

Reducing Email Spam

How to Use Spam Trap at Ithaca College

What is Spam?

Spam is unsolicited mass-mailed email, usually containing advertising. Spammers send their messages to large numbers of addresses, often obtaining those addresses without the permission of the address owner. If you use email, you have probably received spam. You can either delete spam from your account when it arrives, or use Spam Trap software at spamtrap.ithaca.edu to help control spam before it is received in your inbox.

Using Spam Trap

Spam filtering is not 100% effective. By choosing to activate spam filtering on your account and selecting the option to reject suspected spam, you are acknowledging that valid email messages could possibly be rejected by the system (and subsequently not be delivered to you). In addition, regardless of which level of filtering you choose, some unwanted spam messages may still be delivered to your account. ITS recommends that you "tag suspected spam" messages for several weeks to see what messages are being flagged as spam before you choose the option to reject suspected spam messages. Please also keep in mind that internal Ithaca College-to-Ithaca College email and email destined for off-campus does not pass through spam trap, and is not possible to filter for spam. You can take a look in the message headers to see if the message passed through spam trap or not. By having spam trap tag messages as *spam*, some email programs can then filter and delete them. Using the rule settings the sender or origin of spam can also be used to reject or allow all email from that source. See the **Terminology** section of this guide for more information.

Setting the Scanning Level

To access Spam Trap, go to <http://spamtrap.ithaca.edu/> and log in with your e-mail username and password. You also may access your Spam Trap settings when you are using Webmail within myHome. You will find the Spam Settings link on the Webmail banner, just to the right of the Options link.

Select the desired level of scanning from one of the two radio buttons provided and then click the **Set Spam-Scanning Level** in order to take affect. The scanning level will remain in place and there is nothing further you need to do unless you want to set specific rules using Accept lists and Reject lists. Descriptions of the basic spam scanning options are listed below:

Options

Tag suspected spam with *SPAM* in the subject line, but deliver it as usual

This option will modify the subject line of any suspected Spam message by adding [Spam: *****]. The number of asterisks indicates the (bad) points the message received. If, after several weeks, you are satisfied with how Spam Trap handles your mail, then go back and select **Reject suspected Spam and return it to sender**. (See below)

Reject suspected spam and return it to sender

This option will instruct Spam Trap to reject suspected spam immediately so you will never see it in your inbox.

In This Guide

What is Spam?	Page 1
Using Spam Trap	Page 1
Terminology	Page 2
The Sender/Domain Action Table	Page 2
Bulk Blacklisting and Whitelisting	Page 3
Tips for Using Spam Trap	Page 4
For More Information	Page 4

Quick Guide

Terminology

Before setting specific rules, it's important to understand some of the terms used in the Spam Trap interface.

Senders - A sender is the specific email address for which you want to set a rule. (such as jdoe@hotmail.com).

Domains - A domain is a name, such as aol.com, that is assigned by the Domain Name System (DNS). The domain name serves as an alias to an IP address of a specific system on the Internet.

Reject – Rejecting is the publication of a group of domain names or sender addresses that you know to be sources of spam (the “bad guys”). Rejecting provides a way to block spam by denoting its origin as a sender of spam.

Accept – By accepting someone a list of the “good guys” is created in Spam Trap. You can accept domain names and email addresses from which you would like to receive email. Messages from accepted sources will always go through, no matter what your spam scanning level is set to.

Actions

If you want to set rules on specific senders or domains, there are various actions you can set.

No Change – Keep the current action.

Always Allow – This setting will “always allow” emails sent from the specified sender or domain no matter what your spam scanning level is set to.

Hold if looks like spam – This is the default setting. Mail from this sender will be held if it scores high enough on the spam scale.

Always Reject – This setting will “always reject” emails sent from the specified sender or domain no matter what your spam scanning level is set to.

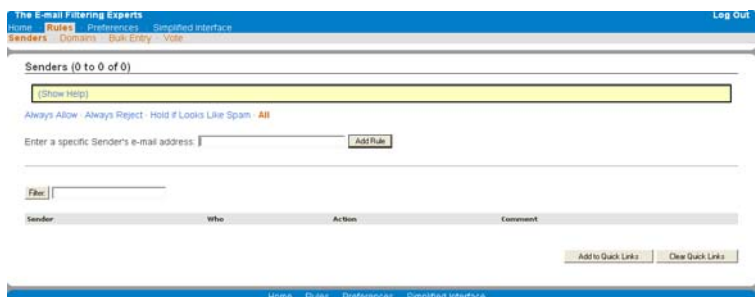
Delete from Table – The **Delete from Table** option will remove any sender or domain set in your Rules.

The Sender/Domain Action Table

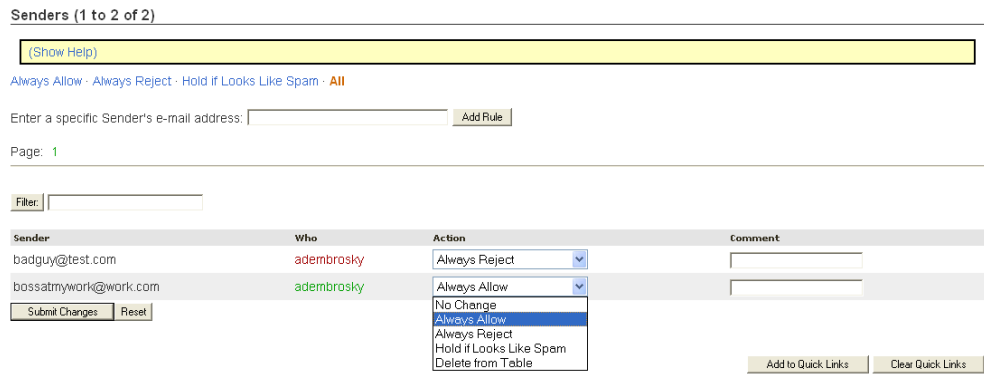
Use Rules to create Accept lists and Reject lists to block or allow all messages from a specific sender or domain. Email from sources that are put on an Accept list or Reject list will not be tagged; they will either be allowed completely or rejected completely.

1. From the main Spam Trap interface, click on the **Enable Expert Interface** button.
2. Click on the **Rules** link below the Email Filtering Experts.
3. Click on the **Senders** or **Domains** link to choose the desired source type of email to block or allow. To view senders or domains that you have already added, click on the **Allow-Always**, **Reject**, **Hold if Looks Like Spam** or **All** links. The **Bulk Entry** link can be used to paste several domains or addresses into the system at one time. See the **Bulk Entry** section of this guide for more information.

Blacklist a Sender



4. Type the sender or domain address into the presented field and click on the **Add Rule** button. The sender or domain will be saved in Spam Trap and more information will be displayed onscreen so you can set whether messages from this source should be delivered or blocked.



5. Under **Action**, use the drop-down list to select the desired action to perform on email from the selected sender or domain.
6. If desired, type a comment as a reminder of what the source is or how Spam Trap is handling email from this source.
7. Click on the **Submit Changes** button to apply the selected settings.
8. To return to the simple user interface after the desired settings are in place, select the **Simplified Interface** link at the top of the page.
9. If you are done, click on the **Log Out** link to log out of Spam Trap.

Changing Actions for Senders and Domains

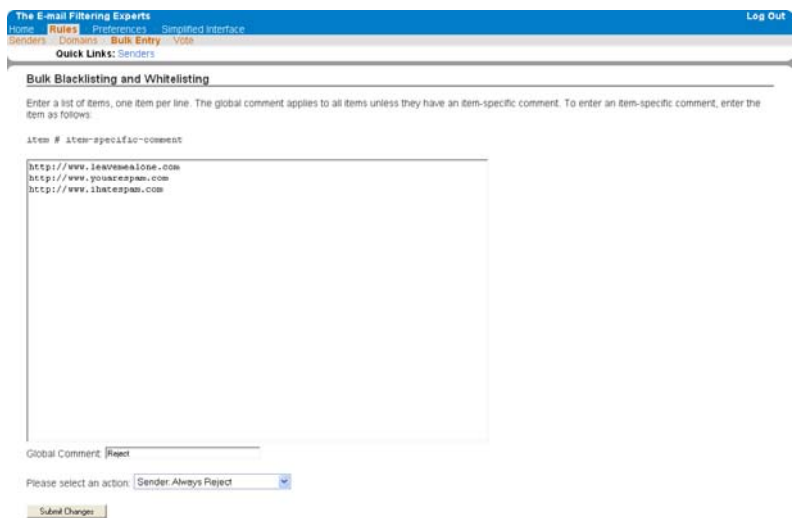
Remember, you can log back in at any time to change spam scanning settings. Click on the **Rules** link, specify whether you would like to see the senders or domains you have entered into Spam Trap by clicking on the appropriate link and then click on the **Allow-always** link, the **Reject** link, the **Hold if Looks Like Spam Link** or the **All** link to view items stored in Spam Trap. To change an action, choose a new action from the **Action** drop-down menu and click on the **Submit Changes** button.

Bulk Blacklisting and Whitelisting

To save time when entering many items, specify multiple senders and/or domains using bulk entry blacklisting and whitelisting.

1. From the main Spam Trap interface, click on the **Bulk Entry** link.
2. Type or paste domains or addresses into the text field. The list used must be all domains or all addresses; they cannot be mixed in the same window.
3. In the **Global Comment** field, type a comment that describes what these addresses are and/or what is being done with them by Spam Trap.

Bulk Blacklisting and Whitelisting



4. Select an action from the list. Be sure to select an option that applies to the type of source you have listed. For example, to allow senders, select **Sender: Always Allow**; to block domains, select **Domain: Always Reject**. If an option is selected that does not correspond to the type of source (domain or sender) in the list, the changes will not be applied, even though a message stating that changes have been made may be displayed.
5. Click on the **Submit Changes** button to apply the selected settings.
6. To return to the simplified user interface after the desired settings are in place, select the **Simplified Interface** link at the top of the page. If you are done, click on the **Log Out** link to log out of Spam Trap. Remember, you can log back in at any time to change any of your spam scanning settings.

Tips for using Spam Trap

If you subscribe to a newsletter that contains advertising, Spam Trap might tag or reject messages from that newsletter as spam. To ensure that you continue to receive such messages, add the sender (such as **editor@xyz_company.com**) or domain (such as **xyz_company.com**) to your Accept list.

If you signed up for an email newsletter and can't seem to unsubscribe from it, you can prevent the newsletter from being delivered to your email account by adding the sender (such as **editor@xyz_company.com**) or domain (such as **xyz_company.com**) to your Reject list.

For More Information

For more information on Spam Trap, go to the go to the ITS Support Site at <https://www.ithaca.edu/computing/support/>. For additional help, contact the ITS Helpdesk at helpdesk@ithaca.edu or 4-3282.