Message from the CIO

October 2010 is the sixth annual Department of Homeland Security “Cyber Security Awareness Month.” As part of this national initiative to raise awareness and minimize risks associated with cyber crimes, the TTU Office of the CIO has designated the week of October 18th as “TTU Cyber Security Awareness Week.” During this month, we have already been providing educational information through messages, posters, public service announcements, and displays. To highlight this critical IT topic, we are dedicating this issue to key IT security topics: Understanding “Scareware,” the IT Security Landscape, and Reporting a Security Incident. In addition, we have several Upcoming Security Events for the TTU community. We will culminate the week of activities with our Fall Shred Day. Securing our information resources at TTU is a shared responsibility; please think before you click!
-Sam Segran
Associate Vice President for IT and Chief Information Officer

Don’t Get Spooked by Scareware!

Scareware, also known as rogueware, is defined as malicious software that poses as security software, such as an antivirus or anti-spyware program, in order to trick you into installing it or clicking on links to get rid of the warning messages. In the last two years, the amount of “scareware” has risen dramatically, infecting unsuspecting visitors to compromised websites. When you visit one of these sites, a pop-up window warns you that your system is infected with a virus, and recommends that you click a link to install their brand of antivirus software. When users click the link, the software installs itself on the user’s computer and begins to disable legitimate antivirus and anti-spyware software, such as Symantec EndPoint Protection. The software may also attempt to trick you into providing your credit card information in order to “purchase” a full version of the fraudulent software.

The TTU IT Division recommends the following Safe Computing tips to help protect yourself from this and other online scams:

- Do not install Antivirus/Anti-Spyware software that you are unfamiliar with. Symantec EndPoint Protection is available for download at http://eraider.ttu.edu at no cost to the University community.
- Don’t give your credit card information to an online vendor unless you are certain that they are legitimate and the transaction is secure. Most secure website addresses will begin with “https://” or will display a padlock at the bottom of your browser window.
- Keep current on critical system updates:
  - Windows Users: http://windowsupdate.microsoft.com
    For instructions to set up Automatic Updates, visit http://safecomputing.ttu.edu/criticalupdates.php
  - Mac Users: Use Software Update in System Preferences
- If a website appears suspicious, or you have any doubts whatsoever about its validity, contact IT Help Central or your local computer support personnel first. It is better to be safe than sorry!

Additional Safe Computing tips can be found online at http://www.safecomputing.ttu.edu or by contacting IT Help Central at (806) 742-HELP or by e-mail at ithubcentral@ttu.edu.

The IT Security Landscape – The Threat Grows

Reports, evidence, and expert opinions in the IT industry indicate that security threats will continue to grow, targeting individual users and systems. Enticements designed to lure individuals to malicious web sites or to unknowingly download and install malicious software will also become more creative and more difficult to detect. In this constantly changing environment, individuals need to be more informed and aware than ever before. The TTU Office of the CIO will continue with our Safe Computing Practices campaign, to include bulletin articles, periodic TechAnnouncements, training opportunities, and website information (www.safecomputing.ttu.edu).

Internet-based data theft has become a profitable underground sector that depends on successfully preying on individuals. Some of the specific trends include:

- More sophisticated hacking and theft tools are widely available, with an organized market for sale and distribution;
- Some individuals offer to lease their computer systems to be used by Internet criminals as host computers;
- Criminals have created an intricate market for buying and selling stolen identity information;
- Applications that steal confidential data (such as passwords, credit card information, and Social Security numbers) are constantly improving and finding new software vulnerabilities to exploit; and
- Internet criminals have begun to mine social networking sites and tools in order to locate private information and perpetrate theft.

While the TTU IT Division works diligently to constantly improve infrastructure and IT security practices, you are an important partner in protecting institutional information resources. IT security is a shared responsibility and we appreciate your partnership in improving the institutional IT security posture.

Procedure for Reporting an IT Security Incident

Texas Tech University has procedures in place for reporting computer security incidents as outlined in the Incident Management Security Policy, which can be reviewed online at http://www.infotech.ttu.edu/security/docs/incident_management.php. Faculty and staff must file a report prior to any attempt to remediate, solve, or troubleshoot the incident.

continued on back
A wide variety of data security incidents must be reported including: virus, worm, and Trojan horse infections; unauthorized use of computer accounts and systems; complaints of improper use of information resources; data theft and fraud; and computer system compromises. Should you become aware of a data security issue, there are two fundamental things that you should do:

- Immediately report the incident as outlined below:
  a. For virus & worm infections, compromised systems, or improper use complaints, contact the IT Security Team at security@ttu.edu or (806) 742-0840; or
  b. For potential criminal acts (data theft, fraud, etc.), the exposure of confidential information, or a threat to personal or homeland security, directly contact either the TTU Information Security Officer, J Stalcup, at (806) 742-8000 x7000 or J.Stalcup@ttu.edu, or TTU Chief Information Officer and Information Resources Manager, Sam Segran, at (806) 742-5151.

- Perform appropriate remedial action in accordance with the Information Security Officer’s instructions and IT guidelines.

- Some incidents will require some investigation to assess the severity, scope, and risk. In many cases, further forensics are required and will be conducted by the Information Security Officer or his designee. Again, please contact the security staff above before altering the computing system or attempting to “fix the problem.” Typically, virus and worm infections can be cleaned up without further investigation and IT Help Central can provide assistance.

For more information or questions, please contact IT Help Central at (806) 742-HELP (4357), via e-mail at ithelpcentral@ttu.edu or online at www.ithelpcentral.ttu.edu.

It’s Here! Fall 2010 Shred Day

Since 2007, the TTU Community has shredded over 43 TONS of documents as a result of this event! We appreciate your participation and partnership.

As part of TTU Cyber Security Awareness Week, the TTU Office of the CIO, in partnership with the TTU Archives & Records Management and Traffic and Parking, invites you to participate in Fall Shred Day on Friday, October 22, from 9am-3pm, in the United Spirit Arena Parking Lot. In preparation for the event, we suggest that you review paper files and gather documents to be shredded.

Shred Day Event Details:
When: Friday, October 22, 9am-3pm
Service: The TTU Office of the CIO has contracted with Shred It/SecureIT and Westex Documents to provide mobile shredding units
Where: United Spirit Arena Parking Lot, north end
Who: TTU Community, including personal documents

Please note that Custodial Services provides departmental shredding services for your shredding needs outside of Shred Day. For additional information about Custodial Services shredding, please contact Custodial Services at (806) 742-9777.

Upcoming IT Security Events

Tuesday, October 19th: Microsoft Security Presentation
      Red Raider Lounge, SUB, 2-4pm
      (refreshments)

Friday, October 22nd: Shred Day
      United Spirit Arena parking lot, 9am-3pm

Monday, October 25th: National Speaker Corey Ciocchetti
      Social Networking Security
      Allen Theatre, SUB, 2pm-4pm
      (refreshments)

Thursday, November 18th: Advanced Application Security Session – Part II
      Lanier Auditorium, School of Law, 10am-2pm (lunch provided)

To register for the Microsoft event, Ciocchetti presentation, or the Advanced Security session, please email ITevents@ttu.edu or contact Britta Tye at (806) 742-1650.

Copyright 2010 Texas Tech University

Past copies of TTU IT Division Bulletins may be found online at http://www.infotech.ttu.edu/itbulletin