TechMail, powered by Microsoft Office 365, is your official institutional email service – the required platform for TTU business, education, and research communications. While TechMail can be accessed using Microsoft Outlook and most basic email clients, many of these clients were not designed to be used in the Office 365 environment at Texas Tech, and as a result, you may not be able to utilize all of the features that TechMail has to offer. Because of this, we strongly recommend the following email client options: Office 365, Microsoft Outlook for Windows or Mac, Outlook on the Web (https://office.com), Outlook mobile apps, or built-in, native email clients (that utilize ActiveSync) on mobile devices.

If you decide to use non-supported software to access your TechMail account, please be aware that:

- Most third-party clients connect to your mailbox only. They typically will not connect to your calendar, contacts, tasks, etc.; integration with other TTU resources (Global Address List, Skype for Business Meeting, Skype for Business, etc.) from these clients will be limited; and older email clients may not be updated on a regular basis, increasing the risk of attackers accessing your TechMail account. As Office 365 features and security are updated, legacy clients may be unable to connect.

For additional technical support information, please visit: https://askit.ttu.edu/email.

What Happened? Why you did not receive an email

Office 365 servers process a large volume of email every day. Occasionally, you may not receive an email in your inbox that you were expecting or that someone indicated they sent to you. The most common explanations are:

- The message was identified as spam by your email software;
- The message has been “scored” as spam by Office 365;
- Malware was attached to the message and was detected by antivirus software – many times the sender may not be aware of the infected file;
- The email had a “spoofed” TechMail address (sender address contained in the mail message does not match the actual sender address – commonly used in phishing schemes);
- The message was routed to a subfolder due to an inbox rule;
- The sender made a typo in your email address;
- The message was accidently deleted and moved to the Deleted Items folder;
- The message came from a mail domain that has been blacklisted for generating huge volumes of spam email; and/or
- A technical problem occurred between the originating server and Office 365 email servers, preventing delivery.

One of the biggest culprits of lost email is the practice of “spoofing” email addresses. Internet criminals have exploited an Internet mail feature that allows a sender to specify any email address in the email’s “From” line, allowing them to create fictitious or forged email addresses. Spoofing occurs when an email sender specifies an email address in the “From” line of the email that is different from his/her actual email address. Spoofing is generally used to conduct illegal activity and hide their origination address and identity.
Phishing Facts

Cyber criminals continue to change their phishing tactics to adapt to more sophisticated email protection methods. Regretfully, some in the TTU Community continue to fall prey and click on malicious links, and divulge their eRaider credentials and place institutional data and information resources at risk. In order to provide additional protection for faculty, staff, and student accounts, as well as institutional data and information resources, the TTU IT Division enables Microsoft Defender for Office 365 for all incoming mail messages.

Microsoft Defender for Office 365 checks links and attachments contained in all incoming email to determine if they are malicious. Additional information about Microsoft Defender for Office 365:

- The system is fully automated. No action is needed on your part; and
- As part of protecting users from malicious websites, links will appear slightly different: Links will be prepended with text like "https://nam01.safelinks.protection.outlook.com/?url= when you hold your mouse pointer over them. This will not affect links ending in ttu.edu.

When you click a link, the URL will be checked against a known list of malicious sites. If the site is known to be malicious (i.e. the link could be asking you to provide login credentials), you will be notified by one of the following messages:

- If known to be malicious by Microsoft Defender for Office 365, the message will read “This website has been classified as malicious.”
- If known to be malicious by TTU, the message will read “This website has been blocked per your organization’s URL policy.”

Otherwise, you will continue to the original site. This scan is almost instantaneous, and you may not notice.

Microsoft Defender for Office 365 will also scan all email attachments and remove those that are determined to be malicious. Messages containing large attachments may be delayed slightly, typically less than one minute.

Thank you for your partnership as we work to further secure our community and our data and information resources.

You may find additional information about Microsoft Defender for Office 365 online at https://askit.ttu.edu/atp. If you have questions or need additional information, please contact IT Help Central at (806) 742-4357 (HELP) or via email at.

Tips for Email Security

Email security is most effective when every user takes an active role in protecting personal and business accounts. Many times, our own actions can create vulnerabilities that allow hackers, viruses, and phishing scams to be successful.

Some simple, yet painless, tips for safeguarding email accounts are:

- Use strong, complex passphrases and never share them;
- Double-check every sender’s email address to detect impersonation attempts;
- If compromised, change your password immediately;
- Do not open emails or attachments from anyone you do not know;
- Do not click on a link or an “Unsubscribe” button within the email. Take the time to go to the official website and complete the action there;
- Never send personal information via email;
- Keep your anti-virus software up-to-date;
- Avoid public Wi-Fi; and
- Do not forget to log out.

Understanding Your Privacy When Using TTU Information Resources

Privacy policies are mechanisms used to establish the limits and expectations for users of Texas Tech University information resources. Faculty, staff, students, and others authorized to access TTU data and information resources should have no expectation of privacy with respect to these resources. Texas Tech University is a State of Texas agency, and as such, we are all stewards of public resources. The purpose of the Texas Tech University Information Technology Privacy Policy is to clearly communicate our information technology privacy expectations to the TTU Community and is based on state regulatory requirements.

Please note that electronic files created, sent, received, or stored on TTU resources are not private and may be accessed as deemed appropriate and necessary by the Chief Information Officer or other TTU executive leadership. In addition, Texas Administrative Code 202 authorizes the logging and reviewing of information created, stored, transmitted, and viewed using TTU information resources.
Scammers are perfecting their emails, which makes them much more difficult to spot and can result in the loss of sensitive information such as financial account data, credit card information, personal data, and passwords. The TTU Office of the CIO reminds all faculty, staff, and students to stay vigilant and protect themselves, TTU data, and institutional information resources.

Common tactics that scammers use:

- **Scare tactics.** These aggressive and sophisticated scams 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 call recipient’s identity.” They may also ask for money, gift cards, credit card numbers, or money transfers such as Western Union;
- **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 regular mail.** Scammers copy and use official letterhead in email or regular mail they send to victims in an attempt to make the scam look official.

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

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

---

**Beware of Threats to Our Confidential Data**

Historically, Internet criminals leverage current events - tax season, elections, pandemics - to launch various campaigns to steal money, confidential data, and information resources. The TTU IT Division strongly recommends that faculty, staff, and students be vigilant in protecting institutional and personal data and information resources.

The TTU IT Division has the following measures in place to protect confidential and sensitive data:

- **2-Factor Authentication on Selected Critical Services** prevents unauthorized account access by sending a code to the account owner when their account is accessed from a new location; **Note:** 2-Factor Authentication is currently enabled on Texas Tech’s Direct Deposit, eRaider Account Manager, Banner 9 Admin, and W-2 Wage and Tax Statement pages. You can enable this feature for all eRaider-authenticated pages by following the instructions at [https://askit.ttu.edu/2fa](https://askit.ttu.edu/2fa);
- **Symantec Endpoint Protection** is capable of detecting and removing most keylogger software and malware. You may download this software at no cost by visiting [https://eraider.ttu.edu](https://eraider.ttu.edu), clicking on “Manage Your Account,” and choosing “Software Download” in the left-hand menu; and
- **Microsoft Defender for Office 365** checks links and attachments contained in all incoming email to determine if they are malicious.

As a reminder, the TTU IT Division recommends the following cybersecurity practices to protect yourself and TTU resources from 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:** [https://askit.ttu.edu/windowsupdate](https://askit.ttu.edu/windowsupdate)
  - **macOS:** [https://askit.ttu.edu/macupdate](https://askit.ttu.edu/macupdate)
  - **iOS/iPadOS:** [https://askit.ttu.edu/iosupdate](https://askit.ttu.edu/iosupdate)
  - **Android:** [https://askit.ttu.edu/androidupdate](https://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](http://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.
Email Management: Be Prudent with University Resources

Regular email account management helps to optimize TTU data storage resources. Taking a few minutes to sort through your email inbox, folders, and archives will help you stay organized and conserve data storage resources. We encourage you to schedule recurring times on your calendar to sort through your files.

We recommend the following practices when sorting and cleaning your email files:

- Establish a system to organize the emails you receive;
- Delete old/unwanted emails that you are not required to retain;
- Empty the Deleted Items and Junk Email folders regularly.
  - **Note:** TTU’s O365 mailboxes automatically delete items in these two folders after 15 and 30 days, respectively;
- If space is a consideration, archive less important messages that you need to retain.

For detailed instructions on email settings, please contact IT Help Central at (806) 742-4357 (HELP) or ithelpcentral@ttu.edu, or visit "Overview of the Techmail service at TTU" at https://askit.ttu.edu/techmail.

Confidentiality Notice Disclaimers for Email

While TTU recognizes the convenience and efficiency of email correspondence, we must also protect institutional data in transit and at rest on desktops, laptops, and mobile devices. The best practice is to avoid including any confidential information in an email message, unless absolutely necessary, even in a message to another TTU employee or student. For more information, please review the TTU IT Security Policies at http://infotech.ttu.edu/security/, which are referenced through TTU OP 52.04, Information Technology (IT) Security.

Additionally, to preserve the confidentiality of certain TTU data, the TTU Office of the CIO recommends that emails containing important TTU information should include the following disclaimer at the end of the correspondence:

```
“Confidentiality Notice: The information contained in this message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure, distribution, or retention is strictly prohibited. If you are not the intended recipient, or otherwise believe that you have received this message in error, please notify the sender immediately by reply email and delete the original message.”
```

The TTU Office of the CIO created the above disclaimer with assistance from the Office of General Counsel.

Keep in mind that simply adding the confidentiality notice in the email does not absolve you of the responsibility of contacting the unintended recipient and asking them to delete the email.

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 faculty, staff, students, 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 faculty, staff, and students 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 http://cybersecurity.ttu.edu;
- Be respectful, courteous, and ethical in the use of information resources;
- Do not share information resources login information (e.g., eRaider password). Account owners are personally responsible for all uses associated with their account;
- 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 http://infotech.ttu.edu/security. In all things at Texas Tech University, integrity matters!