

Assigning liability for spam

How service providers can avoid taking the fall

By John O’Keefe, CEO & Founder,
Fine Point Technologies Inc.

The new “CAN-SPAM” (Controlling the Assault of Non-Solicited Pornography and Marketing Act) bill, recently signed into law by President George Bush, is the first federal law to establish stringent regulations over the transmission of unsolicited commercial electronic mail, also known as “spam” or UBE

through which the spam was sent, and any other entities that took part in the distribution along the way. These legal loopholes could prove to be highly important.

What this means to ISPs

In the effort to track and catch spammers, authorities can now subpoena an ISP for records of their users’ online activities. In the case that a spammer cannot be tracked based on information from the

ISP needs to have records with information such as: name and address of users, when they logged on and off, and their IP address. Archiving this information is one of the ISP’s most valuable tools in preventing liability from falling on their shoulders in the event that a criminal investigation into a user’s activity is conducted.

Implications beyond spam

Although no one will deny that the ubiquitous nature of spam makes it a nuisance to its recipients, it has other detrimental implications that may not be readily apparent. Spam can exacerbate the transmission of computer viruses, worms and Trojan horses, and Internet fraud, and can bring an ISP’s network throughput down to a screeching halt. It is these ramifications that make spam particularly insidious and a subject that no ISP would want to take the fall for.

The greatest risk to an ISP may not be in court, but rather in the impression that it makes on its subscriber base as well as potential customers. Because of its disastrous implications in the court of public opinion, not taking steps to address these issues could lead to a public relations nightmare. An ISP that can’t produce the identity of its users and is consequently fined by the government suffers the potential of losing current customers and turning off new customers from joining its service. In a worst-case scenario, this ISP could be seen by spammers as a protected haven, because they know they will likely not be identified when they connect to the network, further increasing the exposure to the ISP. ISPs need to ensure that they can verify the actual identity of the subscribers who are using their network at any given time.

Two schools of thought

Internet service providers which require users to provide a username and password to establish a point-to-point connection are already well poised to address the issues sur-

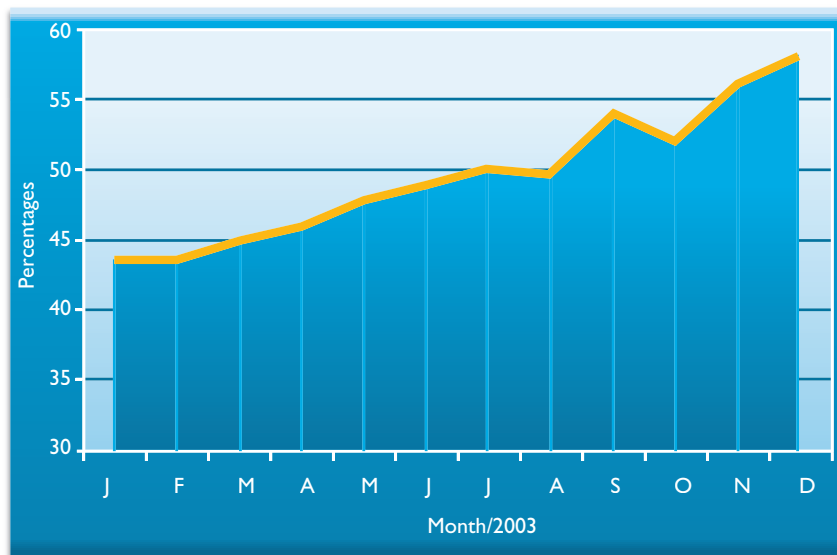


Figure 1: Percentage of total Internet e-mail identified as spam in 2003.
Source: Brightmail Logistics and Operations Center.

(unsolicited bulk e-mail). Designed to strictly regulate everything from the content of e-mails to how the recipients’ e-mail addresses are harvested, this law assigns liability for the transmission of such e-mails.

But how will the government effectively assess fines and jail sentences to those individuals that manage to evade detection? The Can Spam law avoids putting any limitations on who the government can go after in combating spam. This allows the government to extend the liability for spamming from the individual spammer, all the way down to the Internet service provider

servicing ISP, the accountability for sending spam goes back to the Internet service provider. For the first time, ISPs bear the responsibility for the online activity of their users and are forced to closely monitor the way their subscribers connect to and use their network, to ensure that they can pinpoint the source of any illegal activity.

ISPs now find themselves needing to take a more proactive approach in identifying who their users are in order to protect themselves from assuming the liability of their users’ actions.

Given the broad coverage of this law, an

rounding their subscribers' use of service. This information is verified by a RADIUS (Remote Authentication Dial-In User Service) database which allows the user to connect to the service based on the terms of their agreement. Because of the log-on/authentication process required to connect to their service, these ISPs have a much better handle on who their subscribers are, what IP address they are using, and how much bandwidth is allocated to each subscriber. This critical information can all be recorded and retrieved as needed.

Other ISPs have taken a different approach to the connection process by offering an always-on connection without requiring any log-on or authentication. Using

By allowing subscribers to connect to their networks without any authenticated log on process, ISPs make it very easy for spammers to connect without divulging their true identity

this type of connection, a technically knowledgeable subscriber can easily achieve anonymity while connecting to and using the network to send out millions of spam emails without ever being traced, leaving the ISP liable for their activities.

By allowing subscribers to connect to their networks without any authenticated log on process, ISPs make it very easy for spammers to connect without divulging their true identity. By concealing their digital identity, users can use the service to take part in illegal activities like sending spam, while evading liability for their actions. Subscribers can sign up for Internet access through their service provider and "spoof" an IP address and connect to the Internet without being identified. Spoofing is the process by which users can simply go into their network properties and assign themselves an IP address slightly different than the one they are issued by the

Here's the easy part.



The UltraEase™ Series of F-Connectors from Corning Gilbert. Nothing's easier.

Our newest connectors compress so easily, installing them is a breeze. The innovative *Post-Forward* design allows you to quickly see that the cable is seated, and it makes compression nearly effortless. In fact, UltraEase connectors have the lowest activation force in a high-performance F-connector.

To experience the ease and simplicity of UltraEase for yourself, contact Corning Gilbert for samples today. Why force it? Take it easy with UltraEase compression F-connectors.



CORNING
Discovering Beyond Imagination

Corning Gilbert
ISO 9001:2000 Certified

phone: 800 528 5567 (U.S. and Canada)
(1) 623 245 1050 (International)

website: www.corning.com/corninggilbert
e-mail: info-gilbert@corning.com

ISP. By using a different IP address, not only can a user get onto the network anonymously, but they can cause problems with other subscribers' Internet service. The user can further mask his identity by using an off-the-shelf cable modem or network card for which the ISP cannot trace the Media Access Control (MAC) address.

In certain instances, this type of user may only be detected once another subscriber using the service is unable to connect, because their IP address has been spoofed, and calls customer service to

origin of the spam e-mails. Because Proactive ISP requires its user to log on using a username and password, it knows the true identity of anyone using its network at any given time. It produces the records and the government proceeds to prosecute Sammy.

In another part of the country, Jimmy, the junk mail king, logs on to Reactive ISP's service using a "spoofed" IP address. He constructs an e-mail to promote and sell his get-rich-quick plan and sends out 500,000 e-mails to addresses which he procured il-

it comes to maintaining the identity of its users. By integrating a RADIUS server into its infrastructure, ISPs can quickly begin to authenticate, log and record the true identity of their users at any given time.

Considering the options

Authentication using a log-on process can dramatically reduce an ISP's exposure to having the network misused for spamming purposes. Authentication can be addressed in at least two different ways. The first leverages user-based information, which would be any information entered by a user, like a username and password. The second method is based on equipment-based authentication, which would allow a subscriber to establish a connection based on information embedded into the user's networking equipment that can be electronically verified without any input from the user. The latter solution is logistically more challenging to deploy for ISPs that already have an established subscriber base, because it would require replacement of currently deployed equipment. Equipment-based authentication can also be forged as we have seen in the satellite TV arena, with their use of "smart cards."

ISPs can transition to an infrastructure that provides a true authenticated connection between the user and the ISP by using a protocol such as PPPoE. This provides a great deal of flexibility not only in authenticating users, but also in automating IP address configurations, supporting multiple user sessions, integrating with back-end billing and offering customized service and content delivery. By requiring a username and password to establish a point-to-point connection, ISPs authenticate each connected user through a RADIUS server and verify their connection against the terms of their service agreement.

By implementing tighter controls on Internet service use and monitoring the activity of users, not only can ISPs protect themselves from the liability of spam, proliferation of viruses and poor public image, but they can realize higher network efficiency as a result of eliminating gluttonous users, creating a more satisfied customer base. ■

- **Include full address in every e-mail.**
- **Subject lines must be descriptive of content and indicate ADV for advertisements.**
- **The "from" line should indicate sender's information.**
- **Unsubscribe link must be conspicuously displayed.**
- **E-mail addresses must not be automatically harvested or procured using a webcrawler.**

Figure 2: CAN-SPAM in a nutshell.

help troubleshoot. Once the customer support representative goes into the system, only then would he be able to see that the IP address was being used by another machine, although there would be no guarantee that the individual using it could be identified.

Let's consider the following hypothetical scenarios to help demonstrate the ramifications of taking a reactive approach versus a proactive approach to this issue.

Proactive ISP

Sammy, a spammer, logs on to Proactive ISP's service using a username and password and is authenticated to use the service. He constructs a spam e-mail to promote his new diet pill and sends the e-mail to 400,000 recipients, whose addresses he illegally procured. Two weeks later, hundreds of complaints have been filed against the e-mails he sent, but because he covered his tracks, the government is not able to track him down. They can, however, find the ISP from which the e-mails were sent. The government contacts Proactive ISP to further investigate the

legally. Two weeks later, the government receives hundreds of calls about the mail that Jimmy sent. The government launches an investigation, but cannot track down the sender, because he covered his tracks very well. The government contacts Reactive ISP to ask for their assistance in finding the spammer. Reactive ISP, however, never really knew the identity of Jimmy when he logged on using a "spoofed" IP address, and is unable to produce any records that could help catch the spammer. Since the origin of the spam e-mail could only be tracked up to Reactive ISP's network, Reactive ISP is fined for the offense.

In an effort to address the issue of subscriber authentication at log-on, ISPs need to consider shifting from a reactive approach to a proactive approach in securing the use of their services. Cable Internet service providers offer an "always-on" connection, and often promote the feature as a selling point of the service because it doesn't require the subscriber to do anything to gain Internet access. However, in today's changing environment, this type of connection can leave an ISP exposed when