This spring finds TTU in a whirlwind of activity on every front, as the University community prepares for the summer months. In this issue, we introduce two factor authentication (2FA) services that will be deployed soon to further protect critical institutional data and information resources. In an effort to reduce institutional risk associated with unneeded paper files that contain personally identifiable information, the TTU Office of the CIO co-sponsored a successful extended shred campaign, in partnership with the Operations Division. We also invite you to visit the upgraded lab and additional IT Help Central services in the Student Union Building basement. Finally, we provide suggestions to help you protect information against Internet organized crime, such as the recent global ransomware attack. Enjoy the warm weather, and remember to practice safe computing throughout the year. Go Tech!

—Sam Segran, Associate Vice President for IT and Chief Information Officer

**Message from the CIO**

This spring introduces two factor authentication (2FA) for some eRaider web-authenticated resources. 2FA (a password + an additional piece of information you are given) adds an additional layer to account security. In order to access some resources, you will enter your eRaider password, as well as a code typically received by voice or text.

Effective Sunday, March 12, 2017, support for international and non-mobile phone numbers was added to the eRaider account management system. Also, everyone will be required to provide a valid contact phone number for either voice or text verification numbers. This number will be used, along with username and password, to sign in to web applications that require 2FA. You can check your contact number by signing in to https://eraider.ttu.edu and clicking the “Update Information” link under the “Contact Information” area. As a reminder, Texas Tech department and direct phone numbers (beginning with 806-742- or 806-834-) may not be used for this field.

We will provide additional information regarding 2FA, including implementation dates, in the near future. For questions or concerns in the meantime, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

**Two Factor Authentication (2FA)**

The TTU IT Division will soon add two factor authentication (2FA) for some eRaider web-authenticated resources. 2FA (a password + an additional piece of information you are given) adds an additional layer to account security. In order to access some resources, you will enter your eRaider password, as well as a code typically received by voice or text.

**Shred Weeks Success**

A huge Red Raider thank you to our partners in the Operations Division. For the second time this semester, the TTU IT Division was able to provide Shred Weeks to the TTU campus!

From May 22 to June 2, Red Raider Shred picked up 67 boxes, with an estimated weight of 2,680 pounds or 1.34 tons.

This service was provided at no cost to TTU departments, as the TTU CIO Office funded shredding during this additional spring shred campaign.

Red Raider Shred provides shredding services to TTU areas and departments at a very reasonable cost. For additional information, please call Red Raider Shred at (806) 742-8327 (TEAR), or visit www.depts.ttu.edu/services/redraidershred.
With the recent ransomware attacks reported across the globe, the TTU IT Division is reaching out to the Texas Tech community and providing some suggestions for keeping yourself protected. Should your system become infected, a recent backup will be helpful to recover your data. The following suggestions and tools may be employed at your home and work environments to ensure that you are protected on every computer you use:

• Ensure you have Symantec Endpoint, or another anti-malware software package, installed, enabled, and automatically updated. The TTU IT Division provides Symantec Endpoint protection at no charge to all TTU Staff, Faculty, and Students at https://www.eraider.ttu.edu. Be sure you upgrade to the latest version, currently Version 14;

• Confirm that all critical operating system updates are installed, and enable automatic updates. Updates will frequently include patches for newly discovered security vulnerabilities that could be exploited by ransomware attacks;

• Keep all third-party software on your computer updated, as these updates will often patch vulnerabilities that ransomware can exploit;

• Stay vigilant and cautious when receiving emails with attachments, especially when unexpected or from untrusted senders, which may prompt you to enable macros or execute code that launches the ransomware attack;

• Do not visit untrusted websites or follow links provided by unknown or untrusted sources; and

Back up your important data is the most effective way to combat ransomware; clean data can be restored after the ransomware is removed, avoiding any hidden portions of the ransomware that may still reside with your compromised data.

• Utilize the 1TB of cloud storage in OneDrive for Business provided to you through the University’s Office 365 to automatically sync a backup of your data. OneDrive for Business data will also keep previous file versions for a short amount of time, currently 14 days, so maliciously encrypted files could be restored to their previous non-encrypted versions. OneDrive for Business is included in Office 2016, that is available for download through www.office.com;

• For business data, utilize centralized storage solutions—TechShare and SharePoint to store data, as these systems are backed up nightly and can be restored from backups; and

• Utilize removable media for backups, such as USB hard drives and sticks. Ensure that you remove the device when not in use, so ransomware cannot encrypt that data, if your system is infected. Maintain at least three copies of your important data in a secure location, and keep one copy of your data at a safe, off-site location.

Note: If your computer becomes infected with ransomware, immediately disconnect from the Internet to prevent it from spreading. Then contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu for assistance.