
SPAM

UNDERSTANDING & AVOIDING

SPAM – UNDERSTANDING & AVOIDING	5
What is Spam?	6
How to avoid Spam	6
How to view message headers	8
Setting up a spam rule	10
Checking and emptying Junk E-mail	12
Adding an exception list to a spam rule	13
Alert CompServ of spam in the Inbox	15
Using Outlook 2003’s Blocked Sender’s List	16
Using Outlook’s Junk E-mail Filter at home	16

SPAM – UNDERSTANDING & AVOIDING

In this lesson, you will learn how to:

- Identify Spam
- Avoid Spam
- View message headers
- Set up a spam rule
- Check and empty your Junk E-mail folder
- Add an exception list
- Let CS know about spam getting through
- Add repeat spammers to blocked senders list
- Use Outlook's Junk E-mail Filters at home

WHAT IS SPAM?



Discussion

What is Spam?

Spam is generally defined as electronic junk mail or junk newsgroup postings. Usually it is commercial mail -- solicitations or advertising, otherwise known as UCE (unwanted commercial e-mail) -- although sometimes "spam" is used to describe any unwanted message that is sent to a large group of people.

Why is it a problem?

Unwanted "junk" e-mail or newsgroup postings waste people's time, waste bandwidth and slow everything down on the 'Net. The cost of this form of junk mail is shifted to the recipient, who has little choice but to receive the messages. Some analogize it to junk mail showing up at your house postage due, where you have no choice but to pay. Junk e-mail also cost consumers money through increased expenses that service providers must pay to handle the increased load. And sometimes junk mail carries spyware or viruses.

HOW TO AVOID SPAM



Discussion

It's just about impossible to avoid getting spam. But there are ways to minimize it, and methods to avoid getting more.

- **Never respond directly to junk email!**
Never reply to spam, even to demand that you be removed from their list. This action will practically guarantee that you receive even more unwanted mail. It tells the spammer that not only is your e-mail account active, but also you read your email often. While the spammer may not send you any more e-mail, he will certainly sell your e-mail address to another spammer.



"99% of spammers use fake reply to: addresses"



If you're willing, try complaining to the Internet Service Provider (ISP) where the spam came from. Since many spammers "fake" or "spoof" their message headers, figuring out where junk mail originated can be tricky. To do this you must view the e-mail message headers (see "How to View Message Headers" below) and look for IP addresses or domains within parentheses in the header's received lines. (Information outside the parentheses could be faked.) Then verify the information at UXN Spam Combat (<http://combat.uxn.com>). Once you've identified the most likely culprit, and found the appropriate contacts, send a message requesting that their ISP stop the spam coming from the offending domain or IP address.



If you've already made the mistake of replying to a spammers "so-called" remove request and got more junk email, but you're not sure how to track down the source of the spam, consider changing your email address for an immediate solution.

- **Never buy anything from a spammer.**
Spammers are con-artists. They fake the source of their e-mails to cover their tracks, hijack e-mail servers that allow open relaying to deliver hundreds of thousands of their bogus e-mail messages. They clog the Internet and mail servers with a large number of spam, hoping to compensate for the low percentage of people who actually purchase their product. In fact, purchasing anything from a spammer only supports this dishonest means of advertising. In most cases, the people that buy their bogus products get ripped off.
- **Beware of "free drawings" and "lottos"**
If you sign up for services that give free prizes, expect to be spammed! In most cases these sources of "all things free" are fronts for collecting email addresses.
- **Stay anonymous**
Spammers use email robots called **mailbots** to collect addresses from newsgroups and the web. You can outwit them: Never add your address to Internet email directories. When you're on the web, leave the email address field in generic web forms blank, or supply a decoy address, such as nospam@nospam.org.
- **Turn off Picture downloads**
Blocking the automatic downloading of pictures in e-mail can prevent junk e-mailers from verifying you as a prospective spam target. In Outlook 2003, select Tools > Options, click the Security tab, then click "Change Automatic Download Settings..." button under the category "Download Pictures". Verify that "Don't download pictures or other content automatically in HTML e-mail" is checked. All e-mail containing links to downloadable pictures will instead display red x's. Right-click on a red x to download pictures for any e-mail you know to be safe.
- **Scramble your address when posting to public forums.**

If you post public messages to newsgroups or web discussion boards, you can limit the amount of junk sent to you by practicing address munging. Adding extra characters or words to your outgoing address confuses mailbots (you can make the change in your email application's preferences). For example, if your real address is joe@isp.com, a scrambled version would be joe@removethis.isp.com. Be sure to add instructions in your signature file that explain how to decode your address so you can receive legitimate replies. Don't include your actual email address because mailbots scan the contents of all posts.

- **Remember to forward your “deceptive” spam to the FTC**

The Federal Trade Commission monitors the spam situation on behalf of the government and has asked that you forward any “spam email that you think is deceptive” to this email address: spam@uce.gov. For more information, go to <http://www.ftc.gov/spam/>.

HOW TO VIEW MESSAGE HEADERS



Discussion

You can't believe what is displayed in an e-mail, not even Outlook's visible header section (which includes the To, CC, and Subject fields). However, hidden in the “message header” lies, at least in part, the truth about an e-mail; where it came from, who might have sent it, where those embedded hyperlinks really go.



Procedures

1. Double-click on the desired e-mail to open it in a new window.
2. From the e-mail window's menu bar, select **View > Options**.
3. View the message header info in the bottom pane of the Options window.



Step-by-Step

From Outlook's message Inbox, open the e-mail with the subject “**SPAM I AM**”. Select a cell, row, and column in a table.

<i>Steps</i>	<i>Practice Data</i>
1. Double-click on the desired e-mail. <i>The will appear in a new window.</i>	Double-click on the e-mail with the subject “ SPAM I AM ”.
2. Select View > Options. <i>The Options dialog appears.</i>	Select View > Options from the menu bar.
3. Observe the message header into in the bottom pane.	Observe the message header into.

Try This: Copy the message header information and paste it into a new e-mail message.

1. Select the message header information by clicking once in the text, then pressing [Ctrl]-[A]. *All of the information will be highlighted.*
2. Copy the selected text by pressing [Ctrl]-[C].
3. Switch back to the Outlook window.
4. Create a new e-mail message.
5. In the message field of the new e-mail, click once. *The blinking insertion point will appear in the message field.*
6. Paste the copied text by pressing [Ctrl]-[V].

At this point the message header information could now be e-mailed to a support person who could analyze it and possibly identify the source of the spam.

Below is an example of a message header:

```
Return-Path: wang@netease.net
Received: from fixthisrelayserver.com ([000.000.000.000] verified) by
mailhost.myISP.com with ESMTP id S.0000214849 for
<me@myISP.com>; Sat, 05 Aug 2000 04:21:31 +0100
Received: from ds98.spammer.com ([000.000.000.000]) by
fixthisrelayserver.com with SMTP (Microsoft Exchange Internet Mail Service
Version 5.5.2650.21); Sat, 5 Aug 2000 05:16:04 +0200
Received: from someplace.blah.blah.blah[255.255.255.256];5 Aug 2000
01:55:20 +0000

To: eatyourspam@netease.net
From: <wang@netease.net>
Subject: Earn $50,000 in only 10 Days !!
Date: 5 Aug 2000 05:16:49 +0200
Message-ID: <00d87041603058@fixthisrelayserver.com>

Dear Friend,

You are receiving this because your friend John opted you in to our list!!!
This email contains the ENTIRE PLAN of how YOU can MAKE $50,000!!
Visit my website http://www.cyberpimps.com for a chance to win HUGE
MEGA CASH!!!
```

SETTING UP A SPAM RULE



Discussion

Computer Services, at Cuesta College, does not remove suspected spam. Instead, dubious e-mail is given a “spam score” that is stored in the message header. Each user is responsible for setting up a rule that acts upon messages marked as spam.



The text, “*X-Cuesta-College-SpamScore: ssss*”, in the message header indicates the “spam score”. Your rule is looking for any e-mail with a score of five (5) or more S’s in the message header. (The letter “s” is used as a counter, like a check mark, to indicate each time Cuesta College’s spam filter identifies something “spam-like” in the e-mail.)

If your rule is not filtering enough spam, you can modify it to catch more potential spam by reducing the number of S’s. For example, “*X-Cuesta-College-SpamScore: ssss*” would affect any e-mail with a score of four (4) or more S’s.

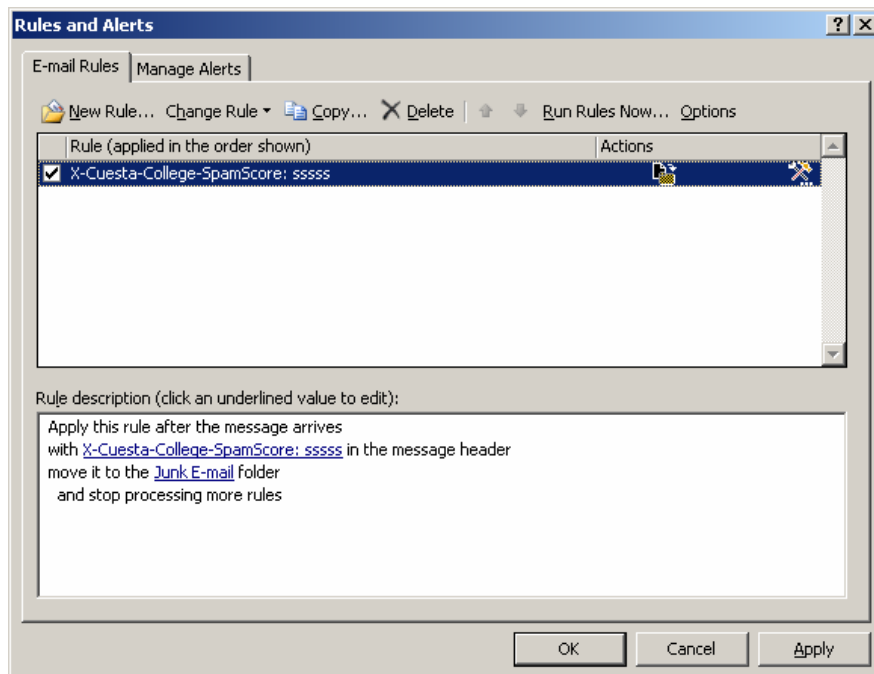
However, be aware that reducing the number of S’s increases the chances that legitimate e-mail will get moved to your Junk E-mail folder.



Procedures

1. Select the following link: <http://email.cuesta.edu/mailinfo/nospam.rwz>
2. When prompted, save the file, **nospam.rwz**, to the Desktop.
3. In Microsoft Outlook, select the **Inbox**.
4. From the menu bar, select **Tools > Rules and Alerts...**
A rules dialog box will appear.
5. Select **Options** button on the Rules dialog box.
The Options dialog box will appear.
6. Click the **Import Rules...** button.
The “Import Rules from” dialog will appear.

7. Browse to the Desktop and double-click on the file, “**nospam.rwz**”.
The “Import Rules from” dialog box will close, revealing the Options dialog.
8. Click the “**OK**” button on the Options dialog box.
The Options dialog box will close, revealing the Rules and Alerts dialog box. The spam filter rule will be displayed.
9. Verify that the check box next to the rule is selected so that it will be applied.
10. **Click the underlined text** (usually the word “specified”) in the Rule description that appears between “move it to the...” and “...folder”.
A window displaying a folder list will appear.
11. Select the “**Junk E-mail**” folder by clicking once on it.
12. Verify that the Junk E-mail folder is highlighted, and then click the **OK** button.
The Rules and Alerts dialog box will appear.
13. Verify that the third line in the rule description reads: “...move it to the Junk E-mail folder...”
14. If you have more than one rule running, use the Move Up button to make sure that your new Spam rule is at the top of the list.
15. Once completed, click the **OK** button.



CHECKING AND EMPTYING JUNK E-MAIL



Discussion

With the creation of the spam rule, you need to periodically check your Junk E-mail folder. When checking the Junk E-mail folder you'll want to verify that the contents *are* spam.

If you find e-mail that is not spam, you can simply drag it from the Junk E-mail folder to the Inbox. You may also wish to add an exception list (see next section below) to prevent future e-mail from that sender getting placed in the Junk E-mail folder.

Once the contents of the Junk E-mail folder has been verified as spam, you can empty the folder to prevent spam build up, and make it easier to do future verifications.



To ease viewing the contents of the Junk E-mail folder, turn off the Reading Pane (who wants to read that junk?), turn off Grouping (View > Arrange By... > Show in Groups), and sort by From.



Procedures

1. Click once to select the Junk E-mail folder in the Folder List.
2. Verify the e-mail in the Contents pane are spam.
(*If not, add to the exception list and/or move the message out of the Junk E-mail folder.*)
3. **Right-mouse click** on the Junk E-mail folder.
A shortcut menu will appear.
4. From the short-cut menu, select **Empty “Junk E-mail” Folder**, and respond “**Yes**” to the confirmation window.
All of the e-mail in the Junk E-mail folder will be permanently deleted.

ADDING AN EXCEPTION LIST TO A SPAM RULE



Discussion

It's very possible that legitimate e-mail (i.e. correspondence from students or others outside of the Cuesta College network) will get incorrectly identified as spam and wind up in your Junk E-mail folder. It's for that reason that you should carefully monitor the contents of your Junk E-mail folder before deleting its contents.

You can modify your spam rule to identify legitimate addressees and prevent future correspondence from them getting moved to the Junk E-mail folder.



Procedures

1. Select (drag across) the sender's name in the From field of the legitimate e-mail that is in the Junk E-mail folder.
The sender's name will be highlighted.
2. Copy (**Ctrl-C**) the selected sender's name.
3. From the menu bar, select **Tools > Rules and Alerts...**
The "Rules and Alerts" dialog box will appear.
4. Select the X-Cuesta-College-SpamScore rule in the top pane.
The rule will be highlighted and the rule description will appear in the lower pane.
5. Select the **Change Rule** button at the top of the Rules dialog box.
A drop-down list will appear.
6. From the drop down list, select **Edit Rule Settings...**
The Rules Wizard dialog box ("Which conditions do you want to check?") will appear with the option "with specific words in the message header" selected.
7. Click the **Next** button.
The Rules Wizard dialog box ("What do you want to do with the message?") will appear with the options "stop processing more rules" and "move it to the specified folder" selected.
8. Click the **Next** button.
The Rules Wizard dialog box ("Are there any exceptions?") will appear.
9. Select the option "**except if from people or distribution list**" in the top pane.
The text "except if from people or distribution list" will be added to your rule on the bottom pane.

10. Click once on the underlined text “**people or distribution list**” in the bottom pane.

The Rule Address dialog box will appear.

11. Click in the “**Specify the address of the sender**” field at the **bottom pane** of the Rule Address dialog box (just to the right of the From button) and paste (**Ctrl-V**) the copied sender name.

The sender’s name will appear in “Specify the address of the sender” field.

12. Click the **OK** button.

12. At the Rules Wizard dialog, click the **Finish** button.

13. At the Rules and Alerts dialog, click the **OK** button.

14. Drag the legitimate e-mail from the Junk E-mail folder to the Inbox.

NOTE: If you wish to add more names to your exception list:

1. Select (drag across) the sender’s name in the From field of the legitimate e-mail that is in the Junk E-mail folder.

The sender’s name will be highlighted.

2. Copy (**Ctrl-C**) the selected sender’s name.

3. From the menu bar, select **Tools > Rules and Alerts...**

The “Rules and Alerts” dialog box will appear.

4. Select the X-Cuesta-College-SpamScore rule in the top pane.

The rule will be highlighted and the rule description will appear in the lower pane.

5. Click once on the previously pasted underlined name(s) in the bottom pane.

The Rule Address dialog box will appear.

6. Click in the “**Specify the address of the sender**” field at the **bottom pane** of the Rule Address dialog box (just to the right of the From button) and paste (**Ctrl-V**) the copied sender name.

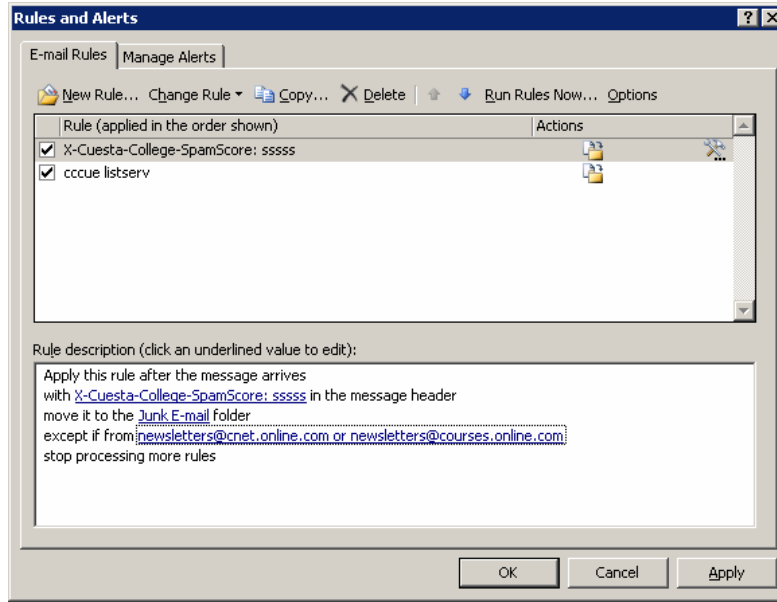
The sender’s name will be added to the list that appears in the “Specify the address of the sender” field.

6. Click the “**OK**” button.

The Rule Address dialog box will close and the sender’s name will be added to the list that appears to the right of “except if from” in the rule description.

7. Click the **OK** button.

8. Drag the legitimate e-mail from the Junk E-mail folder to the Inbox.



ALERT COMPSERV OF SPAM IN THE INBOX



Discussion

Sometimes a spammer will be deceptive enough that their e-mail will receive an insufficient spam score by the Cuesta e-mail filter. In that case, the spam will not get moved to the Junk E-mail folder but will, instead, be delivered to your Inbox.

In that case, you can alert Computer Services by forwarding the spam *as an attachment*.



Procedures

1. Create a new blank e-mail.
2. Address the new e-mail to “SPAM”.
3. Arrange the Outlook window and the new e-mail window so you can see both windows.
4. Drag the spam from the Inbox to the blank message area of the new e-mail.
A copy of the spam e-mail will appear as an attachment in the new e-mail.

5. Send the new e-mail with the attached copy of spam to “SPAM”.
6. Delete the spam from your Inbox.



If you have more than one spam e-mail in your Inbox, you can drag copies of all of them to the one e-mail addressed to “SPAM”.

USING OUTLOOK 2003’S BLOCKED SENDER’S LIST



Discussion

Typically spammers are constantly changing their return addresses. This makes it impossible to filter by return (“from”) address.

However, if you are receiving multiple spam in your Inbox from someone *at the same address*, you can manually block future spam from that sender.



Procedures

- 1 Right-mouse click on the spam e-mail message.
- 2 Point to “**Junk E-mail**” in shortcut list.
- 3 Select “**Add to Blocked Senders List**”.

USING OUTLOOK’S JUNK E-MAIL FILTER AT HOME



Discussion

The Junk E-mail Filter in Outlook 2003 is turned on by default, and the 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 catch legitimate messages sometimes. Any message that is caught by the Junk E-mail Filter is moved to a special Junk E-mail folder. You should review messages in the Junk E-mail folder from time to time to make sure that they are not legitimate messages that you want to see.

To get Junk E-mail Filter updates and Microsoft Office 2003 Service Packs, go to Downloads on Office Online (<http://office.microsoft.com/en-au/officeupdate/default.aspx>). Under **Office Update**, click **Check for Updates**.

There are two parts to the Junk E-mail Filter: the Junk E-mail Filter Lists, and the state-of-the-art technology developed by Microsoft Research that evaluates whether an unread message should be treated as a junk e-mail message. This evaluation is based on several factors, including the time when the message was sent and the content of the message. The filter does not single out any particular sender or type of e-mail message. The filter is based on the content of the message in general and uses advanced analysis of the message structure to determine the probability that it is a junk e-mail message.

There are five Junk E-mail Filter Lists: the Safe Senders List, the Safe Recipients List, the Blocked Senders List, and two International lists: the Blocked Encodings List and the Blocked Top-Level Domains List.

Safe Senders List If the filter mistakenly marks an e-mail message as a junk e-mail message, you can add the sender of that message to the Safe Senders List. E-mail addresses and domain names on the Safe Senders List are never treated as junk e-mail, regardless of the content of the message.

- E-mail addresses in your Contacts folder are included in this list by default. Therefore, messages from people in your Contacts folder will never be treated as junk e-mail messages.
- E-mail addresses of people who are not in your Contacts folder but whom you correspond with regularly are included in this list by default when the Automatically add people I e-mail to the Safe Senders List check box is selected.

Safe Recipients List If you belong to mailing lists or distribution lists, you can add these names to your Safe Recipients List so that any messages sent to these e-mail addresses or domain names will never be treated as junk, regardless of the content of the message.

Blocked Senders List You can easily block messages from a specific sender by adding their e-mail address or domain name to this list. Messages from people or domain names on this list are always treated as junk, regardless of the content of the message. When you add a sender's name or e-mail address to the Blocked Senders List, Outlook moves all messages received from that source to the Junk E-mail folder.

- If Automatic Picture Download is turned off, messages from or to e-mail addresses or domain names in the Safe Senders List and Safe Recipients List are treated as exceptions, and content that is otherwise blocked is downloaded.
- If you have existing lists of safe or blocked names and addresses, you can import this information into Outlook.
- E-mail addresses are matched exactly, and specific address entries take precedence over domain name entries. To block an entire domain but still see

messages from specific safe addresses, add the specific addresses to the Safe Senders List. For example, add someone@example.com to the Safe Senders List and @example.com to your Blocked Senders List. This blocks any e-mail message you receive with @example.com in the e-mail address except a message from someone@example.com.

International List To block unwanted e-mail messages that come from another country or region, or that appear in another language, there are two lists that you can use.

- **Blocked Top-Level Domains List** This list enables you to block e-mail addresses that end in a specific top-level domain. For example, selecting the CA [Canada], US [United States], and MX [Mexico] check boxes in the list will block messages that have e-mail addresses ending with .ca, .us and .mx. Additional country codes appear in the list. This helps you to eliminate unwanted e-mail messages that you receive from specific countries or regions.
- **Blocked Encodings List** This list enables you to block all e-mail addresses that are formatted in a specific language encoding (encoding: A method for representing characters in HTML or plain-text e-mail messages, examples include US-ASCII, Unicode (UTF-8), and Western European (ISO). Outlook automatically selects an optimal encoding for outgoing e-mail messages.), also known as a character set. Today, the vast majority of junk e-mail is sent in the US-ASCII encoding. The remaining junk e-mail is sent in various other international encodings. The Blocked Encodings List gives you the ability to filter out unwanted international e-mail that is displayed in a language that you don't understand.



Procedures

Add E-mail to Junk List

- 1 Right-mouse click on e-mail message.
- 2 Point to “Junk E-mail” in shortcut list.
- 3 Select one of the “Add” options.



Procedures

Edit Junk E-mail Filter Lists

- 1 On the **Tools** menu, click **Options**.
- 2 On the **Preferences** tab, under E-mail, click **Junk E-mail**.

3 Click the **Safe Senders**, **Safe Recipients**, or **Blocked Senders** tab.

4 Do one of the following:

Change a domain name or e-mail address

- a. In the list, click the domain name or e-mail address you want to change.
- b. Click **Edit**.
- c. Enter the new text in the Enter an e-mail address or Internet domain name to be added to the list box.

Remove a domain name or e-mail address

- a. In the list, click the domain name or e-mail address you want to delete.
- b. Click **Remove**.

