SPAM

UNDERSTANDING & AVOIDING
SPAM – UNDERSTANDING & AVOIDING..........................................................5
  What is Spam?........................................................................................................6
  How to avoid Spam ................................................................................................6
  How to view message headers..............................................................................8
  Checking and emptying Junk E-mail.................................................................10
  Rules to Remember ............................................................................................11
SPAM – UNDERSTANDING & AVOIDING

In this lesson, you will learn how to:

- Identify Spam
- Avoid Spam
- View message headers
- Check and empty your Junk E-mail folder
WHAT IS SPAM?

δ 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

δ 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/](http://www.ftc.gov/spam/).

---

**HOW TO VIEW MESSAGE HEADERS**

**δ 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.

**X 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.

**Φ 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.
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: eatyoursamp@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!!!
CHECKING AND EMPTYING JUNK E-MAIL

\( \delta \) 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.

\( \chi \) Procedures

1. Click once to select the Junk E-mail folder in the Folder List.

2. Verify the e-mail in the Contents pane is 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 Folder**, and respond “Yes” to the confirmation window.  
   All of the e-mail in the Junk E-mail folder will be permanently deleted.
RULES TO REMEMBER

Discussion

There is no way to completely eliminate Spam, but there are ways to minimize it.

One way is to create a second e-mail account with a free service like Hotmail (http://www.hotmail.com) or Gmail (http://www.gmail.com). Use this free account when completing online forms that may result in spam. If and when the spam to your free e-mail account is unbearable, simply stop using the account and create another free e-mail account.

In addition, your behavior on the internet can impact how much Spam you receive. Follow these important rules:

- NEVER respond to junk email
- NEVER buy from a spammer
- NEVER click on an embedded link (from an unknown source).
- NEVER open an attached document (from an unknown source).
- NEVER request to be "removed" from something to which you have not originally subscribed.
- Stay anonymous
- Be leery of all "free" downloads on the internet (i.e. toolbars, wallpaper, screensavers, clipart, etc).
- Use your free e-mail account when completing online forms and questionnaires from “unknown parties” (i.e. anyone with whom you are not personally familiar, including acquaintances, businesses, etc.).