Message from the CIO

Spring is well underway and the campus is a flurry of energy and activity - a rejuvenating time on an academic campus. In this issue, we emphasize major cybersecurity areas to watch in 2012. We address one of those areas in an article warning you about “Spear Phishing Attacks” and IRS scams delivered through email. We also announce our new Mobile Charging Stations located at the ATLC, west basement of the University Library building; we have plans to put stations in all our IT-managed public computing facilities. Finally, we encourage you to take advantage of our free online professional development courses, computer-based training (CBT) - anywhere, anytime, for any Raider. Enjoy the spring season and remember to practice safe computing. Go Tech!

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

Cybersecurity Areas to Watch for 2012

Our increased reliance on the Internet exposes us to increasing cyber security risks. Awareness is the first line of defense against being a victim of a cybercrime. The TTU IT Division reminds you to be cautious about all electronic communications and to THINK BEFORE YOU CLICK. For more information on safe computing tips, visit www.safecomputing.ttu.edu.

Mobile Devices & Apps

Each new smart phone, tablet, and mobile app creates another opportunity for a cyber-attack. Threats on mobile devices may include access to your personal information, such as your physical location or contact lists. Apps have become a prime target for some criminals to apply harmful code on your mobile device. Some of these apps are designed to eavesdrop on your phone calls and/or capture your text messages. Cyber criminals have become skilled at hiding malicious code within a legitimate mobile app, successfully luring unsuspecting customers.

Major National and International Events

This year will include the U.S. Presidential election, London Olympics, and the Mayan Calendar end-of-time prediction. All of these events will be heavily covered in 24-hour news, Twitter feeds, Facebook posts, YouTube videos, and other Internet forums. Cyber criminals will likely take advantage of these popular stories to target readers and infect users with sites or messages designed to look like legitimate news stories.

Social Engineering

Cyber criminals continue to use social network space as a playground for the development, testing, and deployment of malicious code. The Texas Department of Information Resources anticipates a flood of malware designed to look like legitimate hosted services for antivirus, storage, and encryption.

Spear Phishing Attacks

Spear phishing attacks are carefully targeted scams, typically delivered through email messages, text messages, or tweets from a seemingly trusted source. Cyber criminals take advantage of seasonal or circumstantial opportunities—such as tax deadlines, holidays, natural disasters, or domestic/world events.

CBT: 5,300 Free Professional Development courses…Just an eRaider Away

Computer-Based Training (CBT) is an online, self-paced interactive training system. The current catalog includes over 5,300 courses, ranging from basic and advanced technology skills, to general financial and management skills. These courses can be used for professional development, résumé enhancement, and as an instructional supplement. Courses are available to download so that you may work offline, and include the ability to track progress, set goals and create reminders. The wide range of course offerings make CBT courses valuable for students, staff, and faculty with all experience levels, training needs, and technical backgrounds.

Browse the catalog to see what resources are available. Add learning assets from the catalog to your learning plan, or launch them directly from the catalog. The catalog is organized by subject matter and by related professional certification for easy navigation. TTU has created a project management catalog that includes a range of specific and general skills. We also have established a SharePoint 2010 training catalog that includes designer, developer, administrator and basic user training.

Examples of other available course topics:

- Application skills (Word, Excel, PowerPoint, Access, Outlook)
- Business certifications
- Adobe Acrobat 5
- Leadership essentials
- Microsoft Office for Mac 2011
- Customer service skills and management skills
- Finance and accounting curriculum

For more information about these courses, please contact Technology Support at (806) 742-1650 or find a complete list of courses by visiting the Computer Based Training website at http://www.cbt.ttu.edu. For technical assistance, please contact IT Help Central at (806)742-HELP (4357).
SCP Tip – Be Aware of IRS Email Scams

As we approach the Federal tax deadline, Internet criminals may be ramping up IRS tax scams designed to steal your information. The Texas Tech University Office of the CIO wants you to be aware of email that uses the IRS name, logo, or website, and requests confidential information from you. Remember that the IRS does not typically collect tax information by email.

Some of these email scams are fairly sophisticated and hard to detect. One of the most common IRS scams informs the recipient that he or she is eligible to receive a tax refund for a given amount. The email instructs the recipient to click on a link contained in the email to access and complete a form for the tax refund. The form requires the entry of personal and financial information. Several recent variations on this scam have claimed to come from the Exempt Organizations area of the IRS. Don’t fall prey to these attempts to steal your information!

Warning signs that the “IRS” email is fraudulent:

- Requests personal and/or financial information; such as name, SSN, bank/credit card account numbers;
- Requests security-related information, such as mother’s maiden name, password, or PIN;
- Offers a special tax refund program available by email;
- Invites you to participate in an IRS survey and receive a stipend or discount on taxes owed;
- Threatens a consequence - additional taxes or frozen tax refunds - for not responding to the email;
- Misspells “Internal Revenue Service” in the email text or website link supplied; and/or
- References an IRS link that does not contain http://www.irs.gov - to see the actual link address, place your mouse over the link text without clicking.

If you receive a suspicious email claiming to come from the IRS, take the following steps:

- Do not open any attachments to the email or click on any links;
- Contact the IRS at 1-800-829-1040 to determine whether the IRS is trying to contact you;
- Forward the suspicious email to the IRS at phishing@irs.gov; and
- Delete the message once you have reported it.

For more safe computing tips, visit www.safecomputing.ttu.edu.

Contributions by: Katherine Austin Beltz, Ph.D., Shannon Bailey, Jeff Barrington, Drew Brooks, Ron Nail, Britta Tye, Allen Young, and John Van Dygriff.
Safe Computing Practices Committee: Sam Segran, Katherine Austin Beltz, Ph.D., Jeff Barrington, Darrell Bateman, Pulin Bhatt, Shannon Cepica, Paco Diaz, Scott Hall, Mark Holwerda, Danny Mar, Ron Nail, Yung Ng, Randall Osborne, Mike Simmons, Phil Smith, Ph.D., J Stalcup, Britta Tye, John Van Dygriff, Allen Young, and assistance from IT Division leadership and staff.