SPAM: EBB THE FLOW

Ellen Freedman, CLM

SPAM, sometimes known as UCE (Unsolicited Commercial Email) is any kind of unwanted email. It was allegedly named after a trademarked and well–known processed pork meat product which some consider similarly undesirable. Spam covers many subjects not exclusively commercial in nature — chain letters, pornography, scams, virus proliferations — and offers unscrupulous marketers an opportunity to perform mass marketing at little cost.

Most Spammers have little if any scruples. They resell your information without your permission, and against your wishes. They ignore the law. They falsify their email addresses to hide their true identity; a practice known as “spoofing”. They use and abuse computer systems of unknowing victims to perpetuate their acts. In short, they do whatever they can to try and separate you from your hard–earned dollars.

Just how big the problem has become is subject to lots of guesstimates. In an article written August 30, 2002 for ZDNet, Robert Lemos predicted that spam “could make up the majority of message traffic on the Internet by the end of 2002, according to data from three email service providers.” Clearly, it hasn’t gotten quite that bad. But the problem is growing exponentially. Joyce Graff, a VP at the Gartner Group, reported that the volume of spam was 10 times greater in 2002 than in 2001, and 16 times greater than in 2000.

In a June 11, 2003 statement by Commissioner Orson Swindle (don’t go there!) before a Federal Trade Commission Subcommittee, he stated “Current estimates indicate [spam] constitutes at least 40% of all email. In addition, recent Commission studies indicate that spam has become the weapon of choice for those engaged in fraud and deception. Nearly 66% of the spam messages that Commission staff examined appeared to contain obvious indicia of falsity. . .” In a May 21, 2003 news release by the Federal Trade Commission which summarizes its *Prepared Statement of the Federal Trade Commission on “Unsolicited Commercial Email*”, (www.ftc.gov/opa/2003/05/spamtestimony.htm), the commission reported its findings on its study of the various aspects of spam. It noted that “the volume of spam is increasing sharply and the rate of increase is accelerating.” The estimate in 2005 is that spam constitutes 60% of network traffic.

How does one get onto the spammer’s lists? Or more importantly, how do you *avoid* getting on the spammer’s lists? Here are the activities at the top of the list for creating the flow of spam. Avoid them as much as possible.

1. Participation in chat rooms, newsgroup discussion groups and other similar on-line locations where your email address can be “harvested” by spam mail list providers. According to the FTC news release referenced above, “. . .one hundred percent of the email posted in chat rooms received spam; one received spam only eight minutes after the address was posted . . . . Eighty-six percent of the email addresses posted at newsgroups and Web pages received spam, as did 50 percent of addresses at free personal Web page services, 27 percent from message board postings, and 9 percent of email service directories.”

2. Selection of a previously owned email address that has been a spam target in the past. This can be particularly troublesome if you’re using a free email provider like Yahoo, for example.

3. Choosing a common email address, like “bob@” will make you a ripe target for spam. Spam engines routinely send out emails to thousands of common names at various internet domains. Remember, unlike regular mail, there is no cost to them for incorrectly addressed and/or returned emails.

4. Signing up for a free service on a web site in exchange for your email address. Just because the web site looks good, doesn’t mean it doesn’t belong to a spammer trying to harvest addresses. And sometimes even “legitimate” businesses will secretly sell their email lists to spam mail list providers for the easy revenue. I have tested this myself. You’d be amazed at how many “legitimate” businesses engage in this practice. To give them the benefit of the doubt, maybe they don’t know and unscrupulous employees engage in the practice for additional “under the table” earnings. No matter, you become the spam victim either way.

5. Virus infestation creates spam, too. Klez, for example, is fairly well known as an epidemic which stole subject lines and contents from files on the victim’s computer, and sent the information out to addresses in the victim’s Outlook address book. Can you say “loss of client confidentiality?”

How do you fight back? Well, let's start with the easiest solution. Use of a good virus scanner puts virii like the Klez out of commission. But it is estimated that as many as 10,000 new viruses are released into the "wild" each week. So you must also regularly update the virus definitions by going online and downloading a new file. If you use Norton or Inoculate it will do this automatically for you. I use Inoculate, and it automatically updates the latest virus definitions every hour, in the background, as I work. McAfee works at the touch of a button. If you're an Outlook user, make sure you install all of the Microsoft free software patches to plug the vulnerabilities as they're discovered.

The most powerful prevention tool is your DELETE key, or the "X" on the tool bar in your email program. If you suspect a message is junk mail, treat it as such by deleting it without even opening it. Look at the subject heading and sender for clues. I automatically delete anything with an attachment from an unknown source, without opening it. Remember that just opening an email can sometimes activate a virus within. So can using Autopreview. Instead, I use an inbox "view" which displays just the first couple lines of text, which is usually enough to let me know if the email is legitimate. When I receive unexpected attachments from people I know, I carefully examine the full filename, including extension (e.g. .DOC for a Word document) before opening. If I'm not sure of the legitimacy, I email the sender first and ask what they have sent, before I open it. I have avoided much pain and regret this way, as usually the sender replies back that they had a virus and didn't know it, and that the virus, not them, sent the attachment to duplicate itself.

If you do receive spam, do NOT reply. A reply can perpetuate what you're trying to stop, as it verifies to spammers that they've reached a valid email address. This just ensures you'll wind up on more spam mailing lists in the future. In the previously referenced FTC release, it was noted that their test as to whether spammers were honoring "remove me" or "unsubscribe" options found that ". . . 63 percent of the removal links did not function." I'll take it a step further and tell you that they function to the *opposite* of your desires by validating your address.

As an alternative, if you are an Outlook user you can automatically block additional email from a source by right clicking on the email, and selecting Junk Mail/Add to Junk Email Sender List. You will never have email in your inbox from this source again. It will not help for the fraudulent spoofed addresses, as those spammers change the "from" address regularly. But for "legitimate" junk email (how's that for an oxymoron?) it will stop further receipt without the associated risk of validating your address for additional spammers.

Use of email filters is another method to deal with the influx of spam. Filters examine email headers and message bodies for signs that they're spam or worse, such as prohibited email of a sexual or illegal nature. The problem with filtering methods is that they are somewhat indiscriminate in what they block. A filter can exclude legitimate business emails because they discuss blacklisted words. These are called false positives, and can cause important messages to get delayed or lost. One editorial I read somewhere likened false positives to the dolphins that get tangled up in the tuna nets. Very apropos, as I discovered firsthand at a law firm I managed which did employment law. The words and phrases which would be automatic triggers for filtering would have stemmed the flow of legitimate emails.

For reviews and links to popular filtering software programs, search on the internet. The favorites change frequently. Right now Postini is a favorite for mid to large firms. For small firms or solos, a package called iHateSpam works pretty well, but there are many others available at a cost of anywhere from free to as much as $60 per seat.

Blacklists are another method of blocking the flow of spam. Blacklists are literally lists of domains which are known spam sources. A network manager can either create a blacklist based on spam which reaches the firm's mail server, or can subscribe to services which provide such lists. However, as you can imagine, incorrectly listed domains can block legitimate emails from reaching their destinations. This problem is greatly exacerbated by spoofing techniques, as well as the ability of spammers to use legitimate web mail servers, without knowledge and consent of the owners, as a base from which to send spam.

There are also application service providers (ASPs) which provide email content or blacklist filtering, and even high-grade virus scanning, before the email even reaches your mail server or workstation. Network Alternatives of Langhorne, PA is one such reliable ASP, offering a service called Message Patrol™, which is very affordable. You can reach them at (215) 702-3800 or at www.network-alternatives.com. (Tell them Ellen sent you.)

Along with blacklisting of domain names is the practice of setting up decoy email accounts, which uses a dummy account to attract and capture spam for analysis. Once a system administrator determines that the email is spam, the domain name can be added to the blacklist.

If you believe you are the victim of spoofing look for these tell-tale signs:

1. You receive delivery rejection notices for messages you haven't sent. These messages would be returned to you because the recipient's email

address is invalid. They come back to you because your address was put into the “from” line.

2. You receive complaints from people who believe you are the sender of an email. Check your sent items folder if you cannot remember, but it should be very easy to determine whether or not you actually sent the email. If you did not, you have been spoofed.

3. The traffic on your computer system’s email server is disproportionate to the volume of email you receive and send. This could be a sign that your system is being secretly used by a spammer as a base of operation. It’s a more common practice than you think. In fact, some EULAs (end user license agreements) contain language carefully buried which grants legal rights to the software provider to use part of your system for outbound traffic. *Always* read the EULA before clicking “I Agree.” I found this by accident once when attempting to download some free software utility which was highly touted on a reliable and respectable web site. Needless to say, I did *not* agree to the EULA, and passed up the opportunity for the “free” software.

If you have been spoofed you need to take action. First, you should respond to those who send email complaints. Use a form email which lets them know you did not send the email, and that the sender address was forged. Encourage them to trace the email and report it to the appropriate ISP. You may even want to provide educational information which assists them in tracing the real route of the email. Sites like Spam Abuse (http://spam.abuse.net/userhelp/) and Death to Spam (www.mindworkshop.com/alchemy/nospamlhtml) can be very helpful. You may even want to join, or recommend someone else join the Mail Abuse Prevention System (www.mail-abuse.org).

Second, if it gets too bad, you should consider abandoning your email address by shutting it down, and selecting another. And then be more cautious about where it gets posted.

I would be remiss if I did not mention legislative solutions before ending this article. There has been little of substance accomplished on the legislative front, aside from a number of weak state laws. Federal legislation may be the only effective means to fight an epidemic that has infested a global medium.

There is no doubt that spam is undermining consumer confidence in the internet as a reliable means of communication and commerce. There is also no doubt that it is costing business enormously in actual revenues and in lost time;

some estimates are that management level employees spend as much as ten minutes out of each hour dealing with UCE.

There must be an economic cost for the delivery of unsolicited email, and only strong federal legislation which bans bulk, unsolicited commercial advertisements will accomplish that. At the least, creation of a national do–not–spam registry would be helpful. It has certainly helped with unwanted telephone and fax solicitations. In Japan, where there is tough legislation requiring all spam to have the label "unsolicited advertising" in the subject line, DoCoMo, the country's dominant mobile phone carrier, was awarded 6.57 million yen ($54,420 US) for the cost of delivering unsolicited email. DoCoMo estimates that more than 80 percent of the 950 million daily messages that are sent to its mobile service each day is unsolicited.

If you'd like to know what legislation has been passed, and what is pending with respect to spam, both federally and at the state level, visit www.spamlaws.com. Meanwhile, stay out of those chat rooms!

A version of this article originally appeared in the Summer 2003 edition of the Pennsylvania Bar Association Solo and Small Firm Section Newsletter