By Don Passenger and Jeff Kirkey©

Un-Canned

Getting It Back

This article can make you $900 richer this year—if you use electronic mail (e-mail) and follow our advice. E-mail is a great method of communication used by a majority of lawyers and staff. To use e-mail, you need to make the address available. Unfortunately, one by-product of making your e-mail address available is that advertisers can harvest your e-mail address to send you unsolicited advertisements (Spam).

While not typical, each of the authors of this article received over 6,500 Spam e-mails in the month they worked on this article. This experience vastly exceeds the 2,200 Spam e-mails per year the average person can currently expect,[1] but the better you advertise your availability by electronic means, the more Spam you will receive. Further, the quantity of Spam e-mail has doubled about every four-and-one-half months.[2] From 2001 to 2002, Spam increased from 8 percent of all e-mail to 38 percent[3] and by July 2003 is likely to constitute more than half of all e-mail.[4] This means you will be getting even more Spam than our estimate suggests by the time you read this article.

Think about this: if you get 2,200 Spams this year and spend ten seconds looking at each to be sure it isn't an important communication, hit delete and look at the next e-mail, you have spent over 6 hours out of your year "canning" Spam. At a billing rate of $150 per hour, the cost would be $900 in lost billings. How can you fight back? This article will offer several solutions to reduce the time and economic loss, plus help save your sanity.

Where Spam Comes From

If you have an e-mail address, you have undoubtedly received Spam. Spam comes mainly from three sources:

1. You signed up for something, gave out your e-mail address, and either failed to say "don't send me anything else" (if they were polite enough to ask) or they don't care about your preference;
2. You have your e-mail address on the Internet as part of your firm's marketing web page and a commercial program called a crawler harvests your address (and maybe some keywords to help target the Spam to things you might be interested in); or
3. Random e-mails are sent guessing at common e-mail addresses at known domains.

Receiving Spam presents problems because it takes minutes out of your day to delete it, it can lead to space problems on your hard drive, it may slow performance of downloads, and it can cause you to overlook a legitimate e-mail among the junk.

You Have Options

Fortunately, you are not without some options to reduce the inconvenience. You can attack the problem on several fronts. First, many Internet Service Providers (ISPs) now include Spam filters as part of their services. Second, most e-mail client software, such as Microsoft's Outlook Express, allow you to filter or block e-mail you can identify as Spam. Third, you can get Spam filtering software for use on your machine.

ISP Filtering

If you are fortunate enough to have Spam filtering software on your ISP, you can usually set the level of protection you desire. Unfortunately, if the settings are too high, you may trash good e-mail

Spam

in the Tin

Fast Facts:

If you have an e-mail address, you have undoubtedly received Spam.

Filtering Spam can save you time and frustration.

You can fight Spam through your ISP, e-mail client software, or other Spam filtering software.

with the bad. A medium setting is usually the best choice. It junks the stuff that is definitely Spam, but lets through some questionable material that may include your friend's e-mail with a joke in it. Another potential downside to this filtering method is that e-mail identified as Spam is usually vaporized—it disappears forever—because the deletion occurs prior to your download.

"Filtering" or "Blocking" through Your E-Mail Client

The "e-mail client" is "geek speak" for the program used to send e-mail, such as Eudora, Outlook, Pegasus, Opera, or Outlook Express. In Outlook Express, which is probably the most commonly used e-mail client, you can look at an e-mail, decide it is Spam, click on "Message" in the menu bar and choose "Block Sender." You are asked if you want to delete other e-mail from the sender (be careful with this: if you block e-mail from your mom by accident and then hit "Delete other mail from this sender," you will accidentally delete all your love notes). You then have to enter "Okay" before you resume reading your e-mail. This method works pretty well, but has several drawbacks:

Mistakes Are Hard to Retract

You will make a mistake eventually if you do it long enough. You can get in a repetitive pattern of clicking on e-mails and clicking on "Message/Block Sender." If you mistakenly block the e-mail address of a friend—it is already too late because the block is in. To undo the block you need to click on "Tools/Message Rules/Blocked Sender List," scroll to the very end of the list (because unlike a logical person, the program adds the names to the bottom of the list instead of the top), find the address, click on it, click "Remove" and confirm the removal, close the dialog box and finally resume where you left off. Now that was work!

Smart High Volume Mailers Have Found Ways Around This System

The best one we have seen lately disguises the e-mail so that when you block the address, you block yourself. The spammer masks the e-mail so it appears to have come from your own e-mail address. This means you cannot send yourself any more e-mail until you remove the blocked address. The second and more typical circumvention is where the sender uses a reply address like "218747e07f63d53747e1561@dailyannoyingoffersanddeals.com." These examples contain a number unique to the particular e-mail sent out. It can be decoded so that if you reply, the spammer knows who you are, what offer it related to, etc. Note that clicking on the link in the e-mail will not only take you to the referenced website, but will also pass on information telling the spammer that you in fact looked at the product or offer, thus increasing the risk you will get even more Spam. Blocking this e-mail address will have no effect because the spammer never reuses the unique number. The next time they e-mail you, the number changes to reflect the new offer.

Fortunately, there is another step you can take to help—but not always solve—the problem, called "domain blocking." You can refuse to receive all e-mail that comes from a particular domain. For example, you probably never want to get e-mail from a domain called "dailyannoyingoffersanddeals.com." Assuming that you received e-mail from this domain, you would block it in the normal manner. Every few days you should peruse the list of blocked e-mail addresses, looking for addresses that are from domains you wish to block in their entirety. Then, highlight the desired blocked address, click on "Modify," delete the @ sign and all preceding text, and accept the change. Then work your way up the list in this fashion until you get to where you left off last time. If your blocked list includes a domain like the ones above that sent more than one e-mail, then when you try to block the domain the second and subsequent times you will be asked if you mean to add this in replacement of the same name already in your blocked list. Just say, "Yes."

> ***If you are tired of taking five (or more) minutes to delete your junk e-mail every day, take matters into your own hands.***

Domain blocking will help significantly, but it has two drawbacks. You probably don't want to block "yahoo.com" or "hotmail.com" entirely because your friends use them, so addresses from domains of that type aren't fair game for this solution. The other problem is that the spammers are on to domain blocking. Domain blocking in Outlook Express starts from the @ sign and moves right. The spammers have now introduced "sub-domains," which fool the current version of Outlook Express. Example: In a perfect world you would look at the address "bounce-48905120-997@mail104.dailyannoyingoffersanddeals.com" and determine that you don't know anybody at "dailyannoyingoffersanddeals.com," and block everything at "dailyannoyingoffersanddeals.com" by modifying the blocked address to read "dailyannoyingoffersanddeals.com." Unfortunately this would not block e-mail from "mail104.dailyannoyingoffersanddeals.com." Instead you need to block "mail104.dailyannoyingoffersanddeals.com," by deleting everything from the @ to the left and hitting "Okay." The hitch, however, is that this is the 104th sub-domain this e-mailer has used. Tomorrow they will be sending you mail from "mail105.dailyannoyingoffersanddeals.com" and the day after that.... So every day you have to look at the spammer's first offer before blocking the daily sub-domain and moving on.

There is another method of domain blocking that can help, but it gets more tedious. You can click on the word "Message" in the Outlook Express menu bar and choose "Create Rule." In the third section of the resulting dialog box, "3.Rule Description," click on the e-mail address that appears. When you see the address in the bottom section, you need to add an address by manually typing the domain you want to block. This is more intelligent because you can type "myfunsleuth.com," for example, and it will take out all sub-domains at the same time. Click "Okay" to go back, then choose to delete the mail in the second section, "2. Select the Actions for Your Rule." The only problem with this approach is that having too many rules will impact performance. Still it is a good way to junk the biggest offenders.

It Takes Too Many Clicks

At best, the blocking solution in Outlook Express is clumsy, requiring multiple clicks, with no “undo” or “cancel.” An improvement to Outlook Express would be if it allowed you to select domain blocking as the second step and would allow sub-domains to be blocked as well. Another problem with blocking using Outlook Express is that you cannot export the blocked senders list and edit it in any simple text format.

Spam Filtering Software

There are a number of filtering programs available. Some available for purchase can be configured to do the job nicely. For example, “MailShield” from Lyris (http://www.lyris.com/products/mailshield/) uses “fuzzy logic” but costs $60. “SpamKiller” by McAfee (http://www.mcafee.com/myapps/msk/default.asp) is $40 and is nearly as powerful. For the frugal among us, there are also freeware utilities that work pretty well. “SpamPal for Windows” is one of the best we have seen (http://www.spampal.org.uk/).

The concept of a Spam filtering software is very simple. The Spam filter actually retrieves the mail from your Internet account. To do this, you set the incoming mail server in your Outlook Express or other e-mail client to “localhost.” Your e-mail client then looks at the Spam filtering software for new e-mail instead of your ISP. You can configure the filtering software to check multiple ISPs. When your e-mail client requests e-mail, the filter software pulls the mail from the server. In the case of SpamPal, it adds “**SPAM**” to the subject line of suspected Spam. You could then create a filter to route e-mail with “**SPAM**” in the subject line to a junk or quarantine folder. (To create the filter just click on the first e-mail containing **SPAM** and choose “Message” from the menu bar and then “Create Rule From Message.”) This frees up your inbox to receive legitimate correspondence.

Periodically you need to actually read the Spam mail folder to be sure you didn’t trap any desired mail. If messages you actually want got diverted to the Spam mail folder, you need to adjust. Most e-mail filter programs work from three principals: whitelists, blacklists, and content filters.

Whitelists

A “whitelist” is a list of e-mail addresses that get through the Spam filter regardless of content. This is where you put your mother and friends. Most filtering programs, including SpamPal, will automatically whitelist people in your e-mail address book and people with whom you correspond more than a few times. You can also manually add persons into such a list.

Blacklists

This is the list you do not want to be on. Blacklisted e-mail is sent to purgatory and, at best, gets a cursory glance. Blacklists are assembled by several organizations and SpamPal, like most filtering software, allows you to specify one or more such lists and automatically retrieve updates of the blacklist at set intervals. You can also add your own blacklist entries. This is where you can add the domain you want to kill. Unlike Outlook Express, on SpamPal you can add an asterisk if you want to use a wildcard character. So “*myfunsleuth.com” would get the sub-domain issue cleared up immediately. If you choose too many third-party blacklists to double check, you may see a delay in e-mail performance.

Filtering

While the use of white and blacklists tends to get rid of repeat offenders, there are some Spam messages that get sent from a number of addresses. The messages sent by the Klez Virus are a good example. The messages come from random addresses, but have consistent content. You can establish a filter to look at the e-mail and quarantine it based on the content. You can also set filters to hold e-mail with particular types of attachments. You can get plug-ins for SpamPal, for example, which allow you to search content using a powerful method called “Regular Expressions” (or REGEX for short), permitting you to find patterns of words regardless of how many other words separate them.

Conclusion

If you are tired of taking five (or more) minutes to delete your junk e-mail every day, take matters into your own hands. Get active and block it, filter it, and get on with the legitimate communications using any combination of the suggested three options: through your ISP, through your e-mail client, or through Spam filtering software. To further assist you, the authors have set up a website at www.lawtechhelp.com where they show you step-by-step how to implement these suggestions for several popular e-mail clients. ✦

Jeff Kirkey is the program attorney at the Institute of Continuing Legal Education in Ann Arbor. Mr. Kirkey plans ICLE’s substantive law seminars, and he develops and teaches technology training seminars. He also helps develop content for the ICLE website. He has lectured frequently for ICLE and other organizations and has published numerous articles on the Internet and on law office automation. He is a chapter author of ICLE’s Internet and Technology Guide for Michigan Lawyers and a council member of the Young Lawyers Section of the State Bar of Michigan.

Don Passenger is a judge in Grand Rapids District Court. A moderately advanced computer user, he has frequently taught computer skills to other judges and attorneys at seminars sponsored by the Grand Rapids Bar Association, the Michigan Judicial Institute, and ICLE, including the highly acclaimed “60 Tips In 60 Minutes” program often presented at the State Bar Annual Meeting. Mr. Passenger also teaches in an adjunct capacity for the computer information department at Davenport University.

Footnotes

1. http://story.news.yahoo.com/news?tmpl=story&u=/nm/20021202/wr_nm/tech_spam_dc_4.
2. http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2002/10/09/BU243115.DTL.
3. Id.
4. http://zdnet.com.com/2100-1106-979069.html.