Legal

by Mark Navin

The issue of unsolicited commercial e-mail or spam clogging up inboxes has dominated the world of technology over the last few years. Most recently, a brother-sister spamming team was prosecuted under new laws in the United States. What does not receive a lot of attention, however, is the detrimental effect on legitimate businesses that do need to do mass mailings. The Club's weekly ENews is a good example.

Without being too melodramatic, spam is one area of technology where there is a war going on. Microsoft's Bill Gates has made it a personal mission to hit back, possibly because he's the most spammed person in the world receiving around four million pieces of junk a day. On one side is the "we want your e-mail address to add to our list" group and on the other is the overloaded IT staff who don't want to give the e-mail address out.

It used to be that any non-delivered mail would be returned to the sender mail server as a non-delivered item, more as a friendly help between companies than anything else. With the advent of spam, there arose two problems with this. First, it confirms that an e-mail address is not valid, and the second is that it confirms that another mail server received the mail and checked its mailbox list. One up for the bad guys.

These days the trend is for a mail server not to indicate bad mailboxes or the mail server presence. Having found a mail server, the next step is to simply try and guess mailbox names. Small companies tend to use first names so an e-mail address such as mark@something.com is an easy find. Some companies use titles such as gm@something.com—another easy find. Most large corporations tend to use firstname.familyname@something.com, which is a bit more of a challenge, but not much. There are numerous name variation dictionaries available for a brute force attack where the software runs through a list of variables such as a@something.com , aa@something.com, and so on. It's more of a nuisance than a malicious attack, as the mail server has to receive and discard each e-mail.

Mail can be stopped at a number of points from sender to recipient. Increasingly, the first point of defense is at the mail server to mail server initial handshake stage. The receiving mail server performs a reverse domain name server check, meaning it checks that the sender mail server is valid. (This became necessary when the new generation of viruses had their own built-in mail server). If the receiving mail server cannot validate the source, it drops the connection and refuses to accept the mail. This line of defense is becoming increasingly popular with its ability to fend off brute force attacks from invalidated sources.

If the mail is accepted, the next line of defense is the spam filter in its many forms. It can be separate hardware or mail server integrated software. The vendors have devised a lot of wonderful marketing terms to describe what they do to block spam, but it's effectively the other side of the brute force equation. The technology examines either some or all of the e-mail details,

including the sender's name, the domain address, the addressees, the contents of the subject line and sometimes scan the contents of the message for key words. It compares what it finds against a known list and then either deletes it or places it in some form of "spam quarantine" to be checked later either by the named addressee or IT staff. Yahoo, for example, delivers all mail but places suspected spam in a specific folder euphemistically called "Bulk," while Hotmail's folder is labeled "Junk E-Mail." Both mail servers automatically delete the contents of these folders on a regular basis, which means valid mail arriving in that folder can easily be deleted before you've read it.

If a mail passes through up to this point, it will be delivered to the user inbox. If you have an old e-mail address (more than two or three years is old), the chances are your address is known and the amount of attempted spam to that mail address will be higher and consequently more will get through. New mail software applications such as Microsoft Outlook or Outlook Express have a built-in spam filter but it lacks the sophistication of the lines of defense mentioned. My spam bucket catches between 200 and 300 e-mails a day specifically sent to my e-mail address (not to the Bill Gates level yet!). This is over and above what the mail server filters.

Once placed in a spam list or folder, it requires user intervention to reverse the decision. Current software is generally not yet sophisticated enough to recognize that spam to one user is a legitimate mass mail to another user in the same mail system. If the system determines that a specific set of rules has been met, the block can be universal. All this sounds slightly draconian but given the percentage of spam versus legitimate mail, it is also understandable. (Spam makes up around 60 percent of e-mail traffic.) Most systems have a reporting process for spam and what this can mean is that one user can inadvertently block a mass mail because he/she doesn't want to receive it.

It's also important to remember that the difference between traditional junk mail and electronic junk e-mail is that there is very little or zero costs involved to the sender. No postage stamps and in the case of virus or hoax spams, the victim bears the costs when his machine is used to send out further spam mail.

If you would like to read any of my previous articles for *iNTOUCH*, you can access the archives at **www.marknavin.com/articles**. Those of you who wish to add comments can use a moderated discussion group at **www.marknavin.com**. □

Keeping Out the Spam

The line between legitimate mass e-mails and spam is becoming increasingly blurred. Below are some basic guidelines to ensure you're able to send and receive legitimate mass mailings, while retaining some control over spam.

Dos

- Protect your primary e-mail address.
- Create a new e-mail address using Yahoo or Hotmail or one of many free mail services for receiving mass mailings. Expect to get spam at this address.
- Check that your personal mail application such as Outlook or Outlook Express is correctly configured for your mail information. The latest versions of these applications can be configured for multiple mail accounts including Yahoo and Hotmail.
- Be sparing with cc (carbon copy) or bcc (blind carbon copy)—spam filters can be set to limit mail based on numbers of recipients.

Don'ts

- Never give your primary e-mail address (private or business) to a Web site unless it's a trusted source. If you do, assume this e-mail address will be spammed.
- Never use your company e-mail address for any purpose but individual business e-mails. If you need to receive regular mass mailings or subscription information e-mails, ask your IT department to set up a different e-mail account for it. More than one person may want to read it so a common mailbox is more efficient for all.
- Never send an e-mail with a blank subject line or with a trite phrase like "Hi," "Read this" or "It's me." It's guaranteed to end up being blocked as spam.
- Never reply or click on the link which says, "Click here if you want to be removed from our distribution list," unless it comes from a legitimate company that you know is genuine. Clicking will ensure that your e-mail address is registered on all future spam lists. It's safer to simply add the sender address to your spam bucket.