



Cloudmark's Definitive Guide to SMS Spam

June 2011

Table of Contents

The value of SMS.....	3
An introduction to SMS spam	3
Types of SMS attacks	3
The difference between email spam and SMS spam	7
Subscribers' reaction to SMS spam	8
The effect of SMS spam on legitimate SMS marketing	8
The rise of SMS spam and its increasing profitability.....	8
SMS spam and the consumer	9
SMS spam and the operator	12
Why traditional methods of fighting SMS spam may not suffice	13
Best practices in messaging security	13
SMS spam - A global problem.....	14
Collaboration	15
What's next?	15

The value of SMS

Individuals across the globe rely on their mobile devices as a readily available and accessible communications channel, keeping them in touch with friends, family and colleagues. However, mobile users may take for granted the ease and convenience of this service, particularly when it comes to sending and receiving SMS and MMS messages. The inherent trust consumers have for this channel and their mobile devices means that when receiving messages, they may not think twice about the source or sender, believing them to be 100% legitimate.

SMS continues to grow at a phenomenal rate and firmly remains the most popular mobile messaging channel. According to Informa Telecoms & Media (January 2011), global SMS revenues are forecasted to rise to \$136.9bn by 2015, as global SMS traffic increases from five trillion messages in 2010 to 8.7 trillion messages in 2015.

In today's mobile-centric world, companies are also increasingly using SMS to interact with their customers. Banks are trusting Mobile Network Operators (MNO) with the delivery of payment authorisation confirmations and financial fraud alerts; doctors, dentists and hairdressers are using SMS to send appointment confirmations and reminders and it won't be long before SMS is used in mobile health applications. Trust is critical in these interactions and SMS is considered by most consumers to be a safe channel of communication.

UK subscribers currently have a high degree of trust in the SMS channel as a means of communication with their MNOs. This is represented in a survey carried out in 2010 by the Internet Advertising Bureau (IAB) and the Direct Marketing Association (DMA). This research showed that 63% of UK participants were happy to receive SMS and MMS messages from their operator. The ability to leverage this mobile SMS and MMS channel is becoming increasingly attractive and profitable for both operators and advertisers in delivering targeted messages.

An introduction to SMS spam

SMS spam is defined as any unwanted or unsolicited text message received on a mobile device. It can take many forms: a simple message to a number enticing subscribers to call or text; a link to a number, encouraging you to call or text a given number; or even a link subscribers follow to a website for more information or to download an application. Similarly to email spam, SMS spam can be a simple nuisance or quite malicious in nature.

Types of SMS attacks

Cloudmark monitors SMS attacks across the globe and has identified three main categories of attack: spam, fraud and malware. In 2010, the GSMA and Cloudmark ran a pilot of a subscriber-focused spam reporting service with six MNOs around the world – analysis of the results showed that the primary motivation (70%) for the attacks is financial fraud in nature.

Some operators such as Bell Mobility in Canada have chosen to promote their messaging security service as a differentiator, offering an “anti-spam” guarantee – complete with a mechanism to refund \$0.15 for every spam message received. Anti-spam is offered as a standalone service or is bundled with the unlimited messaging plan.

SMS spam

This can range from unsolicited advertising to social engineering hoaxes to harmful attempts to steal subscribers’ personal and financial details. Most contain some sort of call to action, the most common of which are listed below:

1. **“Call me now”** - Often used with a reward card, insurance claim or lottery scam where the subscriber clicks on a number, speaks to a fake call centre that attempts to steal personal and financial details. An example of an accident claim scam that is prevalent in the UK is shown below.

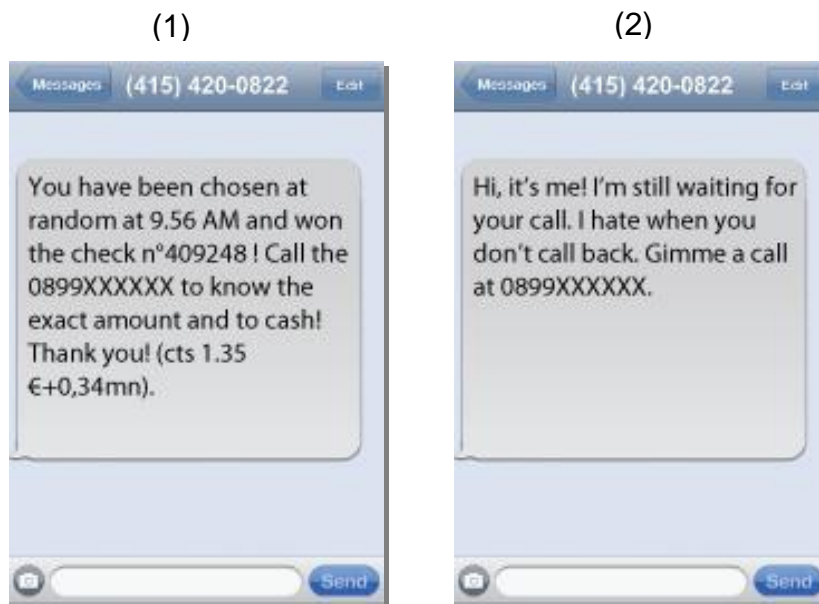


2. **“Click here to view”** – A link to a website is embedded in the message and often leads to an unexpected destination. It may be offensive or inappropriate or may be a way of driving subscribers to a site so the attacker can collect a click-through commission.
3. **“Forward this message”** – This is generally used in social engineering hoaxes where subscribers are encouraged to forward the message onto all of their contacts in return for a reward.

Fraud

The vast majority of fraud attempts are to get subscribers to sign up for premium rate services or call premium rate numbers. The scam often starts when a mobile phone user gets a message offering a prize if they call to claim it. Analysis from Juniper Research in May 2011 revealed that SMS trojans sending messages to premium rate numbers were responsible for 17% of all reported mobile security attacks.

Some examples from across the globe include:



In Australia, the courts recently convicted a fraudster who conned subscribers into making AUS \$4m worth of premium rate calls using a fake dating service scam. 1.8million SMS messages were sent, giving a return of AUS \$2.40 per message.

Mobile malware (including Bots that spread through SMS spam messages) – Malware, short for malicious software, is software designed to infiltrate a mobile device without the owner’s informed consent. Typically, this involves messages containing links sent to mobile users, asking them to download executables (e.g. apps, games) that are harmful and may lead to application exploits. Four of the most common forms of malware include:

- **Virus:** A malicious computer application that is able to reproduce itself. It can infect a new host when an unsuspecting user sends it over a network or the internet
- **Worm:** A self-propagating malicious computer program. It sends copies of itself to other nodes on the network. A worm can spread and infect numerous hosts very quickly in a networked environment
- **Trojan:** A destructive program that disguises itself as a benign application. It does not replicate itself, but instead enables hackers un-authorized access into the infected host. Another severe form of a Trojan is keystroke logging, where a hacker covertly tracks (or logs) a user’s keystrokes without their knowledge or consent
- **Botnet:** A computer programme that resides on a device and is under the control of an unauthorised third party. Recent attacks have involved botnets harvesting personal details and sending unauthorised SMS from infected handsets.

Customers of both Santander and ING Banks were recently targeted in a mobile malware attack. PC botnets were used to harvest customers' internet banking and mobile phone details, which were then used to send a virus to their mobile phones. Once the phone was infected, the attackers were able to authenticate internet payment instructions using the code sent to, and captured from, the mobile device, removing thousands of dollars from customer accounts.

The difference between email spam and SMS spam

There are many reasons why SMS spam attacks differ from email attacks. These include:

- **The billing relationship:** Unlike email users, mobile subscribers have a billing mechanism in place to pay for calls, messages, data and premium rate services. An attack involving a premium rate number is highly profitable for the scammer and, whilst there are strict measures in place in the UK to prevent premium rate fraud, the attackers are staying ahead of the game by using ever changing, highly sophisticated techniques
- **The level of trust and willingness:** As mentioned previously, mobile phone subscribers tend to trust the SMS messages they receive. Any message purporting to be from a friend or trusted organisation, such as a bank, is generally opened, read and acted upon in only a fraction of the time that it takes for a similar message to be opened via email. Smartphone users are also increasingly willing to download applications for mobile banking, stock trading and entertainment. The level of trust of these mobile applications is still at a high level compared to those downloaded from the Internet
- **Sophistication of the handset:** With the increasing number of touchscreen smartphones now available, it is all too easy to accidentally click on a link to a premium rate number or website

Subscribers' reaction to SMS spam

In many western countries, mobile subscribers view unsolicited messages via SMS as an intrusion of their privacy. Their mobile device often contains their most personal information – contacts, photos and, perhaps most importantly, private text messages. Receiving unsolicited and potentially malicious messages often incenses subscribers, compelling them to call their MNO to complain.

The effect of SMS spam on legitimate SMS marketing

Consumers are increasingly opting into mobile services that use SMS as a messaging channel. They do this because they believe the message they receive from their bank, MNO or retailer is legitimate and is safe to act on. However, if SMS spam levels in western countries rise to the level experienced in Asia (where subscribers commonly get 3-4 SMS spam messages per day), then subscribers will have difficulty in determining which messages are genuine, and may stop responding to any of the SMS they receive.

In Canada, Bell Mobility has recognised this problem and has installed comprehensive SMS spam reporting, analysis and filtering technology so it can promote its network as “spam-free”. It firmly believes that, without an anti-spam solution, mobile advertising will never take off and investment in messaging security is not just a network protection investment, but a value investment as well. They have also seen a significant reduction in the number of subscribers disabling their SMS service since launching the anti-spam service.

The rise of SMS spam and its increasing profitability

In the email world, levels of spam are approaching 99% of all email traffic. Fortunately, due to the collaboration between ISPs and email providers and the sophistication of filtering technologies, approximately 98% of this spam is blocked before it is ever delivered. This means attackers have to send billions of messages to achieve any results.

In the SMS world, the reverse is happening. Until mid 2007, the cost to legitimately send one message was around 10p, so the only way to send SMS spam economically was by leveraging signalling fraud techniques to send spam into the

network. Signalling fraud can take many forms, including “spoofing,” where the sender information is altered to appear as though it originated from a different source and “flooding,” where a network tries to consume all of the available bandwidth. Though these spamming techniques had the potential of causing network and bandwidth issues for the operators, today’s spamming methods can bypass traditional network triggers to catch such signalling fraud.

Many MNOs have implemented systems to protect against these attacks and, as a result, levels of spam have decreased. Since then, unlimited texting plans have become universally offered, which has drastically reduced the cost of sending spam using “legitimate” SIM cards. To further compound the problem, some MNOs have not yet deployed any type of SMS content filtering systems, which means a very high level of SMS spam may get through to an unsuspecting recipient.

SMS spam and the consumer

At best, SMS spam is an occasional irritation to the subscriber. At worst, it can cause a significant financial impact, with bank accounts compromised and premium rate services charged to a subscriber’s bill.

The impact on the subscriber depends on the type of attack:

- **Unsolicited advertising:** The level of SMS spam advertisements sent in the UK remains low so there is currently little impact on the subscriber. However, should the level of unsolicited advertisements rise, subscribers may be forced to turn off new SMS alerts to prevent constant interruptions
- **Inappropriate content:** Subscribers expect to be protected from unwanted and offensive content, yet spammers often send adult material indiscriminately, so there is a risk that this indecent material will be received by children
- **Premium rate fraud:** In the UK, premium rate numbers are well-regulated. However, attackers can use overseas premium rate numbers and relatively low volumes of spam in order to avoid detection by the operators, which means that the onus falls on the subscriber to check their monthly bill and to then ask for questionable charges to be

investigated. Many post-paid contract customers would not notice one or two charges of £5, occasionally added to their monthly bill

- **Phishing:** SMS is commonly used in bank phishing attacks, where subscribers receive a message telling them they have won a prize or are due compensation. The message encourages subscribers to call the number embedded within the message to make their claim. If they place the call, it is usually answered by a very professional-sounding operator who tries to obtain personal and bank account details
- **Mobile malware:** Viruses, trojans and botnets are perhaps the most malicious of all attacks propagated by SMS messaging. Once installed on a mobile phone, hackers can steal login details, transact calls and text premium rate numbers and send SMS spam to a subscriber's contacts. The financial impact ranges from unauthorised items appearing on a subscriber's bill, to thousands of pounds being transferred from bank accounts



Subscriber protection

Subscribers can protect themselves from the impact of SMS spam attacks by adhering to the following guidelines:

- *Never click on a link or call a number embedded within an unexpected SMS message, even if it looks like it is from a friend. This may download a self-propagating virus on the device that can send itself to all of the user's contacts.*
- *Only download mobile applications from reputable app stores. Be aware that the Android Market is not policed by Google in the same way that the Apple Store is monitored by Apple and instances of applications containing malware have been identified on this platform. Juniper Networks recently revealed that the number of Android malware attacks has increased by 400% since last summer.*
- *Never respond to an SMS requesting login details or other personal details, particularly if it claims to be from a bank.*
- *If an offer in an SMS seems too good to be true, then it probably is. Companies such as Microsoft, Nokia or your network operator do not run free lotteries for subscribers, nor do reputable banks offer cheap loans via SMS advertising.*
- *Request your MNO to set up content filters on your mobile account so that premium rate texts cannot be charged or adult material displayed.*

Subscribers should always report SMS spam to their operators so that effective counter-measures can be taken to protect themselves and other subscribers from the same attack, as well as rapidly mutating attacks from the same spammer. In many cases, MNOs are only made aware of attacks when a subscriber reports it. It is important to remember that the vast majority of SMS spam attacks are attempts at financial fraud and therefore should always be taken seriously.

If the MNO has a short code reporting service such as 7726 (S-P-A-M on the mobile keypad), the subscriber should forward on any spam for the service to investigate and analyse. If the short code 7726 is not available, then the subscriber should call the customer care centre so that the MNO can investigate the attack and take appropriate action.

SMS spam and the operator

Although increased customer knowledge and caution is important in the fight against SMS spam, MNO's also have a vital role to play. This involves regularly assessing their networks and ensuring they are confident in the security measures they have implemented. For MNOs, it is also clear that the consequence of allowing mobile spam to proliferate could be hugely damaging to their reputation, leading to a rise in complaints and significantly contributing to customer churn and increased customer care costs. How the MNOs deal with these complaints and the protection they provide against future attacks will also have an impact on customer retention. The negative impact of SMS spam on the MNO includes:

- Increased number of spam-related calls to the call centre
- The cost of investigating spam attacks
- The cost of compensating subscribers for any financial loss experienced
- Subscriber dissatisfaction if the MNO does not provide a method of reporting spam
- The possibility of churn if subscribers do not believe their MNO is doing enough to protect them from SMS spam. (e.g. In Canada, Bell Mobility actively promotes their network as "spam-free" in an attempt to woo subscribers from less well protected networks)
- The possibility of controls being put in place by the regulatory authorities which, for example, can prevent the sale of unlimited SMS plans and place other costly burdens on the MNO

In the same way that email spam has impacted the success of online marketing, the wider mobile value chain may also lose out on growing revenue opportunities. Unless networks can remain free from clutter and malicious activity, MNOs will be unable to capitalise on the mass-market adoption of smartphones and the resulting surge in data consumption as well as added revenue from legitimate

mobile advertisers. Only by safeguarding the networks will operators be able to provide customers with the confidence to take full advantage of the increasing number of mobile services being made available to them.

Why traditional methods of fighting SMS spam may not suffice

Western MNOs have traditionally focused on network fraud prevention and have implemented anti-faking, spoofing and flooding systems to protect the SMS channel. Until recently, this was an effective method of preventing SMS spam, as the alternative of sending messages using “legitimate” SIM cards was not economically viable.

However, following the introduction of unlimited data plans a large proportion of SMS spam is now originating within the MNO’s own network or on other networks in the same country. Some MNOs have been using manually updated policy control systems that limit volumes of SMS sent by each SIM and search for keywords within messages. These have proved unwieldy to keep up to date. Attackers also are using increasingly sophisticated methods to avoid detection, such as sending low volumes of messages from large numbers of SIMs and varying content within each attack.

Best practices in messaging security

MNOs can protect subscribers from SMS spam and SMS-born virus, botnet and phishing attacks by implementing a comprehensive, automatically updated, messaging security solution. The key to a successful security solution is to ensure it includes:

- A method for subscribers in any region to report mobile abuse quickly and easily, preferably via a common short code or an embedded mobile client creating a network of global threat intelligence across mobile operators
- An awareness of SMS message content, protocol and context with carrier-grade accuracy and performance, protecting users before the threat spreads across more users
- Support for subscriber-level and operator-level policy controls for security policy decision and enforcement

SMS spam - A global problem

SMS spam does not respect national boundaries and, in some cases, actually benefits from crossing continents so that law enforcement agencies have a slim chance of identifying and detaining attackers. Western MNOs have experienced virus attacks that call premium rate numbers in Russia in the middle of the night. There have also been incidents in which bank customers have had their login details stolen and their SMS payment authorisations forwarded to attackers.

The global issues that contribute to the rise in SMS spam are:

- Guaranteed payments to spammers for premium rate numbers dialled (such as those mandated in the UK)
- Spammers get paid by a UK MNO if a premium rate number is dialled and the premium rate service provider is outside of the UK. As the subscriber is typically a victim of SMS spam, the UK operator rarely sees payment from the subscriber
- The increasing profitability of SMS spam attacks, driven by unlimited messaging plans. Many SMS fraud attacks yield very high returns, ranging from £5 for a premium rate scam, to thousands of pounds in a bank phishing attack
- The increasing openness of the SMS messaging channel to the internet
- The increasing sophistication of smartphones
- The high level of trust in the SMS channel

By its very nature SMS spam is a global problem that needs a global, comprehensive solution. As soon as one network or country puts protection in place the attackers move their focus to another MNO or country. They will continue to attack the least protected networks as attackers can benefit from a highly successful delivery rate.

Collaboration

To fight this global problem MNOs should collaborate as an industry and share details of attacks. In general, the security operations teams of MNOs are happy to collaborate to lessen the impact of large attacks. This was demonstrated at a recent MNO summit in San Francisco (hosted by Cloudmark and the GSMA) where participating MNOs agreed that there were two levels of collaboration that warranted further research:

1. **Contact sharing** – MNOs should publish the contact details of its security operations team so, when an attack originating from one network hits another MNO's network, both operators can be alerted and take appropriate action
2. **Data sharing** – Details of attacks (and attackers) should be shared between MNOs that participate in a global reporting service enabling MNOs to be notified of "bad senders" in their networks and of significant attacks witnessed in other parts of the world

What's next?

As SMS continues to remain ubiquitous, we will continue to see the rise of SMS spam. Market research firm Infonetics (May 2011) has forecast that sales of mobile security software will grow 50% a year through 2014 to hit \$2 billion. However, as preventative measures are beginning to be implemented to protect subscribers from attacks we will continue to see escalating levels of innovation from the perpetrators. They will continue to take advantage of the rise of mobile computing and the increasing power of smartphones and tablet devices. They will create more sophisticated attacks, making use of SMS-borne viruses and botnets to secretly send spam from legitimate subscribers, harvest personal details and self-propagate across the mobile networks.

To counter the rise of SMS spam, the GSMA and Cloudmark have collaborated to create the GSMA Spam Reporting Service (SRS), a global initiative designed to allow subscribers to report instances of SMS spam to their network. The MNO automatically forwards the reported message to the GSMA service where it is analysed using Cloudmark's advanced message fingerprinting technology. The data is then corroborated and an analysis of attacks within the reporting MNO's network is produced.

The MNO then uses this information in their policy management and filtering systems to address the spam in the network. The GSMA Spam Reporting Service was commercially launched in the Spring of 2011, following an extensive pilot programme involving six network operators from Asia, North America, Canada and Europe. The pilot ran over six months and revealed a dramatic increase in SMS spam across the globe, both in volume and severity of attack.



Americas Headquarters
Cloudmark, Inc.
San Francisco, USA

Asia Pacific Headquarters
Cloudmark, Inc.
Singapore

Europe Headquarters
Cloudmark Europe Ltd.
London, UK

© 2001-2011 Cloudmark, Inc. All rights reserved. Cloudmark, the Cloudmark logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Cloudmark and its subsidiaries in the United States and in foreign countries. Other brands and products are trademarks of their respective holders. All product information is subject to change without notice. MM100.0610V01