Protecting the Last Refuge of Spam-Free Communication

How to Defend Against Spam Text Messaging Attacks

Table of Contents

Syniverse®

We make mobile work

Introduction

It's the world's No. 1 form of electronic communication. Globally, almost 6 billion people use it. And in just 2011 alone, it was used to send more than 7 trillion communications.

SMS, or text messaging, has truly become one of the world's most popular and practical forms of communication. In a fragmented mobile world of multiple devices, operating systems and service providers, messaging remains the one constant that offers a singular ubiquitous channel through which all end users can communicate with each other.

Not only is messaging the most widely used form of communication, it's also one of the most trusted. And because it's such an omnipresent and trustworthy communication channel, messaging has become a prime target of fraudulent activity. Once the scourge of email providers and postal services, spammers have now begun to zero in on messaging and infiltrate one of the last refuges of spam-free communication.

The new focus on this channel has led to a soaring increase in spam in the past few years. In the United States, for example, consumers received roughly 4.5 billion spam text messages in 2012, more than double the 2.2 billion received in 2009, according to Ferris Research. In addition, approximately 60 percent of mobile users in the United States received one or more spam messages from early 2011 to early 2012, and roughly 15 percent clicked on the link included in the message, according to the United States Federal Trade Commission. What's more, the FTC received at least 50,000 complaints about spam text messages from 2010 to 2013, and the number of complaints has been growing rapidly, with seven times as many complaints in 2012 over 2011.

However, because messaging is so widely used and highly trusted, combatting spam is no simple matter. Since a vast majority of messaging traffic is legitimate, highly accurate content analysis and filtering is required to remove

spam but at the same time ensure reliable delivery of legitimate messages is maintained. Moreover, a number of anti-spam tools are dependent on end users owning a smartphone or configuring their feature phone in a certain way.

Now, though, new technology breakthroughs offer an answer to the rising problem of spam messaging. Advancements in anti-spam solutions have the capability to deliver highly accurate analysis and filtering of messaging traffic as well as solutions that do not require end-user downloads and device configurations. As a result, with spam messaging continuing to grow in volume, it is imperative that mobile service providers implement these solutions to keep end-user devices clear of fraud, protect against unexpected charges and maintain trust in messaging as a service.

A Convergence of Causes

Although spam messaging is illegal in many countries, a number of factors have converged to drive an acute rise in spam messaging, including the ease and low cost of distribution, the increasing sophistication of spammers, the ineffectiveness of traditional methods of spam blocking, and, especially, end users' high trust of messaging.

One of the biggest drivers of spam messaging is that technology has increasingly made spam easy and cheap to send. Spam messages aren't tapped out by individuals using mobile devices, but instead are generated from computers, using programs that send text messages to every conceivable telephone number, automatically and at minimal cost. Since mobile service providers can detect when a large volume of spam is sent from one phone number, spammers turn to large banks of phone numbers, using computers to generate millions of possible number combinations and send messages to those addresses without knowing whether they have called a working number.

In addition to spam messages being easy and cheap to send, spammers have grown more sinister and inventive in their methods. For instance, they regularly change the websites they try to get consumers to click, and blast their messages from the Internet using "over-the-top" messaging systems,

which allow them to send millions of messages cheaply. The minute an operator blocks one number, spammers simply start using another. Moreover, with devices like a SIM box, spammers can plug hundreds of SIM cards – each representing a different mobile phone number – into a single phone. By the time a user has received a text and reported the number, there's a good chance it has been used hundreds of times and discarded.

Compounding these challenges is that end users have few options in blocking spam messaging. Replying to unwanted messages with "no" or "stop" – the usual method for unsubscribing from an unwanted text message list – may only verify to spammers that an end user has a working number that can be resold. At the same time, reporting a number to a mobile service provider or, in countries where spam messaging is outlawed, a government authority to block spam may offer little solution since spammers constantly change the phone numbers they use.

Yet one of the biggest enabling factors of the rise of spam messaging is end users' inherent trust of the messaging channel. Messaging is a communication associated with close acquaintances, personal topics and private conversations, making it more highly trusted than other channels, like email. And this high trust along with the sheer volume of text messages – SMS traffic will reach 8.7 trillion messages worldwide by 2015, up from over 5 trillion messages in 2010, according to Informa – has made messaging an attractive platform to spammers looking to abuse end-user confidence.

A Lose-Lose Situation for End Users and Providers

As a result of these factors and the sharp rise in spam they have driven, both end users and mobile service providers suffer financially, technologically and experientially.

For end users, spam messaging presents a serious risk that can negatively affect quality of service and satisfaction, with the most serious consequence being financial fraud. Although some spam is of the harmless marketing variety, a majority is more insidious, with one tap of the finger putting users at risk to a number of scams that can swipe their personal or financial information.

Of the two most common scams, for example, one features "need cash now" spam, in which end users are promised quick cash if they disclose personal and financial tidbits about themselves. The other is a gift card swindle, which lures end users into taking a survey, in many cases on a spoofed website, and

answering questions about their salary, debt levels, marital status and health history. After end users divulge personal information like their address or transaction history, spammers can use it to access end users' credit cards and even compromise their bank accounts.

In addition to this direct financial fraud, spam messages also indirectly cost end users who don't have unlimited text message plans. Getting as few as 10 spam messages a month at 20 cents each would cost $24 more a year, for instance.

Along with end-user financial consequences is the hassle of having to take time to rectify fraudulent charges and the embarrassment of having personal information compromised by third parties. Users have to call banks and credit card companies to have charges removed as well as have new accounts opened and cards issued. If their phone numbers have been sold to digital marketers, they may need their mobile service providers to block certain numbers.

At the same time, some spam messages can infect devices with malware that silently sends out more spam messages from the users' own phone numbers, adding to end users' embarrassment of having their information violated in the first place. Moreover, regardless of whether or not a spam message even succeeds in luring an end user to fraud, simply because messages are so highly trusted, end users can feel an even greater sense of violation when an unwanted message is received through that coveted channel rather than another one.

For mobile service providers, the costs of spam messaging are even greater, with increased expenses, regulatory issues and dissatisfied end users resulting from illegitimate activity that must be absorbed.

The first cost is the additional network bandwidth that spam messaging consumes, causing legitimate messages to be delayed. The rollout of LTE networks is also presenting new attractive opportunities for spam messaging and new potential vulnerabilities that must be tested, validated and secured.

A second cost is the potential of having a network blocked. For example, one mobile service provider discovered that

it was being blocked by an Asian network because the Asian network operator had been receiving high amounts of incoming messages from the provider's network. An investigation revealed that another operator was selling bulk messaging delivery through the provider's network, and that this was being used by spammers to deliver messages internationally to other networks.

Likewise, regulatory intervention is another risk that spam messaging poses. For instance, if many end users are unknowingly subscribed to a service related to spam messaging fraud, regulatory agencies can mandate a reset for all subscriptions to that service, which also may disrupt other subscriptions to legitimate services. As a result, these resets can cause many end users to not bother to sign back up again for the legitimate services, leading to a loss to those service providers as well as to mobile service providers in general.

A more serious issue for mobile service providers is the cost of fielding complaints from exasperated end users. The cost not only involves the amount that has to be paid back to the end user, but also includes the cost for each call made to a customer service center, the cost of staffing a call center and the cost of attempting to gain refunds from various enterprises involved in a chain of fraudulent activity. Moreover, there is the cost involving the trust of the messaging channel and the perception of a mobile service provider's brand reputation.

Because end users have such a high inherent trust of messaging, they can feel an even greater sense of violation when they become the target of spam through this channel. Trust in messaging has driven end-user confidence to communicate, collaborate and consume. Once this trust is compromised, however, end users' frustration can quickly turn into distrust toward a mobile service provider.

A New Imperative to Combat Spam Messaging

As these threats show, the rise of spam messaging presents a serious and rapidly growing risk to both end users and mobile service providers. Both have become outmatched by an enemy with vast resources and a long head start, resulting in an enemy that must be battled on all fronts.

However, new technological advancements now provide stronger and more comprehensive solutions for prevention of spam messaging. Critically, these technologies ensure the highest level of accuracy in detecting, filtering and blocking spam while at the same time ensuring the highest level of

delivery for legitimate messages. These technologies also enable network-based solutions that can be implemented and managed by mobile service providers without having to depend on end users to download anything or configure mobile devices. With spam messaging rising rapidly in volume, it is imperative that mobile service providers implement these technologies now to protect against fraud, maintain network integrity and ensure end-user satisfaction.

Syniverse, building on its 25-year-plus history as a pioneer in messaging and innovator in real-time intelligence, is taking these new technological advancements for anti-spam solutions further. From its unique position at the center of the mobile ecosystem, where it helps more than 900 mobile service providers and enterprises connect, Syniverse has developed one of the industry's most accurate and comprehensive solutions for addressing the soaring rise in spam messaging and its threat to mobile service providers and end users.

Syniverse Messaging Trust

Syniverse's Messaging Trust gives mobile service providers an all-in-one spam messaging solution to identify and assess targeted messaging threats and the perpetrators behind them, gain insight into ongoing attacks at a detailed level, and take proactive steps to defend against them. Unlike traditional ISP and enterprise security products, Messaging Trust provides highly accurate analysis of traffic in order to identify the sources of fraud and spam within mobile networks where the majority of traffic is legitimate and potentially revenue-generating. In this way, it preserves the cleanliness of the mobile messaging channel without interfering with, or slowing down, legitimate traffic. Moreover, Messaging Trust can be provided to all network subscribers as it is device-agnostic and doesn't rely on an end user having a smartphone or configuring a feature phone.

Messaging Trust has been designed from Syniverse's strategic vantage point in the mobile ecosystem, where it processes more than 2 billion intercarrier mobile messages per day, including more than 95 percent of the United States' international messaging. The current deployment of Messaging Trust is now processing over 170 million SMS messages per day and this is planned to increase to over 800 million during 2013.

Developed through a partnership with AdaptiveMobile, a leader in comprehensive network-based security solutions for mobile, Messaging Trust

leverages Syniverse's and Adaptive Mobile's real-time intelligence capability, global messaging visibility and a proprietary tool set to enable these benefits:

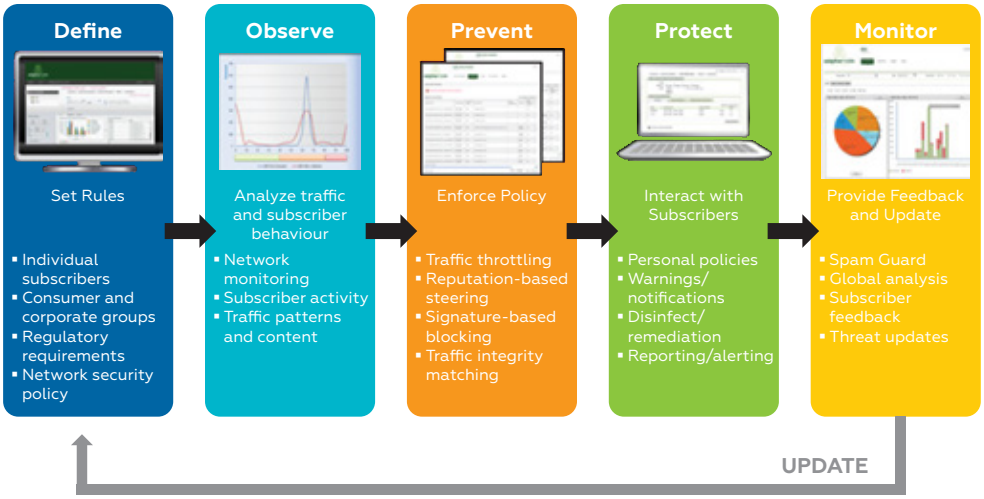
- Accurate and proactive monitoring and removal of identified spam from all message flows.
- Prevention of the re-initiation of known spam campaigns under new telephone numbers by comparison of message content to known spam campaign content.
- Decreased costs, requiring no hardware to deploy and no architecture change in a network, and a structure where costs are transaction-based versus a perpetual licensing fee.
- Removal of the threat of spamming payload activities.
- Increased end-user satisfaction through the prevention of the delivery of spam messages to end users' devices.
- Protection of the reputation and enhancement of the brand of mobile service providers through the decrease of the amount of spam on their networks.

In particular, Messaging Trust is distinguished by these three core capabilities:

- **Highly accurate content analysis and filtering** - Unlike traditional ISP and enterprise security products, Messaging Trust is designed to provide a highly accurate analysis of content for mobile networks where the majority of traffic is legitimate and potentially revenue-generating. This provides a robust way of passing live traffic through a high-speed, anti-spam filtering engine. The platform incorporates an offline analytics system to automatically identify new threats and create fingerprints. This highly tuned platform will only identify a message as harmful, and subsequently block it, after processing a large repository of analytic data and real user reporting.
- **Ability to be deployed quickly without network interruption or additional hardware** - Deployment for mobile service providers is simplified, as they can implement this anti-spam solution without network interruption, additional hardware or increased operational costs. The platform can be used in analysis mode or to actively block SMS spam. In either of these modes, it provides detailed reports and access to a reputation database, so the provider can identify the sources of spam messaging and take other actions.

- **Ability to be offered as a service to all subscribers or as an opt-in services** - Messaging Trust allows mobile service providers to decide whether they want to offer the solution either to all of their subscribers or as an opt-in service. Subscribers can then directly control whether they want to block spam or be provided with spam reports on their own account. A phone app, called SpamGuard, is also available and works in conjunction with this service. This allows subscribers to quickly and easily report spam and gives them the additional feature of blocking any further messages sent to them from that source. Spam messages received by the platform via the SpamGuard app are added to the analytical engine to assist with fingerprint generation. Information from SpamGuard can be vital in identifying "local" or new forms of SMS spam.

Messaging Trust: Total Protection



In addition to these core capabilities, Messaging Trust encompasses the following features in its end-to-end anti-spam solution:

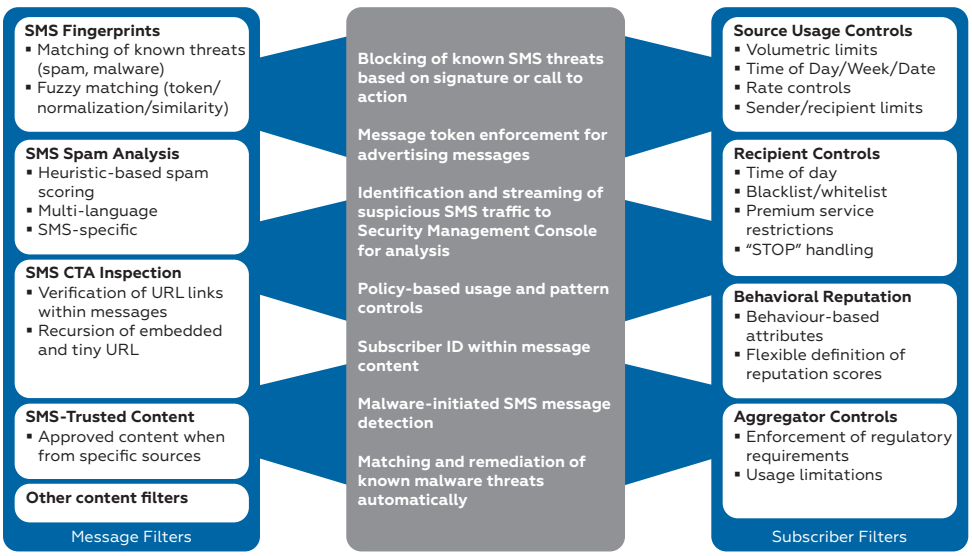
- Detects, flags and blocks spam messages through a phone number rating process and generates new SMS spam signatures/fingerprints.
- Categorizes spammers according to campaigns, originating countries, behavior and other filters.
- Learns subscriber usage patterns, allowing the service to detect complex spamming activities.

Syniverse®

We make mobile work

- Uses a combination of filters to identify suspicious elements in messages, including:
  - Reputation score of the message sender
  - Blacklists
  - Message status
  - Message content
  - Service type to which the message relates
  - Filter type triggered by message
- Provides Web-based graphical daily reports on these areas:
  - Top spammers
  - Top spam campaigns
  - Top operators affected by spam
  - Unique recipients per sender (MSISDN)
  - Blocked messages by category
  - Allowed and blocked profiles
- Offers user-level control for spam protection by enabling subscribers to stop unwanted messages with personal blacklist/stop commands.

Capabilities: Real-Time Analysis



Syniverse®

We make mobile work

Reporting Dashboard Concept

SMS Traffic Reports
- Usage reports across MO, AO, MT traffic
- Drill-down analysis by filtering decision
- Hourly, Daily, Weekly, Monthly data

Source/Destination Reports
- Top SMS sources
- Top recipients
- Blocked vs. Received per source network/country/top recipient

Subscriber Reports
- Top spammers
- Total spam senders plus MSISDN + Volume
- Malware-infected users
- Blocked per sender/per reason

Content Reports
- Top CTA
- Top spam
- New observed "suspicious" messaging
- Analysis per word/phrase/expression

Messaging Trust in Action

In 2012, a major "you just won" spam attack targeted more than 48,000 subscribers on one operator's network in Australia. Twelve senders blasted between 2,676 to 5,432 spam messages each, targeting some subscribers two to four times. To avoid simple signature detection, the senders used the message below, which used a real company name in the URL and varied the opt-out number with unique numbers ranging from 4,000,001 to 5,107,280.

> *The Entry You Made Last Month WON! Go to http://www.(company_name).com.au.wonthatprize.com to claim the prize. Reply STOP to Opt out. 5104980*

Messaging Trust detected the attack by picking it up through its filters for user traffic analysis, fingerprinting and URL categorization. As a result, the operator was able to immediately block the attack and subsequently take further steps to isolate the attack from its network and protect its subscribers. Critically, the operator was able to prevent its subscribers from being exposed to a scam or being charged for unwanted messages, and it was able to prevent its network capacity from being burdened with extraneous traffic.

Preserving the No. 1 Form of Electronic Communication

In a fragmented mobile world of multiple technologies, formats and service providers, messaging is the one constant that offers a ubiquitous channel for all end users to communicate. But now this channel, one of the last refuges of spam-free communication, has come under attack.

Both because it's so widely used and highly trusted, messaging has become a prime target of fraudulent activity that has led to a soaring increase in messaging spam in the past few years. Yet since most messaging is legitimate, identifying and filtering spam while ensuring delivery of the huge volume of legitimate traffic has been a complex challenge.

Fortunately, new technology breakthroughs offer an answer to the rising problem of spam messaging. Advancements in anti-spam technologies have the capability to deliver highly accurate analysis and filtering of messaging traffic as well as solutions that don't require end-user downloads and device configurations. With spam messaging continuing to grow in volume, it is critical that mobile service providers adopt these technologies now to protect end users from fraud, prevent the disruption of network performance and maintain trust in messaging as a service.

Integrating these technologies, Syniverse has developed one of the industry's most accurate and comprehensive solutions for addressing the soaring rise in spam messaging and its threat to mobile service providers and end users. Messaging Trust provides an all-in-one solution to ensure the highest level of accuracy in detecting, filtering and blocking spam while at the same time ensuring the highest level of delivery for legitimate messages. To this end, Syniverse provides a powerful solution to preserving the trust of the world's No. 1 form of electronic communication.

For more information on Messaging Trust, visit www.syniverse.com/products-services/product/Messaging-Trust-Service.

Syniverse®

We make mobile work