

Spam: What Can You Do to Stop It?

Spam...it's more than just canned meat. It's more than an inconvenience. It's a real threat to your computer system and to your privacy. If you use Microsoft Outlook or Outlook Express, you are at significant risk from potential damage to your system and invasion of your privacy. However, you are also at risk if you use Eudora, Yahoo, MSN Mail or other software packages.

So what is spam?

By definition, in order for a message to be considered spam, it should meet at least the following criteria:

A) Unsolicited, B) Undesirable and C) Sent from an individual or organization with which you have no previous or desired relationship.

Spammer Techniques

Much spam is received from e-marketers. They want to sell you something, and because they know that you'll probably delete a message that is clearly marked as spam, they try to disguise the subject line to look like a legitimate message. As a result, you open the message, and that's where the fun begins.

Many spam messages contain embedded scripts that perform an action when you open the message. Information can be collected about you and your system and sent back to the spammer or even mass-mailed to every person in your address book. Or, an action can be taken to delete critical files on your computer.

Pictures are frequently embedded into spam messages can also embed pictures that are actually not in the message itself, but located on the spammer's computer somewhere in West Woebegone. [These are known as "graphic beacons."] When you view the message by opening it or viewing it through the Preview Pane, information is sent back to the spammer indicating that they've got a "live one" and that they should add you to a larger list of addresses for future spam blasts.

Return receipts are frequently attached to messages. Accepting the receipt sends a message back to the spammer that his message was opened and read.

Spammers more and more frequently send their messages to individuals but put a fake name and address in the From field. If the message is rejected for any reason, the non-delivery report will be sent to you rather than the spammer. You may have already seen these non-delivery reports in your Inbox, wondering how they got there since you never sent the message and you didn't even know the recipient. Regrettably, there is not much that can be done about this at the moment.

So what can you do to protect yourself?

A. One very convenient feature of Microsoft Outlook and Outlook Express is the Preview Pane. It allows you to see the contents of an e-mail without actually clicking to open the message. However, embedded scripts or graphic beacons can be triggered just by viewing the message through the Preview Pane. Therefore, it's important to **disable the Preview Pane** on your Inbox, even though it reduces the "convenience factor." To disable the Preview Pane in Outlook, go to your Inbox and select "View | Preview Pane." If the pane was previously enabled, this will disable it. To disable the pane in Outlook Express, select "View | Layout" and clear the "Show Preview Pane" option. [You can ignore this step if you use Microsoft Outlook 2003, or Outlook Express 6 on Windows XP with Service Pack 2, both of which disable the beaconing feature of graphics.

B. Many spam messages contain a hyperlink or other instructions to remove yourself from their mailing list. Unless you know that the message is from a truly reliable source such as MicroData Group, Inc., **never actually follow the instructions to remove yourself from the list.** You will not be removed from any lists. Instead, you will actually be added to more lists, because by following their instructions, you have again told the spammer that they have a "live one" at your address.

C. Acquire anti-spam software. There are many software solutions designed to analyze mail and filter spam. Solutions include client-based software for the individual user as well as server-based software for the corporate environment.

Client-based software integrates into the mail application (Outlook, etc) and analyzes incoming messages. It will then perform an action that you have specified for the message, such as deleting the message or moving it to a specified folder for review. This latter option helps to avoid accidentally deleting any messages that you actually wanted ("false positives").

Server-based software performs the same function as client-based software, but it does so before the message ever gets to the end-user's computer. The actions are performed on a server and any quarantined items are placed in a location accessible by a network administrator.

You should be aware that no single solution can eliminate all spam. The best option is "defense in layers." Install server software to safely remove a significant fraction of inbound spam, but also install client software at the workstations to further reduce the amount of spam. Using both techniques, we have observed a greater than 95% reduction in corporate spam with the result of increasing users' productivity.