

Dealing with Spam

By: HSC Information Services

Spam is the common term for unsolicited e-mail. Advertising for products and services, particularly X-rated web sites, makes up the bulk of this but things such as chain letters and similar get rich quick schemes also contribute to the clutter in your in-box.

At HSC Information Services we are keenly aware of this increasingly annoying issue and we do take steps to block some of the flow at our firewall. In fact, roughly 20% of the mail directed at the HSC is blocked based upon content. This is done with the same application that scans mail for virus infection and executable file attachments which account for another 8% of total mail volume.

Unfortunately, the only ways we have to identify spam mail is by the address of the sender or the content. The originators of the spam are well aware of this and work to hide the actual points of origin and regularly change the verbiage within their messages, or insert their messages as images which cannot be scanned for content. As a result, because of the need to avoid setting such tight restrictions that legitimate mail is blocked, some spam mail will always get through. On a personal level, however, there are ways to deal with the spam you receive and to possibly avoid getting on spammers lists in the future.

Tactics for Avoiding Spam

1. First, please, ***never buy anything*** or respond in any way to spam e-mail.
2. Keep separate accounts for business and personal use. You may wish to keep more than one personal account. Yahoo, HotMail and others offer free mail accounts. Consider getting one of these and using it to receive mail from businesses whose advertising you do wish to receive (see 3).
3. When using any sort of e-commerce site watch for the check box, usually on by default, that requests/authorizes future notification of "special offers" by e-mail. Many legitimate companies sell their e-mail lists just as they do their old fashioned postal mail lists.
4. Be very wary of opt-out links in spam you receive. For example: "Click here to remove your name from our list." Spammers often use this ruse to identify working addresses and people who have actually opened and read some of their message. Know where that link is taking you before clicking on it.
5. Switch off automatic receipt sending to avoid confirming your address is active.
 - In Outlook you'll find this under Tools > Options > Preferences (click "E-mail Options" then "Tracking Options"). On the Tracking Options page clear all the fields in the top section and choose "Always ask me before sending a response" in the lower section.
 - In Netscape click Edit > Preferences > Mail & Newsgroups > Return Receipts. In the "When I receive a message..." section select "Return receipts for some messages" then click the "Customize" button, set the three options to "Never Send, Ask me, and Ask me respectively.

6. Ever wonder how BlueMountain.com made money with their free internet greeting cards? They get two working e-mail addresses for each card, yours and your unsuspecting friend. Blue Mountain isn't the only one, read the privacy policy statements before sharing your address. It is generally considered bad e-etiquette to pass out other people's addresses.
7. If you want/need to post your e-mail address to some internet forum, try posting it in "human-interpretable" form. For example, if your address is jdoe@hsc.usf.edu translate it to "my address is jdoe at hsc dot usf dot edu." People should be able to figure it out, but a machine scanning for things that look like e-mail addresses won't pick it up.

If You Are Currently Receiving Lots of Spam

1. Is your address posted on web pages? Spammers use special search engines to find addresses and mail-to links. Consider removing your address from web pages, or converting it to "human-interpretable" form, as suggested in 6 above.
2. If you also receive much "wanted" advertising from vendors you do business with, but are plagued by the unwanted variety, you should consider removing yourself from the lists of those desired vendors. Some may be selling their list.
3. Outlook and Netscape offer the option of running with the "preview pane" closed. Spammers often include web links in their junk mail that link back to web sites which confirm that you have received and viewed their mail. Try to identify the spam and delete it without opening or viewing. Without that confirming web connection they will probably stop trying at some point. To turn the preview pane off:
 - **In Outlook** click View, then Preview Pane to turn this on and off.
 - **In Netscape** click View > Show and then Message to turn this on and off.

Recognizing Spam in Your In Box

Most legitimate e-mail is from people with whom you have communicated before, or within organizations with whom you have dealings.

- If you don't recognize the address there is a good likelihood that it's spam.
- If the user name (the part before the @ symbol) seems to be random, probably numbers mixed in it's probably spam. Note: The presence of numbers alone doesn't automatically mark an address as spam, many sites with large numbers of accounts, including our own, create IDs of the form "jsmith5" when their normal naming scheme starts to overflow.
- The subject line usually reads like the advertising copy it is. Often with liberal use of capitalization or letter substitution.

Setting Filters

As discussed above, there are two ways to filter spam, by address or by content. While you can set your own filters for specific addresses this is unlikely to do a lot of good since the spammers keep changing the point of origin. What you can do,

however, is set filters for mail that contain specific words. This can provide considerable relief from some of the most offensive and profuse spam. However, you take the risk of blocking legitimate mail, so choose carefully.

At the firewall we scan for phrases rather than specific words. While we cannot block all e-mail that references Viagra, for example, you can set your own filter to eliminate offers for this specific pharmaceutical if you are pretty sure you won't be getting legitimate mail discussing it. Here's how:

In Outlook

- Click Tools > Rules Wizard.
- Make sure that "Inbox" is displayed in the "Apply changes to this folder:" field, then click the New button
- Select "Start creating a rule from a template" and highlight "Move messages based on content"
- In the Rule description pane click on the underlined "specific words" to open the edit window
- Here you can enter as many words or phrases inside quotation marks as you wish (you can edit it later as well) When finished adding words click OK to close the edit windows.
- Click the underlined word "specified" to open the edit windows telling where you want the mail moved
- Under Personal Folders highlight Deleted Items and click OK to close the edit window.
- Click Finish. You will be returned to the first Rules Wizard screen and you should see your new rule listed. You may modify this whenever you wish by opening the rules wizard, highlighting the rule, and clicking modify.

As you work through this the first time you will see that there are many other options that you could use to create similar rules based upon sender's name, address, etc.

In Netscape

- Click Edit > Message Filters
- In the Message Filters windows make sure "Inbox" is selected in the "Filters for:" pane, then click New
- Make up a name for your new filter.
- It is usually better to select "Match any of the following" rather than "Match all of the following"
- To filter messages where the word may appear anywhere within the message select "body" of the message and "contains" then enter the word or phrase you wish to filter.
- Select "Move to folder" and then select "Trash" and click OK to finish.
- You will return to the Message Filters window where you could select your new rule for editing at any time in the future.

As you work through this the first time you will see that there are other options that you could use to create rules based on senders name, address, subject, etc.

Tracing and Reporting Spam

This is usually a difficult and time consuming task. And, unfortunately, it is often impossible to find the actual spammer since they have learned to hack the systems of unsuspecting third parties and plant their mail forwarding programs on their computers. However, if you can determine the origin of the spam, most internet service providers (ISPs) will do their part to block the source. USF Academic Computing has a document that describes the process of deciphering mail headers and reporting spammers, a link is provided below along with a few other links to anti-spam and spam tracking organizations.

[USF Academic Computing Spam FAQ](#)

[Network Abuse Clearinghouse](#)

[Sam Spade](#) – Tools for tracing spammers

[Google Spam Directory](#) – For even more resources