Contributions by: Katherine Austin Beltz, Ph.D., Darrell Bateman, Shannon Cepica, Britta Tye, Binari Witanapatirana and Allen Young.
Safe Computing Practices Committee: Sam Segran, Katherine Austin Beltz, Ph.D., Jeff Barrington, Darrell Bateman, Shannon Cepica, Scott Hall, Danny Mar, Ron Nail, Yung Ng, Randall Osborne, Mike Simmons, Phil Smith, Ph.D., J Stalcup, Britta Tye, John VandyGriff, Allen Young, and assistance from IT Division staff.

IT Website: *www.IT.ttu.edu*
Texas Tech University Website: *www.ttu.edu*
Computer-BasedTraining(CBT): *cbt.ttu.edu*
Safe Computing Practices: *safecomputing.ttu.edu*

TIPS SAFE COMPUTING

Scan the barcode to view IT Bulletins online
www.IT.ttu.edu/itbulletin

TEXAS TECH UNIVERSITY
Information Technology Division™
Mail Stop 2008
Phone: 742-5151
Fax: 742-5155

TEXAS TECH UNIVERSITY
Office *of the*
Chief Information Officer™

From Here, It's Possible

Information Technology Division | **Bulletin**

vol.10 no.3 | October 2013

SAFE COMPUTING
Our goal is to empower people with the knowledge and tools to reduce computing security threats

Message from the CIO

October is **National Cyber Security Awareness Month**, sponsored by the Department of Homeland Security in cooperation with the National Cyber Security Alliance and the Multi-State Information Sharing and Analysis Center. Each year, we participate by providing IT security educational events and information – above and beyond our ongoing Cyber Security Awareness Campaign. In this issue, we provide information about **Malware Delivered Through Apps, Mobile Device Security, Password Strengthening, and Social Networking Safety.** We also feature an article on **Phishing Scams**, as some in the TTU Community fall prey each year, putting personal and institutional data and information resources at risk. Finally, we provide a reminder about **Reporting a Security Incident,** including the proper protocol. Creating and maintaining a robust security posture for Texas Tech University is critical for operations, as well as facilitating the achievement of our institutional strategic goals. We rely on your partnership and vigilance to protect institutional information resources. We strongly encourage you to take advantage of the events and information that we will offer this month, as well as throughout the year. Go Tech!

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

Malware: Watch Your "Apps"

If you own a smart phone or a tablet, you have probably downloaded "apps" for a variety of features, such as; listening to music, online banking, playing games, or connecting on social media networks. Unbeknownst to consumers, cyber criminals are exploiting the rising demand for mobile apps by injecting "malware" into various apps. Malware is a general name for any software code that is designed to steal your information, use your device as a host to spread destructive code, and/or destroy information on your device. Our biggest suggestion for avoiding this criminal activity is to be vigilant when downloading apps. Reputable app stores carefully evaluate apps (example; Apple App Store), and require that any app available in their store meet high security requirements before being released to consumers. Beware of free or low-cost apps from unknown, usually much smaller app stores, as the store is less likely to require stringent code standards and formal app review for apps submitted for distribution in the store. Many of these apps either contain malware or have been illegally reproduced. Downloading apps from less trustworthy sources increases the risk that your smart phone or tablet will be infected with malware, leaving sensitive and/or confidential information vulnerable.

Another point of caution when downloading apps involves app updates. Typically, apps are periodically updated by developers to add the latest features and deploy security patches. Only install updates that come as notifications from the app store where you originally purchased or obtained the app. Also beware of app update notifications that are communicated via text messages or email, as they may not be legitimate. Criminals may attempt to intercept the normal update process by directing you to another app store that contains malware, instead of the legitimate update.

If you need assistance or would like more information, please contact IT Help Central at (806)742-4357 (HELP) or via e-mail at **ithelpcentral@ttu.edu.**

Keeping Your Mobile Device Secure

Mobile technology is rapidly developing, providing convenience and connectivity inherent in computing on-the-go. The TTU IT Division reminds you that just as your desktop computer can become infected and overrun by malicious intruders, so can your mobile devices. Awareness of what you are doing and where you're visiting, as well as using safe computing practices, can help protect mobile device activity.

Many mobile devices offer services beyond making phone calls, texting, and receiving e-mail. With such a wide variety of mobile devices and options for connectivity, we strongly recommend that you exercise caution and be diligent about practicing safe computing. The United States Computer Emergency Readiness Team (US-CERT) recommends the following best practices to help protect mobile devices:

- **Enable the personal identification number (PIN) or password to access the mobile device, if available;**
- Maintain up-to-date software, including operating systems and applications;
- Install antivirus software as it becomes available and maintain up-to-date signature and engines;
- Encrypt personal and sensitive data, when possible;
- Disable features not currently in use such as Bluetooth, infrared, or Wi-Fi;
- Set Bluetooth-enabled devices to "non-discoverable," so that unauthenticated devices cannot detect them;
- Use caution when opening email and text message attachments;
- Use caution when clicking links contained in text messages and email;
- Avoid opening files, clicking links, or calling numbers contained in unsolicited email or text messages;
- Avoid joining unknown Wi-Fi networks;
- Don't install apps you don't need and delete unused apps;
- Delete all information stored in a device prior to discarding it;
- Maintain situational awareness regarding mobile device threats; and
- **Do not leave your mobile device unattended.**

Antivirus software exists for some mobile devices; however, it can only assist in protecting against known threats. We are all responsible for understanding the threats and proactively taking steps to avoid them. A high degree of vigilance is necessary to successfully prevent and mitigate future threats to mobile devices.

If you need assistance or would like more information, please contact IT Help Central at (806)742-4357 (HELP) or via e-mail at **ithelpcentral@ttu.edu.**

CYBER SECURITY AWARENESS MONTH

Reporting Security Incidents – It's Everyone's Responsibility

Texas Tech University has procedures in place for reporting computer security incidents as outlined in the Incident Management Security Policy.

The full security incident reporting procedure can be reviewed online at *http://www.infotech.ttu.edu/security/docs/incident_management.php*.

A wide variety of data security incidents must be reported, including: malware 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 steps that you or your departmental/college technology professional should take:

1. Immediately report the incident as outlined below:

   a. For malware infections, compromised systems, or improper use complaints, contact the IT Security Team at **security@ttu.edu** or (806) 742-0840
   b. To report an IT-related incident that may be a criminal act (data theft, fraud, etc), the exposure of confidential information, or a threat to personal or homeland security, directly contact:
      i. TTU Information Security Officer, Darrell Bateman (**darrell.bateman@ttu.edu**), at (806) 834-3669, or
      ii. TTU Chief Information Officer, Sam Segran (**sam.segran@ttu.edu**), at (806) 742-5151.

2. Perform appropriate remedial action only in accordance with the Information Security Officer's instructions and IT guidelines.

Some incidents will require investigation to assess the severity and to determine whether further forensics are required. Please contact the security staff above before altering the computing system or attempting to "fix the problem." Typically, malware 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)742-4357 (HELP), via e-mail at **ithelpcentral@ttu.edu** or online at *http://ithelpcentral.ttu.edu*.

Head's Up: Don't Fall Victim to Phishing Scams

"Phishing" scams, schemes to steal information or device resources disguised as a legitimate email, continue to be a successful and profitable endeavor for Internet criminals, and many in the Texas Tech University Community fall prey every month, putting personal and institutional information resources at risk. Each year, Texas Tech faculty, staff, and students respond to phishing scams that require institutional resources to repair the damage. The IT Division Security team blocks the known sources and associated web links of these emails as soon as we become aware, but criminals can quickly adapt and a similar message may appear from a different location, and bypass the block. We count on your partnership to help protect institutional information resources, as well as your personal information.

Historically, any international disaster or media event causes an increase in these email scams and threats. Criminals often use tragic events as opportunities to lure people into opening an alleged document, clicking on a link, or providing information via a returned email. Examples of common email scams:

- **Requests for donations to charitable organizations** - Many of these schemes appear to be from a reputable charitable organization assisting with a current national or international crisis. The message may request that you donate online, by providing your personal banking information or credit card information.
- **Requests for financial information** - Many of these schemes appear to be from a reputable bank, mortgage brokerage, or financial consulting firm. The message will request your personal banking information, typically under the guise of verifying your account or confirming a transaction.
- **Promises of financial gain** - Claims such as "Make money in your spare time," "Earn thousands per week!" or "Guaranteed income" are almost always a sure signs of a scam. The sender usually requests that you make a small investment with your credit card in order to "earn your fortune."
- **High pressure tactics** - For example, "Sign up now or the price will increase." Again, a legitimate deal with such a restricted time line will probably not be conducted over email.
- **Prize notifications** - Countless scams require that you pay a small fee to claim your prize. The fee is often allegedly for transaction costs, shipping, handling, or pre-award taxes.
- **"FREE" goods, services, and opportunities** - Offering free items is used to lure people into additional purchases, such as other products and fees associated with the "free" items.
- **Internet auctions that require pre-payment** - In a world comfortable with online stock trading and eBay purchasing, illegitimate Internet auctions have become a popular venue for criminals.

- **Requests to be added to your "friends" list** - Criminals have begun posing as social networking companies, such as Facebook, LinkedIn, MySpace and Yelp!, by indicating that someone has invited you to join their "friends" list or by requesting that they be added to your "friends" list.

The TTU IT Division recommends the following cyber security practices to protect yourself and TTU information resources from email scams:

- Do not click on links contained within an email unless you are certain of the sender's identity and expecting the information;
- Do not open attachments unless you are certain of the sender's identity and expecting the information;
- Delete and do not reply to any of these emails;
- Update the antivirus software on your desktop, laptop, and/or mobile device; and
- Keep current on critical system updates:
  - Windows Users: *http://windowsupdate.microsoft.com*
  - Mac Users: Use Software Update in System Preferences.

For questions regarding phishing scams or if you responded to one of these emails and need assistance, please contact IT Help Central at **ithelpcentral@ttu.edu** or (806) 742-4357 (HELP).

Bolster Your Passwords

Internet criminals also know that most people use the same password for multiple accounts. If they figure out the password to your personal email account, and you use that same password for your bank account or another account with sensitive information, then they now have the ability to breach multiple accounts – and they will! It is in your best interest to create unique and complex passwords for personal accounts – even if it takes more on your part to remember them. Remember that you should never use your eRaider password for any account other than for eRaider! Suggestions for creating unique and complex passwords:

- Consider starting with a sentence or phrase that is meaningful to you, but not a common sentence or phrase;
- Remove the spaces between the words in the sentence;
- Convert the words into "shorthand" and/or intentionally misspell a word;
- Add length and complexity with numbers and symbols that are meaningful to you; and
- Use at least nine characters with a mix of numbers, letters, and special characters (!,@,#, etc).

Protecting Institutional Information Resources & Data

As employees of a state institution and in the course of our work duties, we all have a responsibility to protect institutional information resources and data, especially confidential information, such as social security numbers, student grades, home addresses, financial information, etc.. Please review the relevant TTU IT Security policies at *www.depts.ttu.edu/infotech/security*, specifically, the policies on Acceptable Use, Information/Data Classification, and Privacy that address individual responsibility to safeguard confidential data.

For those that manage computing systems, you have additional responsibilities associated with safeguarding data under your purview, regardless of whether you inherited a system or managed it from inception. We ask that you carefully review applicable TTU IT Security policies, such as Account Management, Backup-Business Continuity, Incident Management, Multi-Functional Device Hardening, Password, Physical Access, Security Monitoring, Server Hardening, and Workstation Hardening. We also ask that you familiarize yourself with the following TTU Operating Policies (*www.depts.ttu.edu/opmanual/*):

52.01 - Information Technology Operations

52.02 - Infringement of Copyrights in Information Technology

52.03 - Obtaining Data Network Services

52.04 - Information Technology Security

52.05 - Electronic and Information Resources Accessibility

52.06 - Project Management Practices

52.07 - Website Operations

30.22 - Guidelines for The Educational Use Of Copyrighted Works

48.04 - Cellular Telephones & Data Devices

62.06 - Payment Card Processing By University Departments

62.14 - Red Flag Rules

In addition to the internal scanning and monitoring conducted by the IT Security Team, the Office of the CIO contracts with an external security vendor to evaluate servers and infrastructure. If you receive correspondence from the IT Security Team indicating that a resource under your management has a vulnerability or a security problem, then you are responsible for the timely remediation of that problem to protect Texas Tech resources. As always, please contact the TTU Information Security Officer at **security@ttu.edu** to report any IT security incident or contact **ithelpcentral@ttu.edu** to get assistance in securing your devices and software.

Managing Your Online Reputation

Facebook, Twitter, Instagram, YouTube, and other up-and-coming social media platforms have changed the way reputations are made – and broken. With billions of people using social media, sharing data, tagging pictures, and tweeting, it is important to be aware of your online reputation and to actively manage it.

The IT Division offers a presentation on "Online Reputation Management." Topics include why your online reputation matters, how to manage it and what we can learn from others who had to learn about online reputation management the hard way. This information is relevant to TTU faculty, staff and students in their roles at Texas Tech, and also in their roles as friends and family members. This session is offered as one of our ShortCourses and can also be scheduled as a special presentation. During National Cyber Security Awareness Month, we are offering ShortCourse sessions in the ATLC (west basement of the Library Building). To register for the Online Reputation Management ShortCourse, please visit *http://itts.ttu.edu/training/shortcourses*. If you would like to schedule a special presentation for your department staff, student assistant staff, student organization or any other group, please email **ITeducation@ttu.edu** to arrange the details.