

Eastern University Spam and Virus Filtering

Introduction

One of the growing annoyances in the world of e-mail has been the proliferation of unsolicited commercial e-mail, known as “spam”, and e-mail viruses. Spam is the e-mail equivalent of “junk mail” or telemarketers calling you during dinner. Unfortunately, spam is extremely difficult to control, as it costs very little to send, and is generally sent by “fly-by-night” operators using temporary e-mail accounts.

Hopefully, you have seen a dramatic decrease in spam and e-mail viruses. Eastern University has implemented a system named “Barracuda”, hosted by a company named Tangent, that attempts to remove spam and viruses before you ever see them. While this system is largely automatic and requires no action by the e-mail account holder, this document is designed to explain how the filtering works, and provide methods for “fine-tuning” the filtering, if desired.

How it works

Each e-mail message you receive from the “outside” (i.e. not sent by a person using an Eastern University account) is examined and given a “spam score”. Messages with spam-like characteristics, for example the word “mortgage” or many exclamation points, receive a higher spam score. What happens to the message depends on its overall spam score, based on a 0-10 scale:

Spam Score	Action
0-2 (Low spam score)	Message is sent without modification
2-5 (Moderate spam score)	Message is sent with the prefix [BULK] in the subject line
5-9 (High spam score)	Message is sent with the prefix [QUAR] in the subject line
9 and above (Extremely high spam score)	Message is not delivered, and is returned to sender.

In our testing, most “real” messages score in the 0-2 range, with bulk e-mail messages such as corporate newsletters, and opt-in mailing lists scoring in the 2-5 range. Nearly all e-mail we’ve seen in testing above 5 has clearly been spam.

E-mail messages from the outside are also scanned for viruses. E-mails containing viruses are always blocked. As with spam, this cannot be 100% effective, but it should result in a vast decrease in the number of e-mail viruses received. **You should, however, remain vigilant regarding e-mail attachments, and should never open or click on an e-mail attachment unless you were expecting it – even if the sender is known to you. Instead, call or e-mail the sender to verify that the attachment is legitimate.**

Is this thing going to “eat” my mail?

The short answer is “almost certainly no”. The system, as currently configured, is designed to err on the side of caution. It is extremely unlikely that legitimate e-mails will score above 9 and be blocked. It is probable that nearly all the e-mails you receive marked “[QUAR]” will be spam.

What do I have to do?

The system is largely automatic, and so will block the majority of spam and viruses without any action. The mail filtering can, however, be customized in various ways, such as whitelisting/blacklisting particular e-mail addresses, and setting up e-mail to be “quarantined” in an area outside your e-mail account. To do this, an account needs to be set up with our spam filter provider, Tangent, which is described below.

Fine-tuning e-mail filtering

Most users will probably never need to fine-tune the spam filtering system. For advanced users, however, it is possible to customize it in several ways.

For messages marked as “[BULK]”, probably the best approach is use your e-mail program to set up a mail filtering rule to automatically place the e-mail in a separate folder, which you can then review periodically for legitimate messages. Because setting up such rules vary from e-mail program to e-mail program, consult the documentation of your e-mail program for more information.

For e-mails marked “[QUAR]” there are two options. The first is to set up a mail filtering rule, similar to what is done for “[BULK]”. The second is to set up an account with Tangent which will “quarantine” the message. This means that the messages that would have been sent to you with a “[QUAR]” tag will instead be held by Tangent, allowing you to peruse them at your leisure. Setting up an account at Tangent also allows you to whitelist/blacklist particular e-mail addresses.

Some definitions of terms:

Whitelisting: Marking an e-mail account as one which you always wish to receive e-mail from. E-mail from whitelisted addresses is not checked for spam, although it is still scanned for viruses. If you have trouble receiving e-mail from a particular person, whitelisting their e-mail address should solve the problem.

Blacklisting: Marking an e-mail account as one which you never want to receive e-mail from. E-mail from blacklisted addressed is always blocked, and you will not receive any e-mail sent from that account.

Quarantine: The placement of an e-mail in a special off-site repository. You can configure the quarantine such that you receive daily or weekly messages describing the contents of the quarantine repository, with simple steps to allow or deny delivery. Quarantined mail will eventually be deleted if no user action is taken.

Setting up a Tangent Account

- 1.) Go to <http://tcnoc.com/clientlogin.htm>
- 2.) To create a new account, enter your e-mail address and password (twice) and click “create”. You will then see a message from Tangent informing you that an e-mail has been sent to your submitted e-mail address. **This e-mail contains the username and password you will need to access your Tangent account. The password you submitted to Tangent may be slightly modified for security purposes.**
- 3.) Once you have received your username and password from the Tangent e-mail, go to <http://ms18.tcnoc.com/cgi-bin/index.cgi> and type in your email address as your username and the password they have supplied you and then click “Login”.

4.) Once you have logged in, you will see the following screen. Notice the tabs at the top.

tangent
To create an account on our service please [CLICK HERE](#)

Log Off [dwilsono@eastern.edu](#)
English (US)

QUARANTINE INBOX **PREFERENCES**

Quarantine Inbox Refresh Filter: None Pattern: Apply Filter

Deliver Whitelist Delete Classify as Not Spam Classify as Spam

<input type="checkbox"/>	Date Received	From	Actions
<input type="checkbox"/>	03/18 08:48	NYTimes.com <nytdir	Deliver Whitelist Delete
<input type="checkbox"/>	03/18 03:30	NYTimes.com <nytdir	Deliver Whitelist Delete
<input type="checkbox"/>	03/18 08:13	"Looking Better" <neu	Deliver Whitelist Delete
<input type="checkbox"/>	03/18 00:07	"Generating C. Oddes	Deliver Whitelist Delete
<input type="checkbox"/>	03/17 23:00	"Baseline Offers" <su	Deliver Whitelist Delete
<input type="checkbox"/>	03/18 04:25	slashdot@slashdot.or	Deliver Whitelist Delete
<input type="checkbox"/>	03/17 17:24	"Golf Etc." <newslette	Deliver Whitelist Delete
<input type="checkbox"/>	03/17 18:14	"Marshalls" <marshal	Deliver Whitelist Delete

On this page, you can see any quarantined emails that Barracuda has blocked you from getting. On this page, you can add any quarantined items to the Whitelist. For instance, should someone that you know send you something that gets quarantined and you don't want their emails quarantined, add their email address to your Whitelist and the Barracuda will allow the emails to pass through.

5.) Now let's look at the Preferences tab. There are five buttons on this page. We'll start with the "Quarantine Settings" button.

tangent
To create an account on our service please [CLICK HERE](#)

Log Off
English (US)

QUARANTINE INBOX **PREFERENCES**

Whitelist/Blacklist **Quarantine Settings** Spam Settings Password

Quarantine Enable/Disable Save Changes ?

Enable Quarantine: Yes No

"Yes" recommended. If "No" selected, messages that would ordinarily be quarantined will be delivered with "[QUAR]" in the subject line

Under the "Quarantine Enable/Disable" label, click "Yes" to enable quarantine. This will give you 99.9% security on not receiving an email with a virus. Click "Save Changes" if you make changes to this setting.

On this same page under “Quarantine Notification”, set the “Notification Interval” to “Daily”, as recommended. Click “Save Changes” if you make changes to this setting.

Quarantine Notification Save Changes ?

Notification Interval: Daily Weekly Never

Notification Address:

"Daily" recommended. Determines how often you receive notification that messages are in your quarantine.

Use this entry to override the email address that should receive quarantine notifications for this account.

Lastly, you have the option of changing the default e-mail address (your username) that will receive a notification should e-mails be quarantined.

6.) Next click on the “Spam Settings” preference. The “Enable Spam Filtering” should be set to “Yes”. Click “Save Changes” if you make changes to this setting.

tangent

To create an account on our service please [CLICK HERE](#)

Log Off

English (US)

Spam Filter Enable/Disable Save Changes ?

Enable Spam Filtering: Yes No

"Yes" recommended. If "No" selected, all messages will be delivered without being scanned for spam

7.) Next, click on the “Whitelist/Blacklist” preference button. This allows you to customize your e-mails. Here is another place you can put e-mail addresses that you don’t want to get deleted by Barracuda. Those e-mail addresses will go in the “Allowed Email Addresses and Domains” section. For e-mail addresses that Barracuda did not catch and you’d like it to catch, place the e-mail addresses into the “Blocked Email Addresses and Domains” section. Notice I have “debc42@yahoo.com” in that section. This means that I do not want to receive emails from this address.

Whitelist/Blacklist | **Quarantine Settings** | **Spam Settings** | **Password**

Allowed Email Addresses and Domains (Whitelist)

Email Address	
<input type="text"/>	<input type="button" value="Add"/>

Email sent from addresses entered here will not be analyzed for spam, but will be scanned for viruses.

Blocked Email Addresses and Domains (Blacklist)

Email Address	
<input type="text"/>	<input type="button" value="Add"/>
debc42@yahoo.com	<input type="button" value="Remove"/>

Email sent from addresses entered here will always be blocked.

The Whitelist/Blacklist button is the most powerful feature on this web page. It allows you to add additional e-mail addresses that you would like the Barracuda to catch.

debc42@yahoo.com will now be blocked by the Barracuda for me, because I have added it to my list of emails that I would like blocked.

8.) You can change your Tangent password at any time. Go to the “Password” button and type in your old password, new password and then be sure to re-type your new password. Click “Save Password” to save these changes.

Whitelist/Blacklist | **Quarantine Settings** | **Spam Settings** | **Password**

Password Change

Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Re-Type New Password:	<input type="text"/>
	<input type="button" value="Save Password"/>

9.) Once you have completed the above changes please be sure to click “Log Off” to end your session.