IronMail Anti-Virus/Anti-Spam

SPAM

ITS has evaluated and chosen an anti-virus/anti-spam (AV/AS) appliance to help protect your UNI e-mail account from unwanted mail. The chosen appliance is known as IronMail and is provided by CipherTrust. Ironmail is consistently ranked at or near the top of most evaluations of anti-virus/anti-spam solutions. We have purchased two of these devices, for both load-balancing and redundancy.

The appliances evaluate all mail passing through them for both viral and spam content:

- Viral determination is done via a Sophos engine and is based upon Sophos virus signatures. New signatures are downloaded automatically from Sophos numerous times per day as they become available.
- Spam determination is done via a series of tests, each of which contribute to the spam "score" of the message. The higher the score, the more likely the message is to be spam.
- Messages that are determined to be spam will be quarantined (held) on the IronMail appliances. Users will receive daily quarantine summary message(s) from the appliances listing those messages that have been quarantined during the past day. That summary message will contain an explanatory paragraph, a URL to all of the user's currently quarantined messages, and, in a list format, contain the following for each message quarantined since the last summary message:
    - A link to release the message for delivery to your mailbox
    - Sender
    - Subject
    - Size
    - Time stamp
- The URL leads to a webpage on the IronMail appliance that contains a listing of each quarantined message, along with options to release, delete, and/or whitelist. Whitelisting a sender means that future mail from that sender will not be subject to quarantine for spam content.

Five different options are available:

- DEFAULT: Discard all messages with viral content and quarantine messages likely to be spam.
- QUARANTINE LESS: Discard all messages with viral content and quarantine messages with a higher spam score.
- QUARANTINE MORE: Discard all messages with viral content and quarantine messages with a lower spam score.
- TAG ONLY: Discard all messages with viral content and add the tag "[spam]::" to the subject header of messages likely to be spam. Tagged messages will not be quarantined and will be delivered to the user's mailbox. The score used to tag messages will be the same as used for DEFAULT quarantining.
- BYPASS: Discard all messages with viral content and deliver all other messages untouched, without any tagging or quarantining.

It is strongly suggested that users remain in the DEFAULT group for a period of at least 2-3 weeks. This will give you a good feel for the behavior of the appliances. Users will have the option to vary from the default actions if they see fit. Due to the manual procedures needed to facilitate those changes, **repeated** requests for changes in handling are strongly

discouraged. To request a change from the DEFAULT group, send an email message to IronMail@uni.edu [1] and specify the group that you would like to be placed in. For additional information about using the IronMail devices, visit Spam Support. [2]

Source URL: http://www.uni.edu/its/support/article/574

Links:
[1] mailto:ironmail@uni.edu
[2] http://www.uni.edu/its/support/spam