Understanding Junk E-mail filtering & Anti-Spam controls

Overview: the antispam defenses at ODU are a two layered approach. Our first wall of defense is called Spamtrap, and it can be accessed at https://spamtrap.odu.edu by logging in with your MIDAS ID & password. The second wall of defense is the Outlook Junk E-mail filtering, which controls whether emails are delivered to your Inbox, or filtered into the Junk E-mail folder.

Spamtrap

What Spamtrap does is read incoming emails, and based on the content, the format, where it was sent from, and a variety of other metrics, it assigns a score to that message.

The higher the score of an email, the more likely it is to be spam. As a general rule, messages that score between 1 - 5 points are very likely to be not spam. Messages that score 5 - 10 points might be spam, or they might be legitimate emails with a few embedded images, HTML, or links to website. Messages that score 10 – 15 points are likely to be somewhat spammy, but they could also be newsletters, list-serv messages, or emails sent from countries that have a high volume of spam sent from them (such as China or Russia). Messages that score above 15 points are almost never legitimate, and emails that score above 20 points are usually the worst of the worst (Viagra ads, phishing messages, email scams, etc).

Based on the score of the email, Spamtrap will do one of three things: 1) allow the email to go through to your Inbox, 2) tag the message with “[Spam:” and then the score of the message in the subject and filter it into your Junk E-mail folder, or 3) reject the email and bounce it back to the sender.

Emails that are tagged with “[Spam:” and filtered into your Junk E-mail folder will look like this:

<table>
<thead>
<tr>
<th>From</th>
<th>Subject</th>
<th>Received</th>
<th>Size</th>
</tr>
</thead>
</table>

The score at which Spamtrap will begin tagging the message is called the “tagging level”, and the score at which Spamtrap will reject the message is called the “rejection level”. Each user’s Spamtrap account can have customized tagging & rejection levels.
To log into Spamtrap, go to https://spamtrap.odu.edu and then log in with your MIDAS username & password.

If this is the first time that you have ever logged into Spamtrap, you will see the "Simplified Interface" which just allows you to select a pre-configured set of tagging & rejection levels for your account.
For most people, we would recommend using either the “Medium+Tag” or the “Low+Tag” settings. The “Medium+Tag” setting tags messages that score above 7 points, and reject messages that score above 12 points, which is good for most people. The “Low+Tag” setting tags at 10 points, and rejects at 20 points, which is good for people that may receive a lot of newsletters, list-serv messages, or correspondence in foreign languages. We only recommend using the “High” or “High+Tag” settings for those users who have very little contact with people outside of ODU, as it will reject most spam, and some legitimate emails. You can select the option that best meets your needs.

You can also choose to use the "Expert Interface", where you can customize the tagging & rejection levels, whitelist senders or domains, and many other custom features.

**Using the Expert Interface**

1) To use the Expert Interface, first click the “Enable Expert Interface” in Spamtrap.

2) Within the Expert Interface, there is a lot that you can configure. The two most important sections are under Rules (for whitelisting senders & domains) & Preferences (for setting the tagging & rejection levels).

3) To set your tagging & rejection levels, click on Preferences, then Stream Settings.

4) On the Stream Settings page:
   “S-100 Automatically reject messages scoring more than this amount”: this controls the score above which emails will be automatically rejected.
   “S-300 Spam threshold”: this controls the score above which emails will be tagged as spam in the subject line.
5) To whitelist individual email addresses, click on Rules, then Senders.

6) On the Senders page, enter in the address that you would like to whitelist, then click the Add Rule button.

7) Then under the Action drop down menu, select “Always Allow” if you would like emails from that sender to never be filtered or rejected as spam. Then click the “Submit Changes” button.
8) To whitelist domains, click on Rules, then Domains
9) Enter in the email domain that you would like to whitelist, and then click "Add Rule".

10) Under the “Action” drop down menu, select “Always Allow”, then click “Submit Changes”.
Junk E-Mail in Outlook 2010

As mentioned above, the Outlook Junk E-mail filters are your second layer of defenses against spam. What these filters do is filter possible spam emails to your Junk E-mail folder in Outlook.

Emails that are filtered into your Junk E-mail folder are kept for 30 days by default, and then automatically deleted. As a general rule, we recommend checking the items in your Junk E-mail folder periodically to make sure that nothing legitimate was filtered into that folder. When items are delivered to your Junk E-Mail folder, a number will appear next to the folder indicating that there are new emails there. Antispam filtering is more of an art than a science, and sometimes legitimate emails do get filtered, so please make sure to check that folder occasionally.
To modify your Junk E-mail filtering settings in Outlook, click on the Junk button which is under the Home tab.

Then select Junk E-mail Options.
On the Junk E-mail Options window, you can select the level of antispam filtering that you would like.

Choose the level of junk e-mail protection you want:

- No Automatic Filtering. Mail from blocked senders is still moved to the Junk E-mail folder.
- Low: Move the most obvious junk e-mail to the Junk E-mail folder.
- High: Most junk e-mail is caught, but some regular mail may be caught as well. Check your Junk E-mail folder often.
- Safe Lists Only: Only mail from people or domains on your Safe Senders List or Safe Recipients List will be delivered to your Inbox.

- Permanently delete suspected junk e-mail instead of moving it to the Junk E-mail folder

- Disable links and other functionality in phishing messages. (recommended)

- Warn me about suspicious domain names in e-mail addresses. (recommended)
If you click on the Safe Senders tab of the Junk E-mail options window, you can add individual email addresses or domains to your “Safe Senders” list. Emails from addresses that are added to the Safe Senders list will not be filtered as spam unless they have “[Spam:” in the subject line.

We highly recommend that you select the two options for “Also trust e-mail from my Contacts” and “Automatically add people I e-mail to the Safe Senders List” for best results.
You can also whitelist emails by right clicking on them, then selecting Junk, then the appropriate setting.