



January 2011

Preventing SMS Spam through mobile messaging security infrastructure should be the highest priority for mobile networks, and is crucial in maintaining a trusted relationship with subscribers.

Benefits

Protect Subscribers

Subscribers react quickly to SMS and may unwittingly fall victim to malicious activity. MNOs can protect their subscribers proactively and immediately by addressing issues at a network level.

Improve Customer Satisfaction

SMS Spam is seen as a violation of customers' privacy. Empowering subscribers to report Spam will lessen frustration and improve the MNO reputation.

Gain Valuable Network Insight

MNOs can understand the nature and methods of attack on the network and quantify the volume and impact of attacks to develop more efficient security strategies.

Preserve Brand, Protect Future Revenue

MNOs can attract the highest revenues from the leading global brands with a network that is differentiated by showing security leadership.

Save on Infrastructure and Support Costs

MNOs can optimise network resources avoiding costly Spam, customer support complaints and inter-carrier billing investigations.

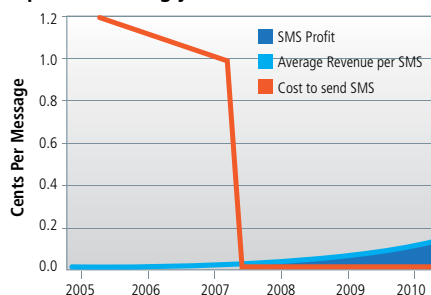
Proactive Regulation

Uncontrolled SMS Spam can lead to regulation for subscriber protection. By proactively working with regulatory bodies this can be avoided.

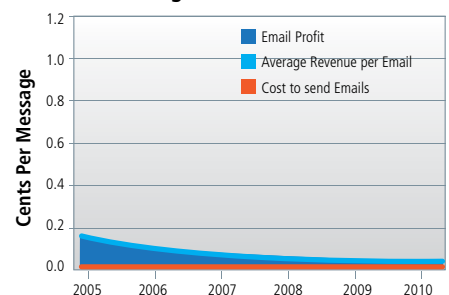
Mobile subscribers across the globe rely on their mobile network operators (MNOs) to provide them with a communications network that keeps them in touch with friends, family, colleagues and organizations they wish to interact with. Increasingly, organizations such as banks are trusting MNOs with the delivery of payment confirmations and financial fraud alerts via SMS. This trust between subscriber and MNO is becoming increasingly attractive to organizations wishing to use the mobile network as a medium for new revenue-generating services such as mobile advertising. Unfortunately, this trusted relationship also makes SMS and MMS an attractive medium for spam attacks which, potentially, could destroy that valuable relationship, severely impact a MNOs brand and cause a rise in subscriber dissatisfaction and churn.

The offering of unlimited SMS plans in most markets has resulted in SMS spam becoming economically viable, unlike traditional email spam, where profits are declining due to better defences through spam reporting and filtering. SMS messages cost milli-cents to send and, due to the trusted nature of SMS, it can yield highly profitable results. For example, in November 2010 an attacker in Australia was convicted of fraudulently receiving AUS\$4M in a dating service scam in which only 1.6M messages were sent.

Spam Increasingly Profitable in SMS

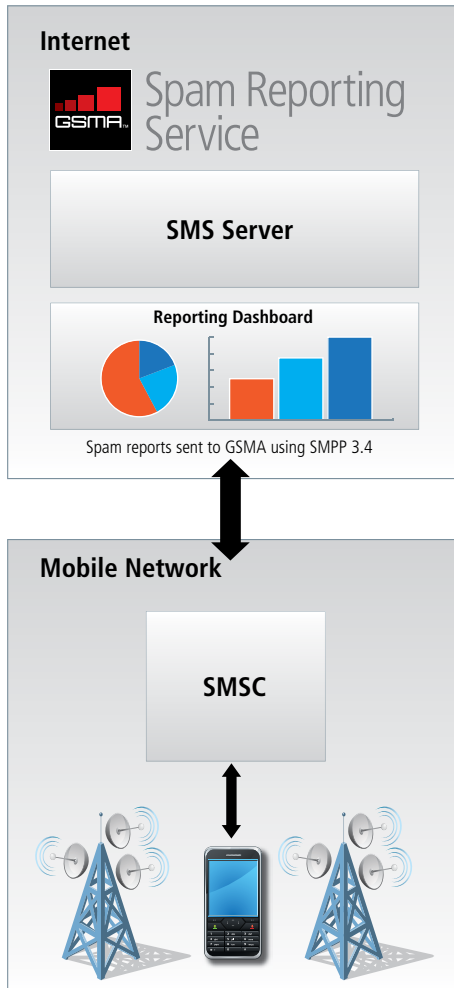


Profit Decreasing in Email



To protect MNOs and their subscribers from the threat of mobile spam the GSMA and Cloudmark have joined forces to deliver the GSMA Spam Reporting Service (SRS). A global community initiative, SRS delivers a global view of messaging attacks and insight into their messaging network usage, a key building block towards implementing effective defences. Additionally, SRS protects existing and new revenue streams, network integrity and trust, and operator brand, while increasing customer satisfaction through subscriber empowerment to easily report spam to their MNO.

GSMA SRS. How it works.



Service Integration Design

The GSMA Spam Reporting Service is an Extended Short Message Entity (ESME) connected to the SMSC using SMPP standards based protocol.

When an SMS spam message is received by a mobile subscriber, the user forwards the message to short code "7726" (or custom) along with the sender's identity (sending MSISDN or shortcode). The spam report is captured by the GSMA SRS service, added to the database and reports and analytics get updated. The user is acknowledged with a friendly message.

Features

Subscriber Interaction with Common Short Code	7726 short code message reception and interaction with subscriber handled by SRS ESME service
Mobile Attack Classification	Identify the type, level, and nature of attacks taking place on the network
Web-based Metrics and Analysis Reporting Dashboards	Insight into traffic and reports on your messaging networks across functional areas including customer satisfaction, fraud/attack analysis and operations
Global Data Correlation	Compare operator analysis and reports with those of global operators to analyze macro trends
Role-based Authentication	Policies to control visibility of SRS reports and analysis based on user
User Selectable Views	Customized reports based on origin, destination, call-to-action, attack and timeline
Simple Deployment	Standards-based SMPP enables easy integration with SMSCs. Turnkey SRS UI delivers reporting and analytics
Sender Reputation	Leverage attack correlation, top senders (MSISDN, shortcode) to deter spammers to get into the network
Raw data feed of all subscriber reports	Helps integrate this into a filtering environment.

Implementation

The SRS service is fully hosted and run on behalf of the GSMA by Cloudmark, the market leader in messaging security for network operators, so implementation is rapid and relatively light touch for the MNO. There are commonly two stages to implementation:

- MNO provisions a spam reporting capability – usually a short code (7726 or "SPAM") for subscribers to forward spam to.
- The GSMA SMS server is set up as a destination for reports

The reporting interface is browser-based and needs no integration with the MNO's infrastructure.

Typical implementation time is between 8 – 10 weeks, depending on the network bind setup.

Identify and analyse the mobile attacks

MNOs subscribing to the SRS service will receive reports and analysis of attacks both originating and terminating within their networks. This data will allow them to identify whether their current anti-spam solution is effective and then take appropriate counter-measures.

Provide a global view of messaging attacks

MNOs will have access to real-time, global data on current messaging attacks allowing them to take action before an attack impacts their network. This community approach will alert MNOs to attacks originating from within their own networks, giving them the chance to block them at source before they have restrictions imposed on them by the receiving network.

Avoid regulatory intervention by being proactive

The service proactively manages messaging attacks to prevent fraud, whilst protecting subscriber privacy, thus reducing the need for government intervention and regulation.

Protect existing and future revenues

Keeps the mobile channel “clean” and trusted for financial transactions and revenue generating services.

Service Availability

Selected MNOs are being invited now to subscribe to the GSMA Spam Reporting Service in advance of the formal launch at Mobile World Congress in Barcelona in February 2011. MNOs wishing to be considered for pre-launch subscription should contact the GSMA via email to spamreportingservice@gsm.org



For further information please contact
spamreportingservice@gsm.org

GSMA London Office

T +44 (0) 20 7356 0600

www.gsmworld.com/spamreportingservice

Version 1 : January 2011

