Written by Terrence O'Hanlon, ReliabilityWeb.com
Wednesday, 01 October 2003 20:30

For anyone who reads this column on a regular basis, you know that I rally against spam.

I define spam as a commercial e-mail message that did not come from a list that I subscribe to or do business with. The other common element is that the e-mail does not come from the company domain address, like sales@purplesocks.com. In fact, most spam does not include any contact information about the sender. Last but not least, I define spam as an offer that is of no real interest to me, like diet plans (perhaps I should be more interested in these messages), hair loss, my golf swing, long-lost classmates, Nigerian money laundering, and body part growth.

Spam has continued to multiply and now makes up more than 50 percent of all e-mail. Spam is worse than junk mail because it is often disguised as e-mail from a friend or other contact. Some of these messages carry files and programs that can be harmful to your computer by releasing worms or viruses. Some contain unwanted adult images that could be stored in your computer and cause problems at work.

At best, American workers spend at least some part of their day deleting spam rather than being productive. All of these problems are reducing the wonderful utility that e-mail provides. I am not willing to let a bunch of cyber-marketing miscreants muck up one of my favorite modes of communication. Spam must die!

Recent upgrades to AOL, Earthlink, and other popular Internet services include some basic spam filtering systems. Even if they are only 50 percent effective, this feature can still eliminate a large amount of unwanted e-mails. Of course, you should check your spam folder after each download to make sure that it has not grabbed opt-in e-mail newsletters and other e-mails that you want.

There are many choices for standalone spam filters, but most are based on rules that you must set up in advance to grab offending e-mails. As an example, most companies block e-mails with the word “free” in them.

But then you will not be getting much e-mail about free speech (a concept our country is built

on), a free maintenance seminar in your area, or a free white paper about reliability strategies. Most spam senders use fr*ee or other spaces and characters to avoid spam traps anyway. As much as I abhor spam, I do not feel that I should hand over control of my online communication to a kid in the corporate IT department who sets up my e-mail rules.

Imagine if you will a system that tracks what e-mails you delete as spam. It also tracks what e-mails I delete as spam and what e-mails 600,000 or more people are deleting as spam. When you, I, or 600,000 other people click “Delete” to remove a spam message from our inbox, it disappears from all our inboxes. Spam filtering rules that are defined by an online community of 600,000 people and are based on their actual spam-deleting behavior are rules I can live with. Enter SpamNet by Cloudmark .

SpamNet is a Microsoft Outlook add-in program that can be downloaded (there is a 30-day free trial offer) and installed automatically. When a spam message is reported by a SpamNet user, the message is sent to a central computer or database that records the spam. When other SpamNet users download their e-mail, the software checks the new messages to see if they contain reported spam. If the system finds a spam message, SpamNet moves it to the Spam folder. This process ensures that your inbox remains clean of spam messages and that none of your regular e-mail is lost or blocked.

Forget the rule-based spam filters and jump on board the SpamNet train. If you would have downloaded a free copy when I first wrote about it, you would be paying only $1.99 per month right now. If you waited, you can currently get SpamNet for just $3.99 per month. If you spend more than 1 minute per day deleting spam, your time is worth more than the service fee. Since I started using SpamNet I feel like I am plugged into a whole different Internet. Now my e-mail inbox is actually filled with e-mails I want to read. **MT**

INTERNET TIP: PRACTICING SAFE E-MAIL

The recent sobig worm and other nasty viruses are spread by e-mail from unprotected computers. The new pattern seems to be that when Microsoft announces a software patch that is related to security, the virus writers rush to release a program that can exploit the security flaw within 30-90 days after the announcement. They know a large percentage of users will not download the Microsoft patch.

This pattern will be with us well into the future, so please practice safe e-mail by installing antivirus software and updating it weekly. This will go a long way toward slowing the spread of viruses and worms. Antivirus software packages are available from Symantec or McAfee .

Joomla SEO powered by JoomSEF