A Moving Target ...

Spam—Junk E-mail sent in bulk to multiple recipients, is continually being redesigned to mimic legitimate business correspondence. This redesign process has caused our spam filters to occasionally identify genuine business correspondence as spam.

It’s critically important that TTI mailbox users receive their e-mail on a timely basis, so, we have relaxed the aggressive features of the TTI spam filter to assure the effective delivery of mail. Our spam blocking policy has undergone some radical changes!

Spam Policy Changes

In the past, TTI sent suspicious messages into quarantine before the messages reached their destination mailbox. This process worked well until we discovered that the content filter incorrectly quarantined a small percentage of legitimate messages. This process was further complicated when several employees indicated that they’d prefer to receive all messages and then use the features of Outlook to separate questionable content from valid messages.

As of December 18, 2007, all messages positively identified as spam or viruses are quarantined on the server rather than being delivered to the destination mailbox. Messages that the Antigen spam filter is unable to positively identify as spam are tagged then released to the intended recipient’s mailbox.
This means that TTI computer users now see an increasing number of messages that are probably spam. The messages may be acceptable to you—if so, they’re in your Inbox. If not, you can divert the spam to your Junk E-mail folder. Here’s how: before passing a suspicious message to the user’s mailbox, Antigen places a tag in the e-mail message’s Internet header with an indicator that the message is suspicious. This allows you, the TTI mailbox owner to decide whether to accept or divert suspicious messages.

**How can I Block Junk E-mail?**

In Outlook, you can add Inbox rules that allow you to select what is acceptable for the Inbox, and what’s acceptable for the Junk E-mail folder. Since the Junk E-mail folder will be gathering a number of questionable messages, the mailbox owner can regularly review and dispose of the content in this folder. Undesirable messages can be deleted, and messages from legitimate senders can have rules set that will keep them from going into the Junk E-mail folder. The mailbox owner will decide when and how often to review these messages.

**Tagging, Blocking, and Scanning**

Before arriving at your mailbox, e-mail messages have been examined by six separate applications that block viruses, then tag or block undesirable content. Here is a list of applications that scan your messages as they arrive at Texas A&M:

- Greylisting
- SpamAssassin
- Virus Blocking
- Antigen AntiVirus
- Antigen Spam Filter
- Microsoft Intelligent Message Filter

The table below lists more information on the scanning applications provided by TTI and TAMU.

<table>
<thead>
<tr>
<th>Application</th>
<th>Provider</th>
<th>Function</th>
<th>Tag Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greylisting</td>
<td>CIS</td>
<td>Blocks hosts if smtp-relay detects suspicious behaviour</td>
<td></td>
</tr>
<tr>
<td>Virus Blocking</td>
<td>CIS</td>
<td>Removes messages which are positively identified as virus-infected.</td>
<td></td>
</tr>
<tr>
<td>SpamAssassin</td>
<td>CIS</td>
<td>Tags messages with spam probability value in the mail message’s Internet header.</td>
<td>X-X-Spam-Level: XXXXXXXXX (probability=80%)</td>
</tr>
<tr>
<td>Antigen AV</td>
<td>TTI</td>
<td>Removes messages which are positively identified as virus-infected.</td>
<td></td>
</tr>
<tr>
<td>Antigen Spam Filter</td>
<td>TTI</td>
<td>Assigns a Spam Confidence Level then apply a tag to the mail message’s Internet header.</td>
<td>XXXXXXXXX (nine upper-case X’s)</td>
</tr>
<tr>
<td>IMF</td>
<td>TTI</td>
<td>Assigns a Spam Confidence Level for Outlook.</td>
<td></td>
</tr>
</tbody>
</table>
Intelligent Message Filter

The IMF evaluates the content of incoming messages then assigns them a rating from 1 to 10 based on the probability that the message is unsolicited commercial e-mail or spam. This rating is stored as a message property called a spam confidence level. This rating persists with the message but can be overridden if the mailbox owner adds the sender to the Outlook “Safe Sender” list. Since the value is assigned as an attribute of the mail message, the SCL is detectable only to Exchange and Outlook.

Arranging Junk E-mail in Outlook

You’ve probably been wondering how legitimate e-mail items are showing up in your Junk Email folder. It’s because the Junk E-mail Filter in Outlook is turned on by default for all TTI computer users. Moreover, since our spam policy has changed to allow TTI computer users even more control over the disposition of spam, you’ll want to be familiar with settings that control the way your mailbox processes messages that contain undesirable content.

You can review or change your Outlook Junk E-mail Options, by following these steps:
In Outlook click Tools | Options | then click the Junk E-mail... button. You’ll see the following dialogue box.

Notice that your protection level is set to Low. This level is designed to catch only the most obvious junk e-mail messages. You can make the filter more aggressive, but if you do it may occasionally catch legitimate messages. You should review messages in the Junk E-mail folder from time to time to make sure that there are not any legitimate messages that you should have received in this folder.
Outlook Safe Sender List

In the same location as listed above, click the tab marked “Safe Senders” to display and edit a list of addresses you don’t want treated as junk mail. These may be addresses of messages you’ve already found in your Junk E-mail folder, but would prefer to exclude from future filtering. Here is my Safe Senders List:

![Junk E-mail Options Screen]

Note the highlighted item in the Junk Mail Options screen above. Because of some odd characteristic in the format of leave request messages from TAMU System Office, the IMF assigns a high SCL value to LeaveTraq requests. This simply means that the filter sees the LeaveTraq message as a threat and tosses it into my Junk E-mail folder. For that reason, I have added LEAVETRAQ@TAMMVS1.TAMU.EDU to my Safe Senders list. This assures that leave requests go to my Outlook Inbox rather than my Junk E-mail folder.

I can also use this screen to edit or remove addresses from my safe senders list. That’s important, for example, in cases where e-mailed magazine subscriptions become an unwelcome source for solicitations from a publisher. Don’t forget the Safe Senders list. It’s very useful.

Add a Sender to Junk E-mail

If you consistently receive messages from an un-wanted sender, use these steps to route all messages from that sender into your Junk E-mail folder.
While showing the Inbox, highlight the offending message header then right-click on the highlighted e-mail item. You’ll see the drop-down menu shown below:

- Select Junk E-mail from the drop-down menu, then click “Add sender to Blocked Sender List”.

Remove a Sender from the Blocked Sender List
While running Outlook, you can review and modify the blocked sender list by clicking **Tools | Options | Junk E-mail...** button | then the **Blocked Senders** tab. You’ll a dialogue box similar to the one shown below:
Highlight an address and click **Remove** to remove a sender from your Blocked Senders List. Click **Add** to add type in a sender you want included in the Blocked Senders List. After making your changes click **Apply**.

### Review Messages in the Junk E-mail folder

An advantage of automated junk mail filtering is that the mailbox owner can choose when to pull spam from the mailbox. Instead of your inbox being loaded with unwanted messages, you decide when to review the Junk E-mail folder to determine whether anything of value has been sent there. Then, after review, you can delete all unwanted items from the Junk E-mail folder.

Click the **Junk E-mail** folder in your Outlook Folder List to review the contents of your Junk E-mail folder. If you find a message that should have been delivered to your **Inbox**, right-click the message, select **Junk Email** from the menu, then click **“Mark as Not junk”**. You then see the screen below:
Click OK to always receive messages from this sender in your Inbox. Or, to continue diverting messages from this sender into your Junk E-mail folder, clear the check box before clicking OK. After clicking OK, the message will be moved to your Inbox and web-based message content will be available to you.
To avoid seeing possibly objectionable message content, you may want to turn off the Reading Pane for your Junk E-mail folder. You can turn the Reading Pane off by clicking View | Reading Pane | off.

Example of an Inbox Rule that handles Spam
In Outlook, click Tools | Rules and Alerts then click New Rule. Now you’re ready to create an Inbox rule. Here’s what my Rules look like:

The figure above shows one Inbox rule. The rule looks for the text, “X-X-Spam-Level:XXXXXXXX” in the e-mail message’s Internet header. In the lower box, you’ll see that if the tag is found, the message is sent to the Junk E-mail folder.
The text is a tag inserted into a suspicious e-mail message to indicate that the message has at least an 80% probability that it is spam—the eight X’s represent 80 percent or higher likelihood that the e-mail is spam.
Create a Sample Inbox Rule

Use the following steps to build an Outlook rule that looks for a spam tag:

- In Outlook, click **Tools | Rules and Alerts** then click **New Rule**. In the dialogue box shown below, click the text, “Check messages when they arrive” which is under the boldface text, “Start from a blank rule”.

![Rules Wizard](image)

- Click **Next >**.
- In the dialogue box shown below, click to place a checkmark in the box preceding the text, “with specific words in the message header”. Notice that the selected condition appears in the lower blank area with specific text highlighted in blue.
In the lower white area, click on “specific words”, the blue text which appears underlined. You’ll see the box shown below:

- Type **X-X-Spam-Level:XXXXXXXXX** in the upper white area then click **Add**. The text you typed will now appear in the lower box with quotation marks.
- Click **OK** then click **Next >**. You’ll see the Rules Wizard box shown below.
In the box shown above, place a checkmark in the box to the left of “move it to the specified folder”. The option you just checked will appear in the lower white area.

In the lower white area, click the word, “specified” which appears underlined and in blue.

A list of your Outlook folders will be displayed as shown below. Locate and click on the Junk E-mail folder, then click OK then click Finish.
The Rules and Alerts box will be displayed as shown below. To activate the rule, click the checkbox to the left of the rule.
Frequently Asked questions

Q. I'm using the Inbox rule, why is stuff still going to my Inbox?
A. The rules are case sensitive. Also, it may be that your rule isn’t finding the text as it appears in the internet header of spam you’ve received. If you’re using an Inbox rule that doesn’t work, cut the tag from the Internet header of a junk mail message then paste the tag into your Inbox rule:

- Highlight an unwelcome message in your Inbox then right-click the mouse. You’ll see the dropdown menu options shown below.

  - Click the bottom menu option, “Message Options”.
  - Near the bottom of Message Options, you’ll see Internet header info.
Notice that “X-Spam-Level: XXXXXXX” appears in the Internet header. This indicates that the message only has a 70% likelihood of being spam. If you want this type of message to go to your Junk E-mail folder, highlight this text: X-Spam-Level: XXXXXXX, then copy and paste it into your Inbox rule for junk mail.

Alternatively, you could use the steps in the paragraph above titled, Add a Sender to Junk E-mail. This will assure that all e-mail from this sender goes to the Junk E-mail folder.

Q. If I’m using an Inbox rule, will I receive all of my email?
A. You will receive all email that is not identified as virus-infected either by the campus mail server or by the TTI mail server. You will not receive E-mail from servers that are actively being “greylisted” by the CIS due to RFC non-compliance. These messages do not arrive at the TTI mail server and therefore cannot be delivered. For more information, see the Intranet Blocked Mail page.

Q. What is an RBL?
A. TTI uses SPAMCOP.NET as an RBL or "Realtime Block List". The RBL operates by responding to queries from TIMAIL about the senders of incoming messages. If the source of an incoming message is listed as a known spammer, our mail server quarantines the message. An RBL allows TTI to accurately identify the worst spam servers. TTI quarantines messages originating from known spammers, making it less likely that spam can end up in your mailbox.

Q. What’s the difference between this anti-spam program and the spam filters on Outlook?
A. Think of your computer as being "downstream" in the flow of email delivery. Server-resident applications process your email first, removing viruses and messages positively identified as spam before you’re the message is delivered to your mailbox.
Q. Why is some junk mail delivered to my INBOX?
A. You may have configured your Outlook Inbox rule to tag the subject instead of delivering the message to the Junk E-mail or Deleted Items folder. Also, spam is continually rephrased and reformatted to evade detection by junk mail filters.

Q. What spam related headers are added to a message?
A. Incoming messages from outside TTI will have the information similar to this in the Internet header. The Internet header tag applied to the message by the CIS is shown in blue:

Received: from tr-6-int.cis.tamu.edu ([127.0.0.1]) by localhost (smtp-relay.tamu.edu [127.0.0.1]) (amavisd-new, port 10024) with ESMTP id wg3ep2FmSR1u for <GARY@TAMU.EDU>; Tue, 7 Oct 2008 09:06:19 -0500 (CDT)
X-Greylist: from auto-whitelisted by SQLgrey-1.7.6
Received: from mh.offers.proflowers.com (mh.offers.proflowers.com [64.5.35.190]) by tr-6-int.cis.tamu.edu (Postfix) with ESMTP id 104B81C8 for <GARY@TAMU.EDU>; Tue, 7 Oct 2008 09:06:18 -0500 (CDT)
Received: by mh.offers.proflowers.com (PowerMTA(TM) v3.5r8) id htdm900ibhk2 for <GARY@TAMU.EDU>; Tue, 7 Oct 2008 09:05:04 -0500 (envelope-from <ProFlowers@offers.proflowers.com>)
Message-ID: <16293%3B430511%3B1199904417%3B19%3B02;28676;20081007090549;3353@offers.proflowers.com>
To: Gary <GARY@TAMU.EDU>
From: ProFlowers <ProFlowers@offers.proflowers.com>
Subject: Save 25% on our top rated fall bouquet. Plus free vase.
Reply-To: "ProFlowers" <ProFlowers@offers.proflowers.com>
Errors-To: PPBounces@postfuture.com
Date: Tue, 7 Oct 2008 09:06:18 -0500
X-PF-ERID: 16293%3B430511%3B1199904417%3B19%3B02
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Disposition: inline
Return-Path: ProFlowers@offers.proflowers.com
X-OriginalArrivalTime: 07 Oct 2008 14:06:19.0830 (UTC) FILETIME=[DF43E560:01C92885]
X-X-Spam-Level: XXXXXXXXX:
X-MS-Exchange-Organization-SCL: 9

Q: What is Greylisting?
A. Greylisting is a process running on the campus mail forwarder that rejects incoming mail connections with a temporary failure code. This process forces the remote server to follow the standard smtp practise of reconnecting, usually within 15 minutes. Spam hosts and compromised systems generally are nor programmed for this behaviour, but will rapidly attempt reconnection then move on to the next spam victim’s email address.

Once a message has been accepted, further messages from that IP address will not be Greylisted for 30 days.

Greylisting also catches SMTP clients that issue a bogus HELO/EHLO like <civilcomputer121>, <fredsdesk>, and <oemcomputer>. The name sent in the HELO/EHLO command should be the fully qualified domain name of the SMTP client, otherwise it’s either an improperly configured mail server or a compromised mail host. In almost all cases, properly configured SMTP servers will not be hampered by greylisting.
Q: What is Bayes classification?
A. The Bayes classifier is used by Exchange IMF on the mail server at TTI. It assigns a spam probability value to messages based on their format and characteristics. That is, the classifier will calculate the statistical probability that a message is junk mail. Bayes classifier is successful in identifying messages that constantly change their wording and format like bank phishing messages and exotic stock solicitations.