5 WAYS TO BLOCK SPAM

Spam is one of those things that nobody wants, but probably has plenty of. If there happens to be anyone out there unfamiliar with spam, we are not talking about the luncheon meat, but the unsolicited, junk e-mail that clogs our inboxes. And in case you are curious, according to some sources, the junk mail version of spam earned its name from a Monty Python skit regarding the luncheon meat of the same name. Care to sing along?

From offers for prescription drugs, to mortgage refinancing, to sexually explicit content, spam can leave us having to sift through mounds of trash to find the few messages we actually care to read. Although eliminating all junk e-mail may be impossible, there are several steps than can be taken to all but eliminate spam from your inbox.

1. Protect Your E-mail Address

One of the best strategies for avoiding spam is to protect your personal e-mail address. Your best defense is for the spammers to not even know you exist, but this is a difficult task to accomplish.

Many spam mailing lists are created by harvesting e-mail addresses from websites where your information may be displayed. Newsgroups, bulletin boards, and chat rooms are just a few examples of places where spammers may run scripts to collect anything that resembles an e-mail address. Many sites, such as bulletin boards, have safeguards to protect their members, but it does nothing if these members post their personal information in one of their posts, their signature, or somewhere else that puts the information in plain sight. In addition, signing up with unknown sources for online contests, mailing lists, and similar occasions where you need to provide an address as part of the registration process may also expose your address to spammers.Using your best judgment is your best defense. If you want to keep your mailbox clean, keep your address private, only giving it out to trusted parties.

2. Create a Spam E-Mail Account

Protecting your e-mail address is easier said than done, and if you find that it is impossible to keep your personal e-mail address completely private, a separate account may be the solution. Referred to by some as a “throw-away” account, this e-mail account doesn’t have to cost you anything, as suitable e-mail accounts are available for free from places such as Hotmail and Yahoo.

This throw-away account is the best choice when you are unsure that your privacy will be protected. Use it when registering with newsgroups, bulletin boards, sweepstakes, or in any other situation where you’re not quite sure your privacy will be protected. You have to use your better judgment, as signing up for something from a trustworthy source, like the Computer Geeks mailing list, is much different than many things we’ll just leave to our imaginations.

Since you are not expecting any important mail at this account, if it becomes over run with spam, you do just as the name suggests and throw it away for a new one.

3. Message Rules in Outlook / Outlook Express

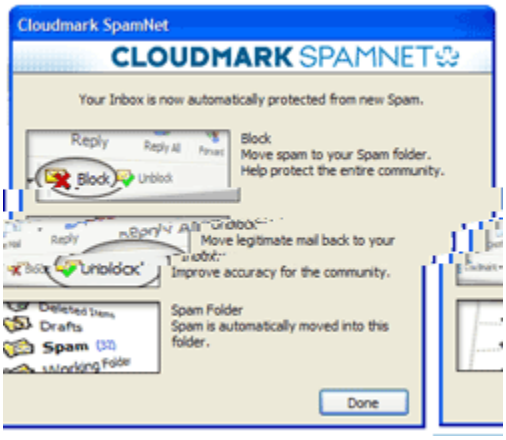
Most people use either Outlook or Outlook Express as their e-mail client, but all of these people may not be familiar with creating message rules in the “Tools” drop down menu. Rules allow you to manually filter the delivery of e-mail, and can be created to analyze the sender’s name, subject line, and message body before processing. For example, a rule can be created so that any message with a particularly offensive word in the subject line is automatically moved to the Deleted Items folder, or even better, just deleted from the server before download.

Another option provided by Outlook and Outlook Express allows the user to add senders to their “Blocked Senders” list. No rule needs to be created, and in a few clicks, a sender of unsolicited e-mail can be added to your personal blocked senders list. Whenever mail arrives from this sender in the future, it will skip the inbox and go straight to the Deleted Items folder.

Windows XP with Service Pack 2 provides even greater security in a variety of areas, including Outlook and Outlook Express. Many spam e-mails have images in the body that are coded to identify receipt of the e-mail. If the individually coded image has been viewed, the spammer knows that you have seen the e-mail, thus confirming your address as valid. With SP2, images are blocked to prevent your computer from being identified, thus keeping the spammer from confirming they have a valid address to continue mailing.

4. Third Party Software

There are numerous applications available for purchase, or as free downloads, specifically intended to filter spam as it enters your inbox. These programs identify telltale signs of a spam message by analyzing hidden tags in the message, use of text and images in the message, and various other clues available that point to a message being unwanted.



A few examples of spam filtering software is available from these three companies; SPAMfighter, MailWasher, and Cloudmark. Each offers its own twist on the interface and manageability, but they all allow users to take control of the spam in their Outlook or Outlook Express mailboxes.

The price tag on this type of software may involve a one time fee of $30 or more, and some come with annual subscriptions costing up to $40. If the free software doesn’t cut it for your tastes, these pay versions generally include a free trial so that you can be sure the program is right for you before you spend any money. The logic and data behind the spam filtering is constantly evolving, so these packages need to be kept updated, much like a virus scanning application, and this is where subscription-based offerings come into play.

5. Server Based Solutions

Most major internet service providers (ISP) now offer a spam filter as part of the package offered to its subscribers. AOL and Earthlink are just two of the big names out there that include a spam filter in with other attractive features like virus protection and pop up blockers. These ISP provide filters which effectively manage spam at the server before delivery, but they are generally not overly

customizable on the end user level, and they obviously only protect e-mail accounts provided by the ISP.

Protection similar to what an internet service provider offers can be implemented by just about anyone with their own domain name, and access to their server. Domain names and web hosting have become so cheap that it is not all that uncommon for people to have their own website, or at least a domain name for e-mail. SPAM Assassin is a no-cost, server based spam fighting solution that can be installed on a server, and has become a common feature included on many web hosting packages.

These solutions use various rules and logic to analyze messages, much like the third party software does, but it all happens at the server level. This keeps the message from having to be downloaded to be processed, thus saving time and precious bandwidth.

Source : http://www.geeks.com/techtips/2005/techtips-JUN30-05.htm