IN THIS ISSUE:
~ Spam Filtering

COMING NEXT MONTH:
~ Home Theater

READY NET GO … NEWS

October 2006 **http://www.readynetgo.net** **610-856-0990**

Tip of the Month

MS Outlook Tips

A) Have you ever received an email without a subject or was the subject so undescriptive that it was pointless?

If you need to keep it, then edit it …

1) In Outlook, **open the message** by double clicking it. You can't edit the subject line in preview mode.
2) **Highlight the text** in the **Subject field** or put your cursor in this field and start typing.
3) When you have added text/edited the subject, click **File** – **Save** then **File – Close**.
4) When you return to the **Inbox**, you'll see your newly edited Subject line.

B) Have you ever sent an email that you shouldn't have? **IF** you're quick and the **recipient** uses Outlook on an **Exchange Server**, you just might be able to recall that message before they read it.

1) Double click the message in your **Sent Items** folder to open it in its own window.
2) Select **Actions** on the Main Menu and scroll down to **Recall this Message …**
3) A dialog box opens with two options: Delete unread copies of this message or delete and replace with a new message. Choose an option and click **OK**.
4) In either case, you will be notified if the recall was successful or not if the last checkbox is checked.

There's **NO GUARANTEE** it will be recalled but it's worth a shot …

How to Manage Spam in Email

The term **spam** is actually a slang name for **UCE** or **Unsolicited Commercial Email**. Spam emails were once considered more annoyance than trouble compared to viruses and other Malware but recently the practice of phishing has added a new reason to be vigilant about managing spam. Until individuals stop clicking on and purchasing from these emails, spam won't stop. In the meantime, we must learn to manage spam through safe-computing practices and configuring settings within the email client and/or third party solutions.

How Spam works

Spammers gather email addresses from a variety of sources such as newsgroups, message boards, email lists, websites, and even companies with whom you do business that are willing to sell your information for profit. It is extremely **difficult to trace** how a spammer got your particular email. Many spammers will troll the web looking for any and all email addresses to add to their lists. As the law of averages dictates, the more email addresses a spammer has and uses, the more likely someone will buy their product or service.

After the spammers gather their lists, they either sell the list to someone else or send out emails directly. Usually, they obtain a free email account and **send messages anonymously** with special programs designed to thwart email servers which obscure their IP address or point of origin. This is how spammers can get away with sending hundreds of thousands of emails and not get caught.

The business is lucrative to the point of being ridiculous and absurd. Start-up costs are very small – all one needs is a computer, an Internet Connection and

---

WWW (Websites Worth Watching)

1) www.whatsthatbug.com – great site, informative, easy to navigate – get the lowdown on what "bugs" you
2) dsc.discovery.com – Discovery Channel; check their TV schedule to find out when shows such as **Dirty Jobs**, **How It Is Made**, and **Mythbusters** are on.

a list of email addresses. Many software programs for sending the emails are free (Open source). Some spammers with the right lists can make a **million dollars or more each month (!)** if just one person out of 2,000 clicks the link and makes a purchase. Once the emails are sent, the account is closed and a new one is setup from a different location - quick and easy and the money rolls in!

Phishing, in particular, is a dangerous form of spam. A phishing email is not simply trying to get you to purchase a product or service. A phishing email attempts to get your personal information such as social security number, credit card numbers, bank account information and other confidential data to steal your identity. Usually spammers will "**spoof**" a bank's website (and design) to **lure people** into thinking it's safe to hand over personal information. They may use similar logos and graphics to mimic the "safe" site. In many cases, it's very difficult to detect a spoofed website from the original.

Other common scams include account verification requests from companies such as PayPal, eBay, and credit card companies. The requests are cautionary in nature usually **requesting account verification** for security purposes. In actuality, once you submit your information through a link in an email, your identity is stolen and the spammers reap the rewards. Again, it is **always safer to manually type** a sites address in your browser then click a link in an email.

How to Manage Spam

There are 3 ways to manage spam:

1) **Workstation level** – use the tools built-in to the MS Outlook client or purchase a third party all-in-one solution to address viruses, spam and/or spyware.
2) **Network Level** – manage spam at the gateway with a standalone hardware device such as from Barracuda Networks or Trend Micro's InterScan Gateway Security Appliance. These devices specifically target spam and offer comprehensive administration. You can also purchase software, such as Trend Micro's InterScan VirusWall, that is installed on a mail server or separate server at the gateway. For this application, software functions as effectively as a hardware device.
3) **Off –site** – mail first goes to a third party provider before downloading to your mail server or client. There is a monthly fee per mailbox for this service – keeps most spam out of your network.

While spam cannot be eliminated entirely, **there are many ways to lessen the impact**:

1) First and foremost, **keep your email secure** – don't post your primary email address (whether business or personal) on newsgroups, directories, or message boards.

   If you must post information, change your email by adding characters to it. This will prevent the auto-email scavengers or bots from adding your address to a database. Examples: instead of *jennifer@readynetgo.net* type jenniferNOSPAM@readynetgo.net or m*a*r*k@readynetgo.net.

   Then, in your post, instruct people to remove the words "NOSPAM" or "asterisks" from the username before sending email to you. Generally people modify the username but you can also modify the domain. In either case, any mail sent to that faulty address will be returned to the sender as a bad email address.

2) Tell everyone you know: **Don't click on a website link in an email if you are interested in a product**. Go to the website directly or do a general search using Google, Yahoo, MSN, etc.

3) Use a **free email address** for online purchasing, product inquiries, and online surveys. Yahoo, Microsoft (Hotmail), and Google (Gmail) all offer free email accounts.

4) Be aware of what spam emails look like, specifically typical subject lines. Some sender's names are clearly spam-related while others are more normal, resembling someone's personal or business name. Read the Name **and** Subject before you click. If it seems suspicious, don't open it. For examples go to http://onguardonline.gov or peruse Trend Micro's Phishing Encyclopedia at http://www.trendmicro.com/en/security/phishing/overview.htm.

   In particular, **be wary** of messages that have **RE: in the subject line** especially if it's blank. This is a very common indicator of a spam message. RE: stands for reply and will only appear if someone replies to an email that you sent them. If the subject isn't relevant to a message you sent, delete it without opening. *Remember:* **When in doubt, throw it out!**

5) Be vigilant about what emails you open especially if there is an attachment. In many cases, merely opening the email may send a response back to the spammer that your email is legitimate, hence, your email is live and worth more than an email that is unopened. For better protection, **don't leave the preview pane open in your Inbox**. To turn the preview pane off in Outlook 2003, click View on the Main Menu, scroll down to Reading Pane … and over to Off. This way only the headers will be visible, such as the fields: **From, Subject,** and Date **Received**. Delete obvious spam messages without opening them.

   Helpful Hint: Select the spam messages and hold down the **Shift** key as you click the **Delete** key or icon to permanently delete the messages – not just send them to the Deleted Items folder.

6) If you receive an email from a company with whom you do business and the email is asking you for personal information, don't send it via email. Nearly all companies now have policies in place to not ask for personal information via email. If you do receive an email request, **call the company** and ask them if they recently sent you an email. If they did, give them the information over the phone.

   Email is not a secure environment – in other words, email messages may come from a different source than anticipated or can be intercepted in midstream. Never send anything in an email that you wouldn't write on a postcard including your Social Security Number, mother's maiden name, birth date, or financial account information.

7) Configure your email client to filter junk addresses. **Outlook 2003** has **email filtering built-in**. When you receive a message that is junk, help Outlook by configuring the junk email filter.

   Right click the message and scroll down to Junk Email ► You have three options:

   - Add Sender to Blocked Senders List
   - Add Sender to Safe Senders List
   - Add Sender's Domain to Safe Senders List

   Choose the appropriate choice and a dialog box will appear confirming your selection. Click **OK** to return to your Inbox.

   To view or edit your Blocked and Safe Sender addresses and domains or choose the level of protection,

   - Right click a message in your Inbox;
   - Scroll down to Junk Email ► and over to Junk Email Options... ;
   - A dialog box opens with 5 tabs: Options, Safe Senders, Safe Recipients, Blocked Senders and International.

   The **Blocked Senders tab** will list the spam addresses that have been added. Keep in mind that spammers are constantly changing their addresses so **don't be surprised** if the spam doesn't stop entirely by adding addresses to the Blocked Senders list.

To add a Safe address (one you don't want to be filtered),

- Click the **Safe Senders** tab
- Click **Add** and enter the address
- Click **OK** and the name will appear on the list
- Click **OK** to close the dialog box for Junk Email Options

8) If your email client's filtering isn't working well enough, **use commercial anti-spam filtering software**. There are many options available – some free, others must be paid for – all are designed to scan email messages before they download to your Inbox. Keep in mind that none are effective 100% of the time. False positives are the biggest complaints meaning that the software considers an email to be junk when it's not or a false negative meaning that the spam email is not filtered and appears in your Inbox.

   Many anti-virus products such as those from Trend Micro, Symantec (Norton), and McAfee include spam filtering along with anti-virus filtering. Configure these third party products to work in concert with your email client's filter for robust protection. Please contact our office if you need assistance with this task.

9) **Don't click on unsubscribe links** in emails other than from reputable sources, i.e., newsletters that you have specifically subscribed to. Unsubscribe links in spam emails are another way for spammers to **legitimize your address**. If you click it, you'll probably get a lot more spam than you want.

   Likewise, **never respond** to a spam message even if you want to give the spammer a piece of your mind. They don't know who you are and they really don't care about you as an individual and how disturbed you are by their email – spamming makes money – that's it! **Be Safe and Smart!**

10) **For your part, make sure that your emails don't get caught in spam filters**. Check to see that your entire name or email address appears in the Name column, include a descriptive Subject line and put text in the body of the email. Some spam filters will filter out emails that don't have a subject line or text in the body.

11) **Report spam to the Federal Trade Commission** (FTC) – email spam@uce.gov or use the FTC online complaint form at http://www.ftc.gov/ftc/consumer.htm

    When sending an email, include the body of the email message as well as the email headers:

    - Right click the message, scroll down to **Options...**
    - A Message Options dialog box opens.
    - In the **Internet Headers** box (at the bottom), copy the text and paste into the body of your message to the FTC.

Check out the following sites for more information:

www.viruslist.com – Informative site for learning more about viruses, hackers and spam. Lists examples and offers advice for protection.

www.trendmicro.com – Valuable software for anti-virus and anti-spam solutions

www.antiphishing.org – Anti-Phishing Working Group; worldwide association focused on eliminating phishing, pharming and email spoofing. Check out their list on phishing attacks reported since September 2003.