Tech Trends

Spam Scammers Hit a New Low With Spoofed E-Mail

By Harry A. Valetk
New York Law Journal

Most of us loathe sorting through the ever-mounting heap of unsolicited commercial e-mails -- commonly called spam -- peddling get-rich-quick schemes, weight-loss potions and pornography.

Unlike conventional, passive advertisements, spam messages frequently include misleading subject lines that require painstaking effort to spot and delete. By the time we are finished, we are usually too irritated to deal with legitimate e-mails.

But even with all its faults, spam is a delightful walk-in-the-park compared to a new, and far more aggressive, trend in junk-mail messaging known as spoofing.

What is spoofing?

Spoofing occurs when an e-mail sender hijacks an unsuspecting victim's address by falsifying its routing information so it appears to come from the victim's account. When the message reaches its intended target, all reply messages go to the victim's address, not the actual sender.

For spammers, using phony e-mail addresses means they can remain anonymous, avoid handling countless bounce-back messages from invalid addresses, and simultaneously bypass software filters set to block likely sources of junk e-mail. Plus, as spam and other types of junk-e-mail tactics become increasingly unpopular with consumers, spoofing allows spammers to avoid negative publicity.

For the victim, however, spoofing is nothing short of a nightmare.

Typically, spoofing victims drown in a flood of bounced-back e-mails from bad addresses. Shortly thereafter, an inevitable wave of angry e-mails pour in from spam recipients asking to be removed from the spammer's marketing list.

In some cases, victims lose account privileges, after their Internet Service Provider (ISP) shuts down their service for violating its anti-spam policy.

Flooded With E-Mail

The aftermath of spoofing can wreak havoc on businesses and

individuals alike.

In one case involving a commercial site, a man drowned in bounced-back e-mails touting stocks that poured in at a rate of six per second, totaling 80,000 messages in two days.

For one woman, the flood hit her personal e-mail account over night. One day, she had the usual 20 spam messages in her inbox; the next day, she found more than 3,000.

Part of the problem, from a practical standpoint, is that spoofing is easy to do, difficult to trace, and impossible to prevent.

In fact, in just a few simple steps, anyone using a popular e-mail software package, such as Outlook or Eudora, can modify the address information transmitted at the top of an e-mail.

This disturbing trend has raised new concerns among federal regulators.

According to Thomas Cohn, senior assistant regional director for the Federal Trade Commission's office in New York, "the FTC is aware of . . . spoofing and is very concerned about it, as we are with all spam practices that may be deceptive or cause harm to consumers."

What is the Law?

About 25 states have adopted legislation regulating spam and prohibiting spoofing. For example, Washington, Illinois, and Maryland enacted statutes explicitly prohibiting spammers from sending commercial e-mails that use a third party's domain name without permission; contain falsified routing information; or have a misleading subject line.

Illinois' statute generously offers both the injured person and ISP the right to recover attorney's fees and costs, or the lesser of $10 for each unsolicited, illegal e-mail transmitted, or $25,000 per day.

Taking recent action on behalf of consumers, Washington State Attorney General Christine Gregoire filed an action in state court, seeking injunctive relief and damages against several spammers for sending unsolicited commercial messages violating the Unsolicited Electronic E-mail Act and the Washington Unfair Business-Consumer Protection Act.

The lawsuit alleges that the defendants used deceptive subject lines, like "Payment Past Due," "Check Unclaimed," and "URGENT Account Update," to entice recipients to open e-mails.

New York and New Jersey have no statute specifically addressing spam or spoofing.

Still, the most disconcerting reality for American e-mail users is that no statute specifically regulates spam or prohibits spoofing at the national level. Trying to change that, federal legislators proposed several bills in both the House and the Senate to protect consumers from spoofing and various other spam scams.

Proposed Legislation

In the Senate, for example, Sen. Conrad Burns, R. Mont., introduced the Can Spam Act of 2001 to prohibit spoofing and drastically restrict spamming by:

• Prohibiting unsolicited e-mails containing false or misleading header

information;

• Prohibiting unsolicited commercial e-mails after objection;

• Prohibiting deceptive subject headings;

• Requiring commercial e-mails to include a functioning return e-mail address;

• Requiring spammers to identify e-mails as advertisements or solicitations; and

• Requiring a valid physical postal address of the sender.

In the House, Rep. Christopher Smith, R. N.J., proposed the Netizens Protection Act of 2001 to prohibit any unsolicited e-mail that does not contain the name, physical address, and electronic mail address of the sender; does not provide an electronic method to request no further solicitations; and contains a false subject line as part of a bulk transmission.

Needlessly complicating enforcement, however, the Netizens Protection Act would apply to all e-mails, unless the message is directed to any person with that person's prior express invitation or permission; or any person with whom the sender has an established business or personal relationship.

Prevention Tips

For now, there is little e-mail users can do to prevent deceptive spammers from spoofing their e-mails. Regrettably, although the practice is illegal in a few states, it is often difficult to trace the culprit because most mass-mailing tasks are outsourced to third-party companies, not the business actually marketing the product or service.

Even so, attorneys can offer the following tips to reduce the chances that their client's e-mail will be hijacked by deceitful spammers:

• Do report deceptive or misleading messages to the FTC by forwarding them to uce@ftc.gov.

• Do use an e-mail filter. If your e-mail is spoofed, set your e-mail software to automatically delete all messages that have the subject line used by the offender. If your filter gets overwhelmed, your ISP may by able to help.

• Do consider using two e-mail addresses: one for personal messages and one for newsgroups and chat rooms. E-mail users can also take advantage of popular disposable e-mail address services that create a separate e-mail address that forwards to your permanent account. If one of the disposable addresses begins to receive spam, you can shut it off without affecting your permanent address.

• Do visit consumer information sites such as Junkbusters and the FTC's Spam Facts site at www.junkbusters.com and www.ftc.gov/bcp/conline/edcams/spam.

• Do not use a common e-mail address like mjones@aol.com. Spammers use "dictionary attacks" to sort through possible name combinations at large ISPs or other e-mail services.

• Do not over-display your e-mail address in public, at least not in a form that is easy prey for scavenger programs spammers use to harvest e-mail addresses.

• Do not give away your e-mail, unless you are comfortable with a web site's privacy policy. If the company sells your information or shares it with their "partners," you should consider opting-out or altogether withholding your e-mail address.

• Do not reply to spam. Most spam messages offer bogus instructions to remove your name from their lists. Some spammers actually use replies to confirm an address, then sell it to other spammers.

Harry A. Valetk is an attorney with the U.S. Department of Justice in New York City. The opinions expressed here are the author's and not those of the U.S. government.

Date Received: *September 13, 2002*