Tame Junk E-Mail

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

Take Me Off Your Spam List!

If you're being lambasted with junk e-mail known as spam, you need to solve the problem. Not only does it expose staff to unsavory/unwanted messages, it steals time from productive assignments, it's a security risk and it can clog your e-mail system–or worse, shut it down — for legitimate users. Being aware of the mailers' methods can help you deflect future incoming junk e-mail.

Spam is the distribution of unsolicited commercial e-mail by mass mailing to millions of addresses. Addresses are attained in a couple of ways:

- *Blind spam* — Yours is one of myriad e-mail addresses randomly selected in hopes that it is "live." Many times these are computer generated according to mathematical formulas.
- *Cultivated Lists* — You give out your personal e-mail address over the Internet in response to a survey, filled in a form, joined a newsgroup, participated in a chat room, or joined a list group to name a few of the ways your address gets circulated. The spammers "mine" these lists for addresses to target.

What You Can Do

The bad news is you can't eliminate all junk e-mail. The good news is you can eliminate a lot of it.

Tips to Reduce the Flow

Here is some advice that will cost you $0.00 to implement.

1. *Never* randomly give out your personal e-mail address on the Internet.
2. *Do Not Open*, *Do Not Reply*, or *Do Not Remove* spam using the sender's instructions. If you do, you will alert the sender that the e-mail address is alive and well.
3. Guard your personal e-mail account from strangers, just as you do your home address. Don't give it out to anyone you don't know or trust.
4. Divert spam to a "junk e-mail" account. Create a separate e-mail account through a Web site that offers free addresses, such as www.hotmail.com. Give out that account *only* on the Web. Spam will flow to your junk e-mail account and not your personal online account.
5. Activate the spam blocking programs in your e-mail programs. Many are set up to block those containing certain subject lines that you identify and insert. [For more information on blocking junk e-mail through subject lines in your e-mail program, refer to www.pon.net/support.] This is an ongoing process.
6. Forward spam to your ISP (internet service provider), following instructions on its Web site. Many ISPs block spam at the server level.
7. Find out what methods your ISP uses to block spam at the server level: by identifying the sender or by message content — specific words or phrases, such as "mortgage," "sale," "free" etc.
8. Use a search engine [such as Google] to find organizations and companies that keep "blacklists," which contain ISPs and organizations that actively send spam and other junk e-mail. [A listing of blacklists is available at www.email-policy.com/spam-black-lists.htm.]

Technical Approaches for IT

A multilayered anti-spam strategy using a combination of content filters, white lists, and blacklists is the best way to get spam to cease and desist — at least in your organization's e-mail boxes. Solutions are based on 1) the identity of the sender or 2) the message content. Many strategies combine the two types. The solution can reside on the gateway, server or users. The server-based approach is the most seamless because it doesn't take up space on individual PCs or involve training. The following is summarized from

InfoWorld, July 21, 2003, pages 40-48, "Canning Spam," by Jon Udell.

Anti-spam technologies include:

Blacklists indicate who to keep out. Blacklists can create false positives of legitimate bulk mailings. (such as this e-news).

- Content filtering
- Digital certification of messages
- Digital postage
- White lists indicate who to allow to enter.

Types

Enterprise-oriented Products

Run inbound e-mail through a series of checks defined by organizational policy. You decide which identity or content-oriented spam-detection modules to use and whether to reject quarantine or tag a message that meets the checkpoints.

DNSBLs

A DSN-based blacklist keeps spammers from connecting to targeted mail servers. They look up a sender's IP (Internet Provider) address in databases that track and report spammers. Some anti-spam vendors ship their wares with DNSBL disabled and leave it up to the customer to enact it. Others use them by default, but as part of an overall score (for the spam message).

DNSWL

DNS-based white list is user driven. The system alerts the user to a potential piece of spam. The user indicates whether he/she wants to receive mail from this sender. The program "learns" the preferences of the user and checks content before allowing the message through in the future.

RMX (Reverse Mail eXchange)

A DNS MX record creates a mail route for a domain name. The domain owner uses RMX records to identify hosts within the domain that are authorized to send mail. The server receiving mail would check incoming mail against the lists and only allow entry to those listed. The other mail can be rejected or quarantined.

S/MIME (secure MIME) Digital Signature

An S/MIME allows digital signatures and encryption. Although digital signatures would plug holes in the system that leaks information through e-mail; encryption would not allow other anti-spam strategies, such as content analysis.

Legislation

State Laws

All states except Arkansas, Florida, Georgia, Hawaii, Indiana, Kentucky, Massachusetts, Michigan, Missouri, Montana, Nebraska, New Hampshire, New Jersey, New York, Oregon, Pennsylvania, South Carolina, Texas, and Vermont have some form of anti-spam legislation, according to Jon Udell. Some have been challenged on

grounds of free speech; some don’t allow individual action by recipients of ISPs, some offer the spammer more protection than the recipient.

Federal Laws

The response to the federal do-not-call list to harness telemarketing is spurring Congress to look at anti-spam legislation. Two competing bills (the Burr bill and the Wilson-Green bill) are under consideration, each with its own backers and detractors. Two differences keep consensus from being reached: 1) how to define spam: as legitimate commercial e-mail or as fraudulent e-mail, and 2) the rights of citizens to sue spammers. Layer onto this the viewpoints of the consumer constituents versus the ISP constituents: one wants peace of mind; the other wants a piece of the pie. For more information on this topic read: “Spam heats up Capitol Hill,” by Caron Carlson, *eWeek*, July 21, 2003, page 45; and “Throwing the Book at Spam,” *InfoWorld*, July 21, 2003, pages 42-43.