




Spam and Phishing

Preventing and Deleting Unwanted E-mail

OTS PUBLICATION: TP09 • REVISED 07-16-2006 • ©2005 TOWSON UNIVERSITY • OFFICE OF TECHNOLOGY SERVICES

 =Shortcut  =Advice  =Caution

Spam

In the 21st Century, E-Mail is one of the most efficient and rapid forms of communication. Unfortunately, it's not much use if you are buried under a pile of spam each day.

Definition: Unsolicited E-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or news groups; junk e-mail.

Things to Avoid



These are some things that you'll probably want to avoid doing unless you want your E-Mail address available to Spammers:

- Adding an entry into a public guestbook
- Putting your E-Mail address on a page on your website
- Posting on Internet newsgroups
- Replying to a Spam (hence confirming that your E-Mail address is active)
- Posting a message to a public forum
- Subscribing to a mailing list from a dubious source
- Receive free E-Cards from friends

Summary

Spam

1. Definition
2. Things to Avoid
3. What Can I Do?
4. Setting Up a Rule

Phishing

1. The Warning Signs
2. OTS Recommends
3. Full Header Information



You may want to create a dedicated personal e-mail address to use when making purchases, joining Web sites, etc...

It is very difficult to trace the origin of spam (though in some cases it is possible). As quick as an Internet Service Provider bans a particular spammer due to volume of received complaints they spring up somewhere else via a different (or hijacked) connection.

What Can I Do?

With spam continuing to increase, OTS has implemented a variety of methods to detect and eliminate incoming spam e-mail.:



All e-mail coming into the university now has an **X-Spam-Score** value added to the e-mail header. This information is added by the Spam Assassin program which runs on the e-mail hubs. (It is important to note that only e-mail that *originates from outside the University* has the X-Spam-Score information added, this may mean that OTS cannot block certain sources). Currently OTS receives around 250,000 messages a day and 80% of those are categorized as spam. That means only 50,000 messages a day actually are allowed through to Towson recipients.

Spam Assassin evaluates the characteristics of incoming e-mail in order to determine if the message is spam. Points are accumulated for each criterion that the message matches (such as certain keywords, HTML format, random strings of letters).

Currently, the Towson University mail hubs block all messages receiving a score of 6 or higher. However, it's possible that messages with scores of 3, 4 or 5 are also spam. The mail hub does not block messages with those scores in order to avoid blocking legitimate e-mail.

Setting Up A Rule

Since the X-Spam-Score value is now recorded in e-mail messages, one can set up Outlook or another e-mail client to filter messages with scores of 3, 4 or 5. For example, to do so in Outlook 2003, create a rule like the following:

1. Go to the **Tools** menu and select **Rules and Alerts**.
2. On the **E-mail Rules** Tab select **New Rule**.
3. Choose the **Start from a blank rule** option and highlight **Check messages when they arrive**.
4. Choose **Next**.
5. In the **Step 1: Select conditions** choose the box in front of *with specific words in the message header* (*Figure 1, 1*).
6. In the **Step 2: Edit the rule description** click on the *specific words* link (Figure 1, 2).
7. In the **Search Text** window type in *X-Spam-Score: 5* and choose **Add** (Figure 2, 1). Do the same for *X-Spam-Score: 4* and *X-Spam-Score: 3*.
8. Choose **OK** and then **Next**.

Figure 1

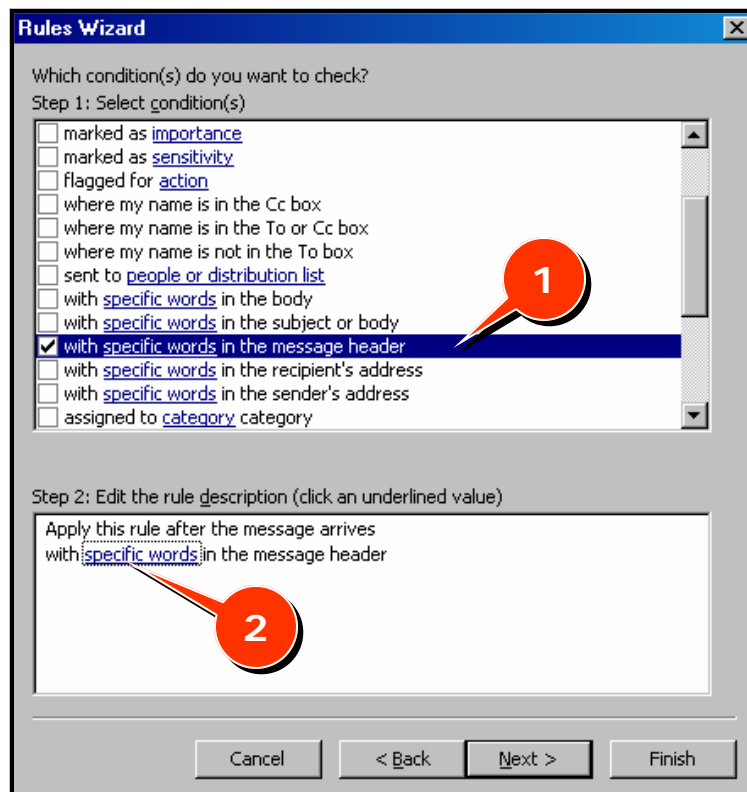
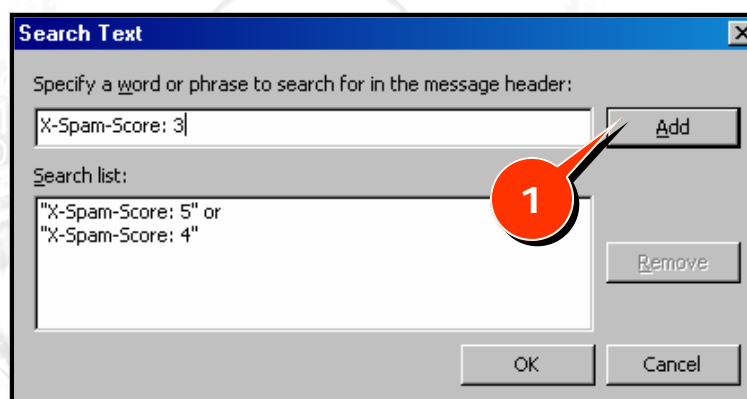
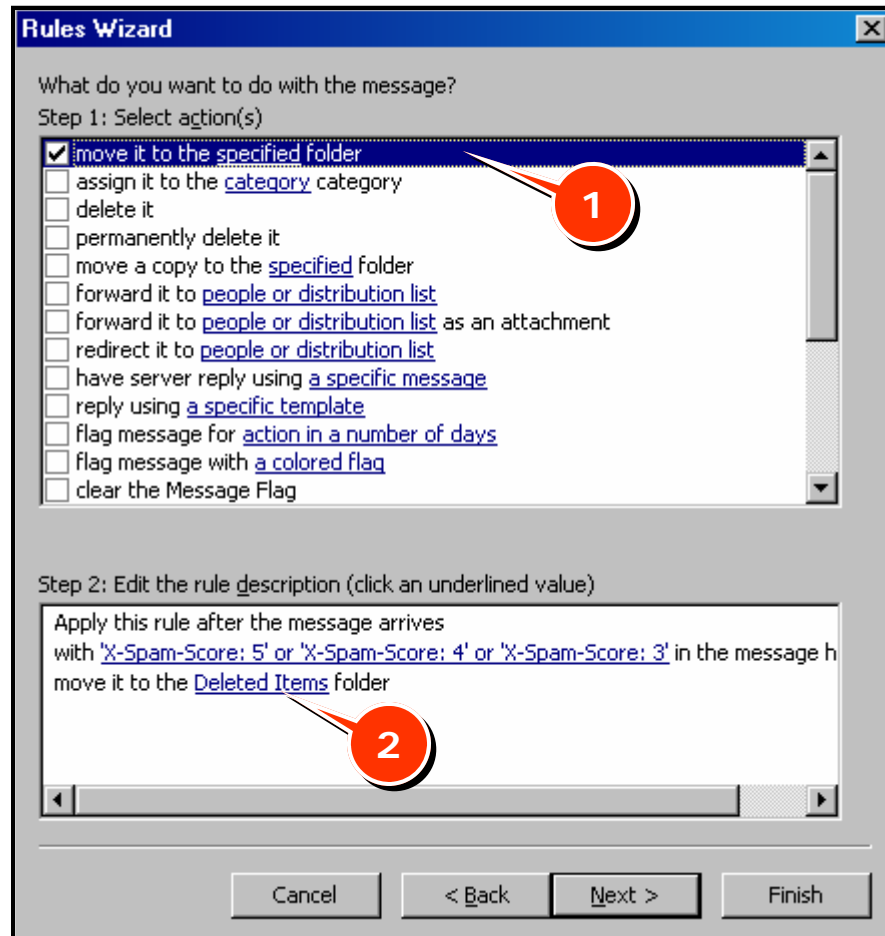


Figure 2



9. In **Step 1: Select actions** choose the box before *move it to the specified folder* (Figure 3, 1).
10. In **Step 2: Edit the Rule Description** click on the **specify folder** link (Figure 3, 2), and browse to the **Deleted Items** folder. Choose **OK**.
11. Choose **Next**.
12. Keep the **Turn on Rule** checked and choose **Finish**.

Figure 3



★ For more information on Spam Assassin go to <http://www.spamassassin.org>.

Phishing

There is an increasing Internet scam known as phishing (pronounced as fishing). Phishing involves the use of seemingly legitimate e-mail messages and Web sites to deceive consumers into disclosing private information, such as bank account information, social security numbers, credit card numbers, passwords, etc.

Bank logos, Web links and graphics are used to mislead e-mail recipients. These attacks have become so sophisticated, it is difficult to differentiate a phishing email from a legitimate one. In most phishing schemes, the fraudulent e-mail message will request bank customers to update or validate their financial or personal information to maintain their accounts. Once submitted, the perpetrator can use it to gain access to financial records or accounts, commit identity theft or engage in other illegal acts.

The Warning Signs:

- Requests for personal information in an e-mail message. Financial institutions never ask for account information via email.
- Alarmist messages which include upsetting or exciting (but false) statements so you'll respond quickly without thinking.
- Remember, if it sounds too good to be true, it probably is!

OTS Recommends the following advise to help safeguard against phishing:

- Never reply or click any links in the body of any e-mails requesting account, billing or other personal information.
- Before submitting financial information through a Web site, check to see if the Web site is using encryption, which will be indicated by a lock icon in the browser's status bar. The beginning of the web address should be "https://" rather than just "http://"
- For any messages asking you for account information, either contact the financial institution through another means, (i.e. phone, in-person) or open a Web browser and type in the institution's Web site address and log in to a secure site. The beginning of the Web address should be "https://" rather than just "http://."
- Review credit card and bank statements regularly. If you unknowingly supplied personal or financial information to a phishing scheme, contact your bank or credit card immediately.
- Report it and/or delete the message. (To report the incident, forward a copy with the full header information to the Federal Trade Commission at spam@uce.gov (see below for instructions) or the [Anti-Phishing Working Group reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org), otherwise, it cannot be investigated).

Full Header Information:

1. Double-click to open the e-mail you received.
2. Click on **View** and then click **Options**.
3. At the bottom of the box you will see 'Internet headers'.
4. Click in to the area next to 'Internet headers' (This is all gray.)
5. Use your mouse to highlight the text inside the box.
6. After it is highlighted right-click and select **Copy**.
7. Close the dialog box and click **Forward** to forward the message.
8. Click in top of the message, then right-click and select **Paste**.

For more information, please visit this URL: <http://www.antiphishing.org/>

If you have additional questions, please call the OTS Help Center at 410-704-5151.