Message from the CIO
Unwanted, unsolicited electronic mail (SPAM) has become an international problem. The Federal Trade Commission estimates that 65 percent of all electronic mail transactions are SPAM. Unlike private corporations that censor incoming e-mail, the TTU Office of the CIO has elected to honor academic freedom and filter SPAM into a “Junk E-mail” folder for the individual to review. To address the seriousness of this issue, we are dedicating this bulletin to SPAM topics and SPAM management. Tagging SPAM in your inbox is an ongoing, daily activity. Please join us in “Operation SPAM Management” – the TTU Information Technology (IT) Division’s war against SPAM!

Dispelling SPAM and Junk E-mail Myths
After reviewing our incoming calls at IT Help Central, we have developed the following list of SPAM myths to address:

Myth 1: Nothing I do increases the amount of SPAM and Junk E-mail I receive.
Yahoo! (2006) reports that 86 percent of e-mail addresses published on Websites are harvested by spammers. In addition, large listserv mailing lists can be compromised and all the recipients harvested for SPAM. Online shopping vendors may also sell e-mail addresses to spammers; be sure to carefully read the privacy policies. Be very careful where you publish your e-mail address! In addition, if you receive a large number of SPAM in your inbox, then your junk e-mail filtering is not set up properly.

Myth 2: If I reply to the message and tell them to remove my name, they must.
The Federal Trade Commission (2005) estimates that 90 percent of junk e-mail originates from an international location. When you reply, you are merely confirming that the address is legitimate. Often these companies that receive replies sell those “active” e-mail addresses to other spammers! Remember that your best defense is the delete button and effective utilization of SPAM filters.

Myth 3: No one reads SPAM and junk e-mail, so they will stop sending them eventually.
The cost of sending millions of messages simultaneously is very small, so it only takes a small percentage of responses to make the endeavor profitable for spammers. Unfortunately, many vulnerable individuals “fall for” the tactics and find themselves the victim of a scam.

Myth 4: TTU sells e-mail addresses to companies.
TTU does not sell e-mail addresses to any outside entity. The only time such information is released is under the terms of an arrest warrant, a legal summons, or an Open Records Act request. Under FERPA, students have the right to prevent the publication of some of their personal information. They may exercise that option at http://techsis.tosm.ttu.edu/student.

And the final myth… TTU does nothing about SPAM and Junk e-mail
Hopefully this bulletin provides strong evidence to the contrary! Effective SPAM management must be a partnership between the TTU IT Division and the University community.

Operation SPAM Management: The TTU IT Division in Action
The TTU IT Division runs a sophisticated TechMail system that includes software that “scores” each incoming e-mail message. Those messages that are deemed “suspect” are automatically delivered to your “Junk E-mail” folder. The scoring mechanism is updated according to industry standards, on a regular basis. Given that no scoring mechanism is perfect, occasionally a legitimate message is marked as “suspect” and sent to junk e-mail. If we elected to automatically delete “suspect” e-mail messages, which the industry refers to as “censorship,” then you would never have the opportunity to review all e-mail sent to your address.

In addition to directing “suspect” e-mail to your “Junk E-mail” folder, the IT Division also takes the following actions to reduce malicious SPAM:

• We have a state-of-the-art virus protection system running in concert with the TechMail systems. Attachments containing destructive files are quarantined and deleted. You will still receive the electronic mail, but it no longer will contain the malicious attachment.

• The TechMail systems block attachments in certain formats that are conducive to viruses and worms. Some examples include: .exe; .com; .csr; and .pif. Note that .zip files are allowed, but the TechMail systems unzip the files first and scan for viruses. If a virus is detected, the file is removed.

Operation SPAM Management: The TTU Community in Action
For those of you using TechMail, the IT Division recently implemented a server-based solution to help manage SPAM by placing suspect e-mails directly in your “Junk E-mail” folder for you to review. Suspect e-mails are only deleted after your review, giving you full control of any e-mail you receive. The most powerful SPAM management comes from settings within your e-mail software. You can reduce your SPAM by implementing the following practices:

Continued on back.
**General Recommendations**

- Enable server-side filtering at [http://mail.ttu.edu](http://mail.ttu.edu) by choosing "Options," then checking "Filter Junk E-mail" and saving your choice.
- Enable "International top-level domain blocking in Outlook 2003" (see link below).
- For spam delivered to your Outlook 2003 Inbox, right click on the message, select "Junk E-mail," and "Add Sender to Blocked Sender's List."
- Periodically review the contents of your Junk E-mail folder for messages that you wish to receive and add them to your Safe Senders List using either Outlook or Outlook Web Access.
- To avoid mailbox quota issues, junk e-mail should be reviewed carefully, and then deleted or archived on a regular basis.
- Select "SAFE LIST ONLY" for the highest level of filtering available in both server-side and client-side processing.

**Customizing Your Junk E-Mail**

1. Configuring Junk E-Mail Filters in Outlook 2003: Enable Cached Exchange Mode (Note: Cached Exchange Mode creates a self-synchronized copy of your messages that are stored on both the server and your client.)
   a. On the "Tools" menu, select "E-Mail Accounts."
   b. You will now see the E-Mail Accounts Wizard window. Select "View or change existing e-mail accounts" and click "Next."
   c. The E-Mail Accounts window will now appear. Select "Microsoft Exchange Server" and click the "Change" button.
   d. The Exchange Server Settings window will now appear. Check the box next to "Use Cached Exchange Mode" and then click "Next."
   e. Now click the "Finish" button.
   f. You must now exit and then reopen Outlook 2003 to continue.
2. Change Junk E-Mail settings in Outlook 2003
   a. On the "Tools" menu, select "Options."
   b. In the "Options" dialog box, click on the "Junk E-mail" button.
   c. Choose the level of junk e-mail message protection you want and click "OK."
3. Add a sender to your Safe Senders List, Safe Recipients Lists, or Blocked Senders List:
   a. Right-click on a message from the sender.
   b. Point to "Junk E-mail," and click either "Add Sender to Safe Senders List," "Add Sender to Blocked Senders List," or "Add Recipient to Safe Recipients Lists."
   c. The first time Outlook 2003 moves a message to the Junk E-mail folder, it will notify you with a dialog box.

**Safe Computing Tips:**

**Strong Password Requirements**

- Must be 8 – 15 alphanumeric characters
- Must contain upper & lower case characters
- Must contain a number(s)
- Must NOT contain a number as the first or last character
- Must NOT contain any word found in a dictionary
- May contain punctuation marks or special characters
- Must be changed every ninety (90) days
- Cannot be reused for one year

Visit [http://www.infotech.ttu.edu/security](http://www.infotech.ttu.edu/security) for additional information about password policies.

Contributions by: Katherine Austin, Ph.D., Alvin Mills, Lori Dudley, Joshua Harrison, Carleen Kelly, Kathleen Burrell, Stephen Ayers, Josh Mathis, and Josh Humphreys.

**Top Ten Phishing Scams**

"Phishing" is the use of electronic mail to trick the recipient into providing personal information, clicking on a link and infecting the system, or opening an attachment that installs software on the system. Phishing artists prey on human vulnerabilities, concerns, and fears. APWG, the Anti-Phishing Working Group (2006) tracks and investigates phishing scams as they emerge. The most common phishing scams are as follows:

- eBay member questions or purchase inquiries;
- Internet banking alert – various bank names are used to indicate that your account has been violated and you must reply with your personal information to secure your account;
- Credit card survey reward program – asks you to click on a link, complete a survey, and have your credit card credited for $50;
- PayPal notifications regarding a charge or the addition of another individual – asks you to verify your information and confirm your approval;
- Credit card suspension notifications – various credit card companies are listed and indicate that your account has been suspended for fraudulent activity, requesting that you respond to reactivate the account and authorize investigation;
- Credit union requests to update your account information;
- Amazon.com notification – indicates that you have been charged for an amount (typically over $2,000) and that you must confirm or deny the charge by clicking on a link;
- Online banking password confirmation – requests that you reply and change your password, asking you to enter your current account, existing password, and new password;
- Network security violation – asks that you enter your personal information to verify your authorization to an account, location, or institution; and
- Philanthropic requests – references a tragic event (Hurricane Katrina victims, injured civilians in the Iraq War, etc.) and requests that you respond with a credit card donation.

These e-mail messages often look official and professional, as if they represent a legitimate source. The bottom line is that no reputable financial organization, corporation, or organization will request sensitive information from you via electronic mail. Your best defense is the delete button and effective utilization of SPAM filters.