TTU is amidst another spring semester full of activity. Our bulletin highlights requirements for acceptable and secure usage of TTU IT resources as we engage in institutional learning, teaching, research, and service activities. The pandemic has introduced new opportunities for internet criminals, and we have seen a rise in phishing email and malicious website activity. Please remain vigilant about recognizing scam emails and phishing attempts and keep TTU computing systems and devices updated with recent operating system versions and updated endpoint security software (Symantec, Defender, etc.). Additionally, we remind you to contact IT Help Central with questions before downloading software not provided by the university, as “free” software downloaded may not be “free” if used on institutional information resources. We have provided an article that describes the situation, and we need your partnership in adhering to these restrictions. The TTU IT Division plans to host another “IT Spring Cleaning Week” in May. Now is a good time to begin planning to rid your office of unneeded electronic and paper documents, and to protect your devices from the West Texas dust. We hope this bulletin finds you healthy and safe – Go Tech!

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

**Message from the CIO**

Most software require acceptance of an End User License Agreement (EULA) at the time of installation. Per Operating Policy and Procedure 72.02 and Regents’ Rules Chapter 07.12, TTU employees and students, as well as departments and units, do not have authority to sign or accept a EULA on behalf of Texas Tech University. Many “Personal,” “Free,” “Consumer,” and “Trial” software packages forbid installation on organization-owned systems, including those owned by Texas Tech University, without a legitimately acquired software license. Software license purchases and all related contract documents are approved and authorized by Procurement Services and the TTU Office of the CIO. In some cases, software packages are licensed at the Texas Tech University System level (i.e., Oracle, Ellucian) for software shared among Texas Tech institutions; other software packages are licensed at the institutional (TTU) level (i.e., Office 365, Adobe, Symantec), and some software packages may have been licensed by a department for a few systems or users.

Any software package, installed on a University-owned device, that is not properly licensed through the System, University or your department is a violation of copyright laws and TTU policies, and must be removed immediately. For example, Malwarebytes, an anti-malware software package, and Oracle VirtualBox, a tool used for virtual system creation and management, offer free consumer versions downloaded from their websites, and, per their EULA, are not authorized on any institutional systems, TTU-owned systems in our case. In compliance with vendor licensing requirements, please immediately uninstall any Malwarebytes or Oracle VirtualBox licenses from TTU-owned systems, unless your area/department has purchased an appropriate license. Additionally, we ask that you review software installed on institutionally-owned systems in your area/department, and ensure that all software is properly licensed, typically through a TTU software site license, or an area/department purchase.

Instead of Malwarebytes, please install the newest version of Symantec Endpoint Protection software (Version 14.3) for both Windows and macOS, available at no cost at www.eraider.ttu.edu. If you have a need to manage institutional virtual servers, please contact the University Data Center for solutions licensed for TTU (serversupport@ttu.edu). For other questions regarding software licensed for campus use, please contact TTU IT Technology Support Licensing (itts.licensing@ttu.edu).

For additional information, you may also contact IT Help Central at (806) 742-4357 (HELP) or ithelpcentral@ttu.edu. If you have questions about the procurement and contract process for any license, please contact purchasing@ttu.edu.

**Removal of Unauthorized Software on University-Owned Devices**

**Reminder: Microsoft Ending Office 365 Support for Internet Explorer and Edge Legacy**

Microsoft announced in late 2020 they would begin phasing out Office 365 support for Internet Explorer and older versions of Microsoft Edge. To avoid problems connecting to Office 365 sites and applications such as Microsoft Outlook and Teams on the web, we strongly recommend that users of these older Microsoft web browsers upgrade to the latest version of Microsoft Edge or use the latest version of Chrome or Firefox.

If you have any questions or need assistance, please contact your department’s local IT support staff or IT Help Central at (806) 742-4357 (HELP) or ithelpcentral@ttu.edu.
IT Alert: Beware of Recent Email, Phone, and Text Scams

Cyber criminals are always looking for new ways to steal your identity or scam you into sending them money. In the last year, scammers have begun impersonating Texas Tech employees, either through emails, phone calls, or text messages. They may even contact a vendor, purporting to be someone at Texas Tech, in the hopes of obtaining funds. Responding to these scams can result in the loss of sensitive information, such as financial account data, credit card information, personal data, and passwords. We remind all faculty, staff, and students to stay vigilant and protect themselves, Texas Tech data, and institutional information resources.

Impersonation messages typically have the following things in common:

- **Scare tactics.** Aggressive and sophisticated scam artists try to scare people into providing confidential information or money. Many phone scams use threats in an effort to intimidate the user and may also leave “urgent” callback requests, sometimes through automated email lists or phone calls (“robo-calls”);
- **Requests for immediate action or information.** These callers frequently try to create a sense of urgency, and often request personal information (such as birth date, SSN, mother’s maiden name, etc.) under the guise of “verifying the caller’s identity.” They may also ask for money, gift cards, credit card numbers, or money transfers (e.g., Western Union);
- **Impersonation and Caller ID spoofing.** Scammers often alter caller ID to make it look like a particular organization or an official agency is calling. The callers may use official titles and fake premises to appear legitimate. They may use online resources to get the user’s name, address, and other details about his or her life to make the call sound legitimate; and
- **Phishing emails and postal mail.** Scammers copy and use official letterhead in email or postal mail they send to victims in an attempt to make the scam look official.

We encourage you to practice cybersecurity and to be aware of these activities designed to steal institutional and personal resources. You may find more cybersecurity tips online at [http://www.cybersecurity.ttu.edu](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.

Adobe Sign is Now Available to TTU Faculty and Staff

The TTU IT Division, in partnership with Adobe, is providing an e-Signature solution for the TTU campus. Adobe Sign is a powerful and secure tool for electronic document processing. Some of the robust features include:

- Document and project management features, such as fillable PDF’s and e-signatures;
- Launch automated document signing workflows, ranging from simple (a few signers) to complex (over a thousand signers);
- Robust automated recordkeeping;
- Fully functional mobile app; and
- Complete document tracking, including email reminders and signature management.

Notes about our TTU Enterprise license:

- Includes licenses for all TTU faculty and staff;
- License required only for employees that initiate documents to be signed;
- Document recipients can sign the documents from anywhere using the email-based Adobe Sign tool (anyone can sign a document sent to them without acquiring an Adobe Sign license); and

If you have any questions or need additional information about this application, or regarding software licensed for campus use, please contact TTU IT Technology Support Licensing at [itts.licensing@ttu.edu](mailto:itts.licensing@ttu.edu).