Denna information kan tillsammans med andra trafikmönster användas som beslutsunderlag att blockera trafik, automatiskt eller manuellt. Ett alternativt, eller kompletterande sätt, är att operatören exponerar en funktion som kan användas för att kontrollera huruvida ett givet telefonnummer har en aktiv abonnent.

Kommentar om RCS

RCS förväntas under de närmaste åren ta över stora delar av trafiken från A2P SMS. RCS kallas SMS 2.0 och erbjuder framförallt en säkrare och rikare kommunikationsupplevelse. Då vissa telefoner saknar stöd för RCS används SMS som fallback. Mot den bakgrunden bör skydd av SMS-avsändare beaktas även vid övergång till RCS.

I RCS kan endast särskilt verifierade varumärken användas som avsändare. Därmed finns inte samma risk för bedrägerier som i SMS. Men mot bakgrund av att SMS används som fallback rekommenderas att SMS Sender ID Protection aktiveras som en del av verifieringsprocessen för RCS. På det sättet skyddas både RCS och SMS mot bedrägerier i varumärkets namn.

MORGANs medlemmar

Branschorganisationen MORGAN består av följande medlemmar på svenska marknaden.

Cellsynt AB

Generic Mobile Systems Sweden AB

Hi3G Access AB

Infobip Sweden AB

Lekab

LINK Mobility Sweden AB

NTH Mobile

ONLINECITY

Sergel Kredittjänster AB

Sinch Sweden AB

SMS-Teknik AB

Spirius AB

Talli AB

Telavox AB

Tele2

Telenor Sverige AB

Telia Sverige AB

TellusTalk AB

Twilio

Viatel

Vonage