**Message from the CIO**

As we navigate through the rest of the academic year, our TTU IT bulletin highlights the acceptable use of TTU IT Resources policy. As a reminder, all software installed on TTU-owned systems must have legitimately acquired and approved software license(s). Current international climate create opportunities for Internet criminals to exploit, so please note that we are all responsible for staying alert and recognizing scam emails and phishing attempts. TTU systems must be kept updated with current versions of operating system, applications, and endpoint protection (Microsoft Defender). Carrying on our spring tradition, the TTU IT Division plans to host an “IT Spring Cleaning Week” in the next few weeks. Now is a good time to begin planning to rid your office environment of unnecessary clutter and properly dispose of all electronic and paper documents that are no longer needed, especially those that contain confidential or sensitive information, while still complying with TTU OP 10.10, Records Retention. Watch for further details in our next bulletin. Go Tech!

---

**Beware of Scams and Threats Related to the Russian Invasion of Ukraine**

Criminals often use these topics to lure people into opening a malicious attachment, clicking on a link, or copying and pasting a web address into their browser.

**Examples of common email scams:**

- **“Breaking News” stories** – Scams may appear to come from a reputable news source, directing recipients to a fake site for breaking news on a specific situation.

- **Requests to respond/register for a “political” issue or cause** – Many Internet criminals leverage political topics of the day to elicit an emotional response, such as a war in the global theatre, domestic issues, or special interest legislation.

- **Requests for donations to individuals in “dire” circumstances or 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.

**Specific Recommendations:**

- If you receive one of these messages, delete it and do not respond to it.

- If you do respond, either by replying, clicking on a link, or visiting the website, your eRaider account will be disabled to protect the TTU community and institutional accounts and data.

- If you are uncertain of the legitimacy of a message, please contact IT Help Central for further assistance.

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

---

**Appropriate Use of Software on University Systems**

Most software requires acceptance of an End User License Agreement (EULA) at the time of installation. Per Operating Policy and Procedure 72.009(2.b) and Regents’ Rules Chapter 07.12, employees and students, as well as departments and units, do not have authority to sign a EULA or any agreement on behalf of Texas Tech. Software license procurements and all related contract documents are reviewed by the TTU Office of the CIO, Procurement Services, and the Office of General Counsel and are approved and signed through the Office of Procurement Services.

Many “Personal,” “Free,” “Consumer,” and “Trial” type of software packages forbid installation on organization-owned systems, including on systems owned by Texas Tech, without legitimately acquired and approved software license(s). In some cases, software packages are licensed at the Texas Tech University System level (i.e., Oracle, Ellucian) for software shared among Texas Tech System component institutions; other software packages are licensed at the institutional (TTU) level (i.e., Microsoft 365, Blackboard, Adobe), and some software packages may be licensed by a department for a few systems or users.

TTU has been contacted in the last few years by several software vendors requesting an audit of appropriate use and licensing of their software on Texas Tech systems. Any software package, installed on a Texas Tech 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. Additionally, we ask that you review software installed on institutionally owned systems in your area/department and ensure that all software is properly licensed.

A list of centrally licensed software available for institutional use is located at https://www.depts.ttu.edu/itts/software/. For 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, please contact contracting@ttu.edu.
As a State of Texas Public University, Texas Tech University may only enter into or renew contracts that involve cloud computing services in any capacity (as defined by Texas Government Code §2157.007) with vendors that are listed on DIR’s TX-RAMP list. If you have an existing or pending procurement for cloud computing services, please share this information with your vendor contact as soon as possible. Also, please allow extra time for contract reviews and for the vendor to apply to be listed on DIR's TX-RAMP certified vendor list. If you have any questions, please contact TX-RAMP@ttu.edu.

We encourage you to be vigilant in practicing cybersecurity. You can find additional cybersecurity tips online 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.

Be Aware: Tax Season Is Here (And So Are the Scammers)

Historically, Internet criminals leverage tax season to launch various campaigns to steal money, confidential data, and information resources. The Internal Revenue Service also warns of tax scams aimed at stealing Electronic Filing Identification Numbers (EFIN). Stealing these EFINs will allow scammers to file fraudulent tax returns for refunds.

Warning signs that a purported IRS communication is fraudulent:
- Requests personal and/or financial information such as name, Social Security number, bank/credit card account numbers;
- Requests security-related information, such as password, PIN, or mother’s maiden name;
- Offers a special tax refund program available by email;
- Invites you to participate in an IRS survey and receive a stipend or discount on taxes owed;
- Threatens a consequence - additional taxes or frozen tax refunds - for not responding to the email;
- Misspells “Internal Revenue Service” in the email text or website link supplied; and/or
- References an IRS link that does not contain https://www.irs.gov - to see the actual link address, place your mouse pointer over the link text without clicking.

The Texas Tech University Office of the CIO wants you to be aware of scams that use the IRS name, logo, or website, and request confidential information from you. Remember that the IRS does not collect tax information by email, voicemail, or SMS. The Federal Trade Commission recommends filing your tax returns early to help prevent fraudulent filings.

The TTU IT Division recommends the following cybersecurity practices to protect yourself and TTU resources from these and other scams:
- Do not click on links contained within an email unless you are certain of the sender’s identity and are expecting the information;
- Do not open attachments unless you are certain of the sender’s identity and are expecting the information;
- Delete and do not reply to any suspicious or suspect emails;
- Update endpoint protection on all of your devices; and
- Keep current on critical system updates:
  - Windows: https://www.askit.ttu.edu/windowsupdate
  - macOS: https://www.askit.ttu.edu/macupdate
  - iOS and iPadOS: https://www.askit.ttu.edu/iosapupdate
  - Android: https://www.askit.ttu.edu/androidupdate

We encourage you to be vigilant in practicing cybersecurity. You can find additional cybersecurity tips online 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.

Reminder: Acceptable Use Policy

As you take advantage of the many information resources provided by Texas Tech University, please remember that use of these resources must adhere to TTU Operating Policies and Procedures, including the IT Acceptable Use Policy. Based on Texas Administrative Code (TAC), the Acceptable Use Policy defines your personal responsibilities when using TTU information resources. Examples of institutional information resources include, but are not limited to, mobile devices, electronic files, data, computer hardware and software, peripherals, networks, etc. Acceptable Use Policy highlights:
- The TTU policy applies to all TTU students, faculty, staff, and others granted access to any University information resources, regardless of location or method of access;
- Information resources must be used in a manner consistent with the mission and objectives of TTU and the State of Texas;
- TTU students, faculty, and staff must only use information resources they have been granted access to and no one may attempt to circumvent IT security measures;
- Information on safe computing practices is available for the campus community at cybersecurity.ttu.edu. Please report any potential or actual IT security violations or weaknesses immediately to the TTU Chief Information Security Officer at (806) 742-0840, security@ttu.edu;
- Be respectful, courteous, and ethical in the use of information resources;
- Account owners are personally responsible for all uses associated with their account. Do not share information resources login information (e.g., eRaider password);
- Incidental personal use is restricted to authorized users within certain guidelines (outlined in the Acceptable Use Policy);
- TTU information resources must not be used for personal or commercial gain or for political activity; and
- All use of information resources is governed by local policies and applicable state and federal law.

We invite you to review the complete list of TTU IT Security Policies at infotech.ttu.edu/security. In all things at Texas Tech University, integrity is a hallmark of our commitment to excellence.