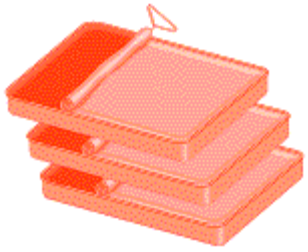
Spam-Free: Protecting Yourself From Slick, Spongy Advertisers

By Ernie Longmire

Ernie brings thirteen years of Internet experience to his job as BASIS' online services coordinator.

If you're like millions of other people online, you're struggling with an ever-increasing amount of junk email when you log on in the morning. As if you didn't have enough things to do, some days you may find yourself wading through more new junk email than real messages.



It all began on April 12, 1994, when Arizona lawyers Laurence Canter and Martha Siegel launched the most notorious single spamming incident and bombarded more than 6,000 Usenet newsgroups with an offer to help people apply for U.S. work permits. Inappropriate advertising had been a problem on Usenet before but never on that large a scale, and the decentralized nature of Usenet made it virtually impossible to prevent. While the messages were almost universally decried as an abuse of the Usenet, Canter and Siegel refused to back down or apologize for their actions. The resultant uproar caught the attention of the national media, landing Canter and Siegel a book deal and exposing the world to the idea that you could put virtually any message you liked in front of millions of pairs of eyes at almost no cost whatsoever. Even if you got only a handful of positive responses to your message, it would cost so little to send it out that you were almost guaranteed to come out ahead.

Why Spam Is Bad

To see the problem that spam poses for the online community, take a look at the classified advertising section of your local newspaper. Each ad in the paper represents someone who was willing to pay a few dollars to have his or her message reach a wide audience--and someone who would be just as happy to have that message end up in hundreds of thousands of email boxes and discussion forums for a few dollars more. If spam becomes a widely accepted form of advertising, every place you read messages will quickly start to look like the classified ad section of your local paper. This is just fine if you like reading classified ads but is more of a problem if you're trying to conduct business online.

Why You're Getting Spammed

People are often surprised at the amount of junk email they receive and wonder how they end up on so many distribution lists. The people who create and sell email address lists will go to amazing lengths to pad those lists with as many addresses as possible. Virtually anything you do online that exposes your email address can result in more junk email. Spammers have been known to gather addresses from:

- Web pages, whether the addresses appear in mail links or not.
- Usenet postings, some dating back years.
- Mailing lists and mailing list archives.
- The InterNIC site contact database.
- Guesswork, trying common personal names like "Steve" or titles like "president" or "webmaster" at every domain name they can think of.

In addition, you may have noticed that many spam messages include a blurb toward the end explaining that you can be removed from the spammer's list by sending a remove request to a certain address. Unfortunately, as many people have confirmed by sending such a request from a new, otherwise-unpublicized account, sending such a request can often get you *added* to other spammers' lists, so it's best not to try.

Measuring The Damage

Spam costs you and your company in a number of ways. The most obvious can be seen in the time and effort wasted in dealing with each message as it comes in. Spammers work very hard to make sure their messages are read, so it's often difficult to tell that a piece of email is unwanted until you've actually opened and read it. No webmaster can afford to ignore a message titled "Question about your website," even if the question in most such messages is, "Have you considered paying us lots of money to help you promote it?"

Your mail system can also be abused by spammers using your mail server to relay spam to other machines. The Internet's underlying email delivery system makes it easy for any site on the network to forward its mail through almost any other site on the network. This can make mail configuration and delivery easier, but it also makes it just as easy for a spammer to use your mail server as it is for a legitimate user. By forwarding their bulk email through your machine, the spammer uses your bandwidth for delivery instead of his or her own and deflects blame for the network abuse. The resulting complaints can come in such volume that the victimized mail server crashes, causing hours of lost time and productivity.

A similar problem comes with forged return email addresses on spam. Most spammers have learned that if they put a valid return email address in their junk mail, they will be quickly deluged with complaints. To avoid this, they put false return addresses on their outgoing messages and ask people to respond by fax or telephone. Sometimes these return addresses are completely invalid--the mailbox they describe doesn't exist anywhere. But other times, these addresses can belong to real people, either picked at random or as an intentional act of abuse. In either case, the result is the same: the mailbox at the address on the outgoing spam message is almost immediately filled beyond capacity with bounced messages and angry complaints. As in cases of relay abuse, the volume of mail involved can shut down a domain's mail services.

Individual Countermeasures

There are a number of ways you can try to keep spam from taking over your mailbox and your life. You should be aware, however, that there is currently no 100% foolproof way to keep spam out short of cutting your connection to the rest of the world with a pair of garden shears. Each step forward in the fight against spam has been met with an escalation on the part of the spammers, who are getting ever more sophisticated in eluding those who would track and stop them.

As an individual, the simplest thing you can do about spam is to ignore it and delete it when you find it in your mailbox. Unless you have the time to track down the sender of each and every piece of junk email you receive, you're not going to be able to do much. Just figuring out to whom to complain can take a good deal of knowledge about Internet message headers. You can't just hit the **Reply** button on your email software because chances are very good that your message will be going to another victim of the spammers, not the spammers themselves.

You can cut the amount of time you spend dealing with spam by collecting suspicious-looking email in a single location. Most modern email programs allow you to filter messages based on things like the contents of the subject line, what sites they are coming from, and so forth. If you watch the spam you receive for a few days, you may notice patterns, like lots of capital letters and exclamation points in the subject line, that allow you to have your email software set aside such messages. Don't just delete these messages before examining them by hand, however, because you run the risk of filtering a legitimate message once in a while.

If your local system administrator is gathering information on spam messages received, you can help him or her get needed information. If you are forwarding the spam to a central location, make sure you include the entire contents of the message, including *all* the message headers, such as the envelope-**From** address and especially the **Received**: headers. These headers are the

message's fingerprint, and without them it's impossible to determine with any certainty from where the message came.

Some people are trying to keep their addresses from getting onto spam lists in the first place by altering the address they use on outgoing mail and news posting--for example, using *webmaster@NOSPAM.basis.com* instead of *webmaster@basis.com*--and then including instructions for correcting the address in the body of their messages. This can cut down the amount of junk email you get, especially if you're a frequent poster to Usenet, but keep in mind that it also increases the difficulty of contacting you directly. Many people feel that this practice of "address munging" is harming, rather than helping, the general level of civility and communication online.

Corporate Countermeasures

Unless your company is a one-person shop, you'll probably find that your time is better spent stopping junk email from getting into your company than safeguarding individual mailboxes. You can apply the same filtering rules to mail coming into your company that you can apply to personal email boxes, with the caveat that when filtering email on a company-wide basis, it's even more important to make sure that you're not sidetracking or deleting email from legitimate customers.

You may find that rather than creating your own spam solution from scratch, it is more efficient and effective to adopt one designed and maintained by a third party, such as the Mail Abuse Protections System (MAPS) Realtime Blackhole List (RBL). The RBL is a list of IP addresses that are known to be sources of spam. Systems that use the MAPS RBL are configured to automatically refuse communication with any machine that is on the list--they will not accept mail, web, FTP, or any other kind of Internet connection from blackhole sites. This can pose some risks in a corporate environment, as it's possible that some of your legitimate customers may reside at sites that are on the blackhole list. But sites that are acting in good faith to reduce or eliminate spam from their IP addresses are removed from the RBL immediately. The MAPS website at maps.vix.com has more information about the rationale and mechanics behind the RBL, as well as detailed instructions for preventing the relaying of spam throughout the Internet.

At this writing, the first commercial anti-spam tools are also beginning to appear. The first one I've seen, called Mailshield (www.mailshield.com), allows the user to protect his or her server with a wide variety of email filtering rules, including an option to hook into the RBL.

Other Resources

Stopping spam is an activity that can quickly escalate from hobby to full-time job, as many system administrators may already be aware. Unless you have an inordinate amount of spare time, you may find that the best thing is to make sure you're not contributing to the problem in any way. Making sure your site doesn't relay email is an excellent start. And if you're interested in doing more, the following resources can help:

-
- Fight Spam On The Internet! spam.abuse.net
  The Coalition Against Unsolicited Commercial Email (CAUCE) www.cauce.org
- John Marshall Law School: Unsolicited Email Cases
  host1.jmls.edu/cyber/cases/spam.html
- The Net Abuse FAQ www.cybernothing.org/faqs/Net-abuse-faq.html

Spam...Spam...Monty Python...And Spam

The name for this new scourge of the telecommunications network--*spam*--comes indirectly from the canned meat product by way of Britain's Monty Python comedy troupe. When unwanted bulk advertising first started to become a problem in email and on Usenet, its online victims noticed a similarity between the seemingly endless flow of repetitive messages and the Monty Python sketch in which an innocent couple are subjected to a chorus of Vikings exalting a restaurant menu featuring virtually nothing but Spam.