Anti-Spam Processing at UofH

The university's email system is protected by an anti-spam device that helps stop spam from being delivered to your mailbox.

Features are:

- Allows you to choose whether or **not** to have your mail scanned for spam
- Allows you to choose how **aggressively** your mail is scanned for spam
- You choose whether messages suspected of being spam are **tagged and delivered** to your account, or are **held** on the anti-spam system for your review
- Allows you to "whitelist" email addresses to assure that mail from people you **know** are received without risk of being blocked

How it works

About once per day, you will receive an email from "University of Hartford Spam Firewall" containing a report of email messages sent to you that have been classified as suspected spam by the firewall, and have been blocked from delivery to your mailbox. (If you have not received any messages that have been quarantined as suspected spam, you will not receive a report.)

Sample report email message

From:	University of Hartford Spam Firewall
Date:	Sunday, January 23, 2005 3:35 PM
To:	kelley@uhavax.hartford.edu
Subject:	Spam Quarantine Summary

University of Hartford SPAM FIREWALL

Spam Quarantine Summary
See http://uhaweb.hartford.edu/spam for help with the Spam Firewall.

Account: kelley@uhavax.hartford.edu

This is your quarantine summary from the University of Hartford Spam Firewall.

You have **1** messages in your spam quarantine inbox.

- Click on the **Deliver** link to have a message delivered to your mailbox.
- Click on the **Whitelist** link to have a message delivered to your mailbox and whitelist the sender so that his/her messages will no longer be quarantined.
- Click the **Delete** link to have the message deleted from your quarantine.

	Messages older than 30 days will be removed

Time R...	From	Subject	Actions
01/22 17:18	David Kelley <kelleydave@gm...	Test 9	Deliver Whitelist Delete

To view your entire quarantine inbox or manage your preferences, click here.

Spam/Virus Protection By BARRACUDA NETWORKS

You can judge whether or not a message is spam by looking at who the message is **From**, and at the **Subject** as shown on the report. If you only have a few messages to review and process, you can just click **Deliver**, **Whitelist**, or **Delete** as you see fit using the links under the **Actions** column of the report. If you have a lot of messages to review and process, or if you want to change the way the system processes your mail, you can click the "**click here**" link at the bottom of the report. This will log you directly onto the system via a web browser.

Logged onto the firewall system

What makes logging on to process large numbers of messages more efficient is that you can use the checkboxes to the left of the screen to select many messages and then process them *all* with the single click of the **Deliver**, **Whitelist**, **Delete**, **Classify as Not Spam**, or **Classify as Spam** buttons above the report headings. If you're not sure what do to with a message based on its origin or subject, you can preview it by clicking on its **From** address or its **Subject** -- the message will be displayed in a pop-up window.

What the buttons do:

Deliver	Delivers message to your mailbox, removes it from quarantine.
Whitelist	Delivers message to your mailbox, removes it from quarantine, and adds the sender's email address to your "whitelist" so that future messages from this address will **not** be categorized as spam again.
Delete	Deletes the message without sending it through to your mailbox

Classify as Not Spam	Delivers message to your mailbox, removes it from quarantine, and helps "train" the firewall that this kind of message is not spam.*
Classify as Spam	Deletes the message without sending it through to your mailbox and helps "train" the firewall that this kind of message is spam.*

    * A copy of the message is uploaded to the firewall vendor, Barracuda Networks, so that their anti-spam definitions can be updated to help block this type of message in the future.

When you are done working on the firewall, you should click the "**Log Off**" link in the upper right corner of the web page.

Taking control

By default, the Spam Firewall will filter your email using settings and preferences set up for you by University of Hartford Office of Technology Services. You may find the default settings too "aggressive" (the system classifies too much "good" mail as spam), or too weak (too much spam still gets through). No filtering system can decide perfectly what *you* would consider to be spam, and what you would not. However, you now have some control over the process! When logged onto the system as shown above, you can modify how the system processes your mail by selecting the "**PREFERENCES**" tab along the top.

The PREFERENCES -- Whitelist/Blacklist screen

On the Whitelist/Blacklist screen, you can add email addresses of people whose email you never want to have filtered by the Spam Firewall by adding them to the **Allowed Email Addresses and Domains** whitelist. (Addresses are also added here if you click the **Whitelist** button as described earlier.) You can also block all email from a specific address by adding it to the **Blocked Email Addresses and Domains** blacklist.

Don't want your suspected spam blocked at all? Click the **Quarantine Settings** button along the top.

The PREFERENCES -- Quarantine Settings screen

If you want to turn off blocking of suspected spam, just set **Enable Quarantine** to "**No**" and click the **Save Changes** button. You can turn it back on again anytime you like. When Quarantine is disabled, messages suspected of being spam are sent along to your mailbox anyway, with the subject line modified to contain the phrase "**[QUAR]**" at the beginning. When Quarantine is enabled, the messages are held on the Spam Firewall to be processed as described above.

Quarantine Notification Frequency
You can now set how often you'd like the firewall to notify when you have messages waiting in quarantine. By default, the firewall will send you a message once per day. You can change the setting to once per week, or to never send you notices (you'd have to manually log onto the firewall from time to time to check for quarantined messages). Note that the firewall will only hold messages in quarantine for up to 30 days (subject to change).

Don't want your mail checked for spam? Or, do you want to change the threshold of "spammy-ness" that the system uses when scanning your mail? Click the **Spam Settings** button along the top.

The PREFERENCES -- Spam Settings screen

If you don't want your mail scanned for spam at all -- perhaps you're having difficulty receiving a legitimate message from someone, or don't like the idea of having a machine sort through your mail -- just set **Enable Spam Filtering** to "**No**" and click the **Save Changes** button.

Want to change the thresholds at which the system classifies a message as spam? Set **Use System Defaults** to "**No**", **click the Save Changes button,** and then change your settings as described below.

The system assigns a "spammy-ness score" to each message it examines using several methods including, blocked network addresses, messages originating from known spam senders, messages containing spam-like "fingerprints" (as reported by you and other users with the **Classify as Spam** button described earlier), intention analysis, Bayesian

analysis, and rules (banned phrases and attachments). The score can range from "0" (system does not think the message is spam at all) to "9" (system really thinks the message is spam). You can control what the system does with the message, depending on how high (spammy) the message's score is. In the example shown above, the **Tag score** is 2.5, and the **Quarantine score** is 3.0. This means that any message whose score is *below* 2.5 will be forwarded to your mailbox as usual. Any message with a score between 2.5 and 3.0 will be "tagged" -- its subject line will be modified to start with "**[SPAM?]**" and forwarded to your mailbox as usual. Any message whose score is between the **Quarantine score** and the **Block score** will be quarantined as you specified -- either held on the firewall awaiting your decision about what to do with it, or passed along to your mailbox tagged with "**[QUAR]**" added to the subject line (if you've disabled quarantine). Any message with a score of 9 or higher will simply be bounced back to the sender without your ever having to deal with it.

Note: Even though the **Tag**, **Quarantine**, and **Block** scores *appear* to have "sliders" next to them, they are simply a visual representation of your setting - you can't slide them. To change a score, enter it in the box (it may contain a decimal) and click **Save Changes**.

Note: You can disable the quarantine function by setting the **Quarantine score** to 10.

Note: If you don't want any chance of blocking a message based on its spam score, set the **Block score** to 10.

When you are done working on the firewall, you should click the "**Log Off**" link in the upper right corner of the web page.

Want to change your Spam Firewall password? Click the **Password** button along the top.

The PREFERENCES -- Password screen

If you'd like to check your Spam Firewall quarantine without waiting for your daily quarantine report email message, you can log in using the password sent to you by the firewall. The automatically generated password is usually your email name followed by several random characters. You can change it to something more memorable (perhaps set it the same as your email password?) by filling out the screen above and clicking **Save Password**.

Don't know your password? Just go to the Spam Firewall's login page at http://barracuda.hartford.edu:8000.

Spam Firewall Login Screen

Just enter your email address in the **Username** field and click **Create New Password**. The Spam Firewall will send you an email message containing a newly generated password which you can then use to log in and set to one of your own choosing.

From:	University of Hartford Spam Firewall
Date:	Sunday, January 23, 2005 7:58 PM
To:	kelley@hartford.edu
Subject:	User Quarantine Account Information

Welcome to the University of Hartford Spam Firewall. This message contains the information you will need to access your Spam Quarantine and Preferences.

Your account has been set to the following username and password:
Username: kelley@hartford.edu
Password: kelleyhf4r

Notes

1. You should log onto the Spam Firewall at least once every few days and process any messages held in quarantine. Messages left in quarantine longer than 30 days (subject to change) may be deleted and are not recoverable. If you do not wish to process your quarantine folder, please disable quarantine for your accounts as described above so that messages do not build up on the firewall.
2. The University has had several email addressing schemes over the years, namely "@hartford.edu" (the current address), "@mail.hartford.edu", and "@uhavax.hartford.edu". If you are still receiving messages at the older addresses, a separate Spam Firewall account will be automatically created for each of them, and you will have to check each of them individually. You will receive a separate Spam Quarantine Summary email for each account, if they receive quarantined messages. (Fortunately, the messages contain a web link that connects you directly into your account on the firewall without logging in.) There is currently no way to combine the addresses/accounts on the firewall.
3. Please bear with us as we make adjustments to the new system. As with any new system, there may be "bumps" along the way!
4. Note that no anti-spam mechanism is perfect. If you do not like the way the system works, you can opt out of it, or adjust its behavior, as described in this document.
5. If you have questions about the system, please contact the Help Desk at 860.768.4357 (HELP), email HELPDESK@hartford.edu or drop by the Computer Support Center in CC113.