Message from the CIO

I was pleased to see the level of TTU community participation in our recent educational events. Second only to our vital partnerships and TTU community collaborations, education is a critical component of effective IT strategies and management. In this issue, we highlight spam myths, taken from our recent roundtable event. We are also recognizing two examples of quality service in the IT Division, the TTU network upgrade team and Mr. Dennis Edwards. Our latest addition is the “TTU Techno Quiz.” I encourage you to test yourself with these questions; you will find the answers on the back. Keep those comments and suggestions coming in – we always appreciate feedback from you!

-Sam Segran
Associate Vice President for IT and Chief Information Officer

Dispelling Myths: Highlights from the Recent Spam Roundtable

On January 31, the TTU IT Division hosted a Spam Management Roundtable, as part of our Safe Computing Practices Campaign. This article highlights key information for those that were unable to attend, as well as those that have requested a synopsis. You can view the complete educational materials from the roundtable at http://safecomputing.ttu.edu/ttu/events/.

Despite the number of advertisements that reach our inboxes offering fantastic deals on loans, prescription medications, software, and credit cards, responding to these mass electronic mailings can be dangerous. While most people refrain from responding to these unbelievable offers, enough people express interest to make spam profitable to businesses. In addition to a potential non-secure transaction, spam also poses other risks, such as identity theft and damage to hardware and software. For instance, some spam is not really intended to sell anything; its only purpose may be to collect your personal information. Remember — if it looks too good to be true, it probably is!

Most spamming operations do not rely on their own hardware and networks to distribute the spam. Professional spammers acquire host computer systems spread throughout the world (a lot of which happen to be in the United States). Typically the host systems are home computers with fast Internet connections that have been commandeered (also referred to as a “zombie”) without the knowledge of the owner. Ironically, the owner of the host system may not be aware that their system has been “abducted” by spammers.

To date most legislation has not been effective against spam. The Can-Spam Act within the United States has made an effort to curb the spam epidemic. However, no matter what laws are enabled for the United States, those laws do not impact international spammers. Furthermore, legislators have a difficult time operationally defining spam. Spam is used to describe everything from commercial ads to chain letters. As a result, legislation is very difficult to enforce. Many spammers are virtually impossible to track down and apprehend. Spamming operations realize the difficulty in enforcement, making the financial rewards outweigh the risks.

Lobbyists, such as the Direct Marketing Association (DMA), have a strong interest in ensuring the Internet can be used for legitimate marketing and influence the creation of legislation.

Most spam includes an “opt-out” option somewhere in the text of the message. Unfortunately opt-out list are often used to validate e-mail addresses. Remember that emailing lists are inexpensive when compared to other forms of sales leads and confirmed e-mail addresses garner premium returns in the spam world. Another problem with responding to spam with an opt-out request is the validity of the return address. Forged return addresses, referred to as spoofing, hide the identity of the spammer. The forged address may look like a friend or family member, increasing the chance a user will open the e-mail or attachment. Unfortunately, there are no clear cut methods for consumers to determine the legitimacy of an individual return address.

Your best defense against spam is effective mail client filters; creating safe senders, safe recipients, and blocked senders lists. Your second best defense is the delete button! For additional information or assistance configuring your e-mail filters, please contact IT Help Central at 742-HELP (4357).
Network Infrastructure Upgrades

Beginning December 8, 2006, Telecommunications Services began a technology upgrade to refresh the network infrastructure of approximately 50 buildings on the University campus. The project includes buildings with network equipment installed in the mid-to-late 90s that needs to be replaced. This upgrade will be largely transparent to the campus community and will improve the network foundation, so that TTUnet can continue to deliver high-quality services.

Prior to any scheduled work, detailed information is sent to the departments located within each affected building. As much as possible, the work will be performed outside of normal business hours to minimize the impact to faculty, staff, and students. The upgrade will be complete later this semester.

Mr. Dennis Edwards

After 25 years of dedicated service, Mr. Dennis Edwards will be retiring, effective February 28, 2007. Over the years he provided technical consulting and assistance to students, faculty, and staff. He has been a staple to information technology at TTU. As an early employee of the original “Academic Computing Services,” Mr. Edwards began his career at TTU providing IBM and VMS mainframe support. He also became a lead consultant for advanced statistics software, such as SAS and SPSS. In the last 25 years, he taught hundreds of faculty, staff, and students SAS and SPSS skills. As his last promotion within the current TTU IT Division, he was responsible for managing quality assurance at IT Help Central. He has been a valuable employee and we will dearly miss him! Please join us in acknowledging his hard work and service.

Safe Computing Tips: Spam “Busters”

Spam has become an international problem and continues to plague private and public email servers. As indicated in the article in this bulletin, spammers continue because a small percentage of people respond to spam, making it a low-cost, high-yield endeavor. An educated university community, coupled with a strategic TTU IT plan is our best approach.

We recommend the following tips:
1. Do not reply to spam;
2. Configure your junk mail filters or safe senders list ([http://www.depts.ttu.edu/helpcentral/info/antispam.php](http://www.depts.ttu.edu/helpcentral/info/antispam.php));
3. Do not click on links within a message to “opt out”;
4. Review where your email address is posted on the Web; spammers often mine web sites for addresses;
5. Do not give your email address to vendors, unless you have a business reason to do so;
6. If you do give your email address to a company, read their privacy policy and make sure they do not sell mailing lists to online marketing companies;
7. Do not open attachments contained in spam messages; and
8. If you are uncertain about the legitimacy of a message, then investigate using the telephone or you may also contact IT Help Central at 742-HELP (4357).

Contributions by: Katherine Austin, Ph.D., Lori Dudley, Kathleen Burrell, J.D., John Vandygriff, Joshua Harrison, Adrienne Daniels, Carlene Kelly, and Stephen Ayers.

IT Web Site: [http://www.infotech.ttu.edu](http://www.infotech.ttu.edu)
Texas Tech University Web Site: [http://www.ttu.edu](http://www.ttu.edu)
Computer-Based Training (CBT): [http://cbt.ttu.edu](http://cbt.ttu.edu)
Laws and Texas Tech Policies: [http://www.itts.ttu.edu/documentation/laws](http://www.itts.ttu.edu/documentation/laws)