Information Technology Division Bulletin

vol. 14 no. 3 | October 2017

Message from the CIO

TTU participated in the inaugural Department of Homeland Security and the National Cyber Security Alliance designation of October as "Cyber Security Awareness Month." This year is our 14th campaign that includes educational sessions and communications for the TTU community. We dedicate this bulletin to timely IT topics and challenges that we face in higher education, and serve to remind us that "we are all responsible" for the protection of institutional, as well as personal, data. We encourage you to be cyber aware, and to think before you click.

As many of you know, we have been providing the IT Division Bulletin online and in print since 2004, and last summer we migrated to a design template to optimize online publication. As such, we will no longer be printing and mailing the TTU Bulletin; we will send you an email with online access information and we will provide printed copies only at our events and educational sessions, or by request to iteducation@ttu.edu. Go Tech!

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

Security Compromise at Equifax Credit Firm

Equifax recently announced a cybersecurity incident potentially affecting 143 million U.S. consumers (source: https://www.equifaxsecurity2017.com). The information accessed includes names, social security numbers, birthdates, and addresses. In some instances, driver's license and credit card numbers were also stolen. Based on Equifax's investigation, the data breach occurred from mid-May through July 2017. Equifax has established a site at https://www.equifaxsecurity2017.com with additional information about this security incident. On this site, customers may also check to see if their personal information was potentially compromised.

If you have confirmed or believe your information is compromised, the following options are available:

- Enroll with a credit monitoring service;
- In this specific instance, Equifax is offering their credit monitoring service at https://www.equifaxsecurity2017.com/enroll. Note: When you register, you will be given an enrollment date. You must return to the website on this date to complete your enrollment in the program. Equifax/TrustedID will not send reminders;
- Utilize multi-factor authentication whenever available;
- Enable account alerts for important accounts, e.g. credit card accounts;
- Monitor your bank and credit card statements closely for suspicious activity;
- If you find evidence that your identity has been stolen, report it immediately to https://www.identitytheft.gov;
- Consider registering for fraud alerts with all credit bureaus (Equifax, Innovis, Experian, and TransUnion). These free alerts must be renewed every 90 days. An extended fraud alert can be set for a longer time period. With fraud alerts, you will be contacted before any credit applications are approved;
- Alternatively, consider utilizing credit freezes with each of the credit bureaus. If you intend to apply for a loan or credit card, you must provide the PIN given to you during the credit freeze setup process. This service may require a small fee;
- At least once a year, obtain and review your free annual credit reports from https://www.annualcreditreport.com/; and
- The Federal Trade Commission recommends filing your tax returns early to help prevent fraudulent filings.

We encourage you to be vigilant in practicing cybersecurity. You may find additional information about this security incident online at https://www.equifaxsecurity2017.com, and more cybersecurity tips at http://cybersecurity.ttu.edu. For more information or questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

Two Factor Authentication (2FA)

For the last several years, the banking industry has been using Two Factor Authentication (2FA) to secure online banking accounts and transactions. 2FA requires a user to have a password and an additional piece of information that you are given in order to access the application, or to complete certain transactions. In the last few months, the TTU IT Division added 2FA for some eRaider web-authenticated resources. In order to access some resources, you will enter your eRaider username and eRaider password, as well as a code that TTU has sent you by voice or text.

Presently, all TTU faculty, staff, and students are required to provide a valid contact phone number for either voice or text verification numbers. TTU will use this number to send you a verification code for those applications that require 2FA.

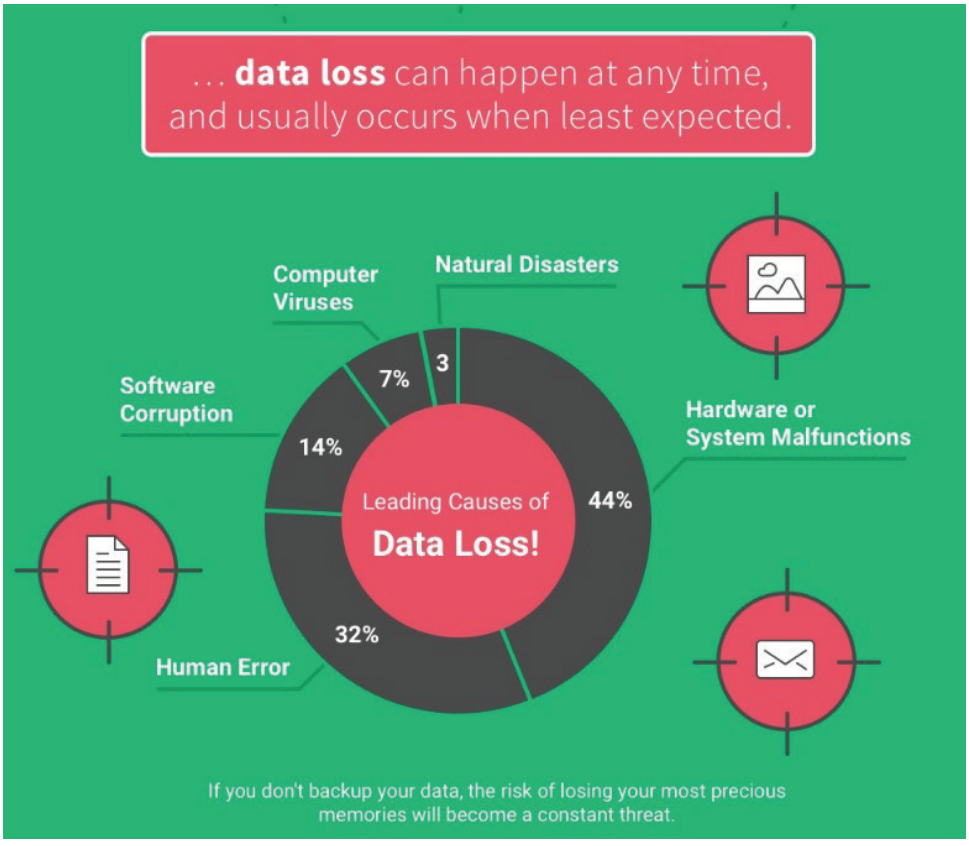
You can check your contact number by signing in to https://eraider.ttu.edu, selecting "Manage Your Account," and clicking the "Update Information" link under the "Contact Information" area. As a reminder, Texas Tech department and direct phone numbers (beginning with 806-742- or 806-834-) may not be used for this field.

We appreciate the collaborations with area and department IT professionals who aided with preparing the TTU community, as well as providing technical support. For questions or concerns, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

Data Loss Due to Carelessness

Data loss refers to the unauthorized or accidental exposure of personal or confidential data that could lead to identity theft. As the infographic to the right illustrates (Prinzlau, 2017), the vast majority of data loss is preventable. As a reminder, faculty and staff who have a business need to access the personally identifiable information of students and employees must exercise diligent care to avoid unintentionally exposing that information to identity thieves. Here are some ways to practice diligent care:

- Never post student grades on bulletin boards, websites, or in other public places using Social Security Numbers or Student ID numbers;
- Do not store reports or data containing student or employee personally identifiable information on individual desktops, laptops, portable computing devices, or removable media; and
- Do not needlessly email files or data containing personally identifiable information, as this information can become a part of personal email archive files or inadvertently forwarded to unauthorized individuals.



Think Before You Click

TTU students, faculty, and staff have recently received email scams with subject lines such as “Account Shutdown,” “Important Message,” or “Re-validate Your Mailbox.” These are three examples, but other scam emails with different subjects have been reported as well. Please do not respond to these phishing emails.

These emails are designed to trick you into giving away your eRaider username and password to computer hackers on the Internet. Remember—no one at Texas Tech University will ever ask you for your eRaider password.

- If you have responded to one of these emails and provided your eRaider username and password, please change your password immediately by going to eraider.ttu.edu, and contact IT Help Central at (806) 742-4357 (HELP) for additional assistance.
- If you have received one of these or similar emails in your Inbox and have not responded, you may simply delete the email - no further action is needed. Thank you for protecting TTU data and information resources!

As a reminder, the TTU IT Division recommends the following cybersecurity practices to protect yourself and TTU resources from this and other 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 suspicious or suspect emails;
- Update your desktop, laptop, and/or mobile device anti-virus software; and
- Keep current on critical system updates:
  - Windows Users: https://www.askit.ttu.edu/windowsupdate
  - Mac Users: https://www.askit.ttu.edu/macupdate

We encourage you to be vigilant in practicing cybersecurity. You can find additional cybersecurity tips online at http://www.cybersecurity.ttu.edu. For more information or questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

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, that can be reviewed online at http://www.infotech.ttu.edu/security/docs/incident_management.php. Faculty, staff, and students must file a report prior to any attempt to remediate, solve, or troubleshoot the incident.

A wide variety of data security incidents must be reported including: virus, worm, and other 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 things that you should do:

1. Immediately report the incident:
   - For virus, worm, and other malware infections, compromised systems, or improper use complaints, contact the IT Security Team at security@ttu.edu or (806) 742-0840; or
   - For potential criminal acts (data theft, fraud, etc.), the exposure of confidential information, or a threat to personal or homeland security, directly contact either 1) the TTU Information Security Officer, Jeff Barrington at (806) 742-5151 or Jeff.Barrington@ttu.edu, or 2) TTU Chief Information Officer and Information Resources Manager, Sam Segran, at (806) 742-5151.
2. After the TTU IT Security Team has reviewed and provided guidance, work collaboratively to 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) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

Raider PC Mart | *Cyber Smart & Cyber Aware*

Raider PC Mart allows departments to electronically connect with other departments that may be interested in outgoing computing equipment. Raider PC Mart is an online equipment transfer application for used computer equipment and peripherals. It is designed to facilitate the transfer of used computing equipment between TTU departments before it is surplused with Property Surplus. These technology exchanges between TTU departments make institutional technology investments last longer, extending the use of computing equipment.

Raider PC Mart allows individuals authorized by the department head to post computer equipment no longer needed in their department, or to review equipment posted by other departments. While inventory transfer paperwork and procedures are required prior to the exchange, Raider PC Mart allows interested parties to discuss and negotiate equipment trades. As with any equipment transfer, all TTU Operating Policies and Procedures apply. Visit www.raiderpcmart.ttu.edu to view the relevant policies.

Please note that Raider PC Mart is a voluntary utility designed to foster communication and extend the life of TTU's IT equipment investment. The departments involved are responsible for the terms of the exchange. The system is designed only for the purposes of computing equipment exchange. We encourage you to dust off that unneeded computer or printer and list it on Raider PC Mart—recycle and extend instutional technology investments!

Mail | Mail Stop 2008
Phone | 742-5151
Fax | 742-5155

View IT Bulletins online at
infotech.ttu.edu/itbulletin

Need IT assistance?
IT Help Central
(806) 742-4357 (HELP)
ithelpcentral@ttu.edu

Computer-Based Training (CBT):
www.cbt.ttu.edu

TTU IT