Securing TTU Data through Laptop and Desktop Encryption

Message from the CIO

As the fall semester draws to a close and the holiday season is upon us, we provide information for protecting institutional data during this holiday period. We’re also providing a reminder about the discounted Dell and Apple bundles available for business and personal purchases by the Texas Tech community.

While this is a festive season for many, the next few weeks of the holiday season are prime time for Internet criminals. We encourage you to stay vigilant and protect business and YOUR personal information. For more cybersecurity tips, visit http://www.cybersecurity.ttu.edu. From our families to yours, Season’s Greetings– and a safe holiday season. Have a restful winter break. Go Tech!

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

Encryption is one important way to protect TTU information resources and to comply with federal and state laws, and with relevant TTU Operating Policies. Encryption is the process of encoding your personal or business sensitive information so that only authorized parties can read it. You should use encryption to keep information in files and folders private on hard drives. The TTU Office of the CIO provides encryption tools to aid you in protecting personal and institutional information. Researchers may also have data that requires additional protection, such as encryption.

Throughout the pandemic, the number of cybersecurity attacks on institutions of higher education has continued to intensify. Some of these threats include malware, ransomware, phishing, data breaches, and identity theft, including eRaider account compromises. TTU employees are increasingly targeted by cybercriminals and must be vigilant in protecting personal and institutional information. Researchers may also have data that requires additional protection, such as encryption.

Encryption is one important way to protect TTU information resources and to comply with federal and state laws, and with relevant TTU Operating Policies. Encryption is the process of encoding your personal or business sensitive information so that only authorized parties can read it. You should use encryption to keep information in files and folders private on hard drives. The TTU Office of the CIO provides encryption tools to aid you in protecting personal and institutional information. Researchers may also have data that requires additional protection, such as encryption.

Please note, in the event that a problem occurs such as hard drive failure, a backup will be the only mechanism to restore encrypted data. If you need assistance in establishing a backup plan, contact your department’s IT support staff or IT Help Central at (806) 742-4357 (HELP) or ithelpcentral@ttu.edu.

- Laptops managed centrally by the TTU IT Division (using KACE or Jamf) will automatically receive the encryption software through coordination with IT Help Central. For laptops not managed centrally by the TTU IT Division, IT Help Central will schedule a time with your department’s IT support staff to implement the encryption solutions.

- Laptops currently encrypted with native operating system encryption—BitLocker (Windows) or FileVault (macOS)—will be seamlessly managed with DDPE (Windows) or Jamf (macOS).

- Once a laptop begins the encryption process, minor interaction may be required (accepting prompts, restarting, etc.).

You may find additional information about encryption online at https://www.askit.ttu.edu/encryption. For any questions or concerns, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

Additional Information:
- Establish an on-going backup plan for your computer and data. We recommend the use of TTU-provided online storage such as OneDrive for Business or SharePoint Online, rather than storing data locally or on removable media.

Computer Discounts

Thanks to our partnership with Dell Computer Corporation and Apple Inc., you can do your holiday shopping anywhere, anytime! The TTU Information Technology (IT) Division has configured hardware bundles for Texas Tech University. The desktop and laptop bundles were created with input from the Texas Tech faculty, staff, and students. For departmental and personal purchases, please visit ithc.ttu.edu/recommend.
This holiday season, the TTU IT Division encourages you to be mindful while shopping online:

- Shop through reputable online stores. Be cautious of sellers in online marketplaces like Etsy, eBay, and Craigslist. Many of the sellers that post on these services are individuals, so your risk of online fraud or not getting the gift you purchased is much higher;
- Be sure that the URL displayed is the correct URL for your intended shopping site;
- Look for the lock icon on the browser’s status bar and make sure “https” appears in the address before completing your purchase. The “https” in the address indicates that the connection is secure, and your credit card information is encrypted. If you don’t see a lock icon or https://, then your connection is not secure, and your information could be at risk;
- Install, enable, and regularly update anti-malware/anti-virus software on your computers and devices. Symantec Endpoint Protection and Microsoft Defender for Endpoint are available for free on our cybersecurity page;
- Pay with a credit card instead of a debit card. With credit card transactions, you have a period of time before money is transferred to the seller, but debit transactions are immediately withdrawn from your account. You may also consider paying via a one-time use credit card or a gift card;
- Regularly update operating systems, application software, and mobile apps. Instructions for updating your operating systems may be found below:
  - Windows: https://askit.ttu.edu/windowsupdate
  - macOS: https://askit.ttu.edu/macupdate
  - iOS/iPadOS: https://askit.ttu.edu/iosupdate
  - Android: https://askit.ttu.edu/androidupdate
- Save emails regarding your online transactions, especially online receipts, and any electronic correspondence you have with the retailer or seller; and
- Review your credit card and bank statements as you receive them and immediately report unauthorized charges.

We encourage you to be vigilant in practicing cybersecurity and invite you to learn more cybersecurity tips online at http://www.cybersecurity.ttu.edu.

For more information or if you have questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

Happy Holidays
~and a~
Joyful New Year