Since 2004 when the National Cybersecurity Alliance designated October as “National Cybersecurity Awareness Month,” Texas Tech University has participated every year to help raise awareness about the importance of cybersecurity. We remain committed to maintaining a secure, reliable, and sophisticated information technology infrastructure, and continuously address the cybersecurity challenges that we face in higher education. In this issue, we provide relevant and timely news on protecting yourself from online fraud. Humanitarian issues in Ukraine and severe weather in the US create opportunities for Internet criminals to exploit, so please note we count on the TTU Community to stay alert and recognize scam emails and phishing attempts. Also included in this issue, you will find information and best practices for protecting institutional and personal information resources and data. Your vigilance and practice of safe computing is a critical component of our institutional data and information security strategies; we are all responsible for exercising due diligence in protecting confidential and sensitive TTU data and information resources. Go Tech!

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

The FBI’s Internet Crime Complaint Center has released its annual report. The 2021 Internet Crime Report (pdf) includes information from 847,376 complaints of suspected internet crime—a 7% increase from 2020—and reported losses exceeding $6.9 billion. State-specific statistics have also been released and can be found within the 2021 Internet Crime Report and in the accompanying 2021 State Reports.

The top three cybercrimes reported by victims in 2021 were phishing scams, non-payment/non-delivery scams, and personal data breach. Victims lost the most money to business email compromise scams, investment fraud, and romance and confidence schemes.

In addition to statistics, the IC3’s 2021 Internet Crime Report contains information about the most prevalent internet scams affecting the public and offers guidance for prevention and protection. It also highlights the FBI’s work combating internet crime, including recent case examples. Finally, the 2021 Internet Crime Report explains the IC3, its mission, and functions.

The IC3 gives the public a reliable and convenient mechanism to report suspected internet crime to the FBI. The FBI analyzes and shares information from submitted complaints for investigative and intelligence purposes, for law enforcement, and for public awareness.

With the release of the 2021 Internet Crime Report, the FBI wants to remind the public to immediately report suspected criminal internet activity to the IC3 at ic3.gov. By reporting internet crime, victims are not only alerting law enforcement to the activity but aiding in the overall fight against cybercrime.

To report an online crime or view IC3’s annual reports and public service announcements, visit ic3.gov.

Resources:
2021 Internet Crime Report (pdf)
2021 State Reports (pdf)
More IC3 annual reports
IT Security and Network Connectivity

Although convenient, public wireless connections are typically not secure. Your home or personal Wi-Fi system may also present security risks. TTUnet Wi-Fi service on campus is secured using industry standard and proven security practices. However, most public Wi-Fi available in retail stores, hotels, airports, and conferences are configured for convenience rather than security.

- Public Wi-Fi precautions:
  - Avoid using public hot spots for important transactions, such as transactions that require a login. You should not make financial transactions or use credit cards over public Wi-Fi.
  - If you are logged into a website or a program, be sure to log out when you are finished.

- Home Wi-Fi precautions:
  - Change the default password when setting up your home Wi-Fi.
  - Enable your Wi-Fi router's strongest security features, such as WPA2.
  - Disable remote administration (a feature on newer Wi-Fi routers that allows administration of the router from the Internet).
  - Make sure your home Wi-Fi access is password protected because “drive-by hackers” or your neighbors could gain access to your wireless network, steal your personal information, or participate in illegal online activities that could trace back to you.

- Be selective about providing home Wi-Fi access to guests.
- Create and use strong, unique passwords for all accounts.
- Install anti-malware/anti-virus software on your computers and devices.
- Update operating systems, anti-malware/anti-virus software, application software, and mobile apps:
  - Windows: [https://www.askit.ttu.edu/windowsupdate](https://www.askit.ttu.edu/windowsupdate)
  - macOS: [https://www.askit.ttu.edu/macupdate](https://www.askit.ttu.edu/macupdate)
  - iOS: [https://www.askit.ttu.edu/iosupdate](https://www.askit.ttu.edu/iosupdate)
  - Android: [https://www.askit.ttu.edu/androidupdate](https://www.askit.ttu.edu/androidupdate)
- Use screen locks and passcodes on your devices.
- Back-up your content.
- Additional Information:
  - IT Operating Policies: [https://www.depts.ttu.edu/infotech/policies.php](https://www.depts.ttu.edu/infotech/policies.php)
  - IT Security Policies: [https://www.depts.ttu.edu/infotech/security/](https://www.depts.ttu.edu/infotech/security/)
  - Cybersecurity Awareness Program: [http://www.ttu.edu/cybersecurity/](http://www.ttu.edu/cybersecurity/)
  - TTU Software Download: [www.eraider.ttu.edu](http://www.eraider.ttu.edu)

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

The Texas Department of Information Resources Security Office has advised state agencies and higher education institutions to be on heightened alert for cyber-attacks from nation-states and Internet-based special interest groups (hacktivists). The TTU IT Division advises students, faculty, and staff to be vigilant for malicious cyber activity seeking to capitalize on the Russia-Ukraine war. Historically, any international conflict, natural disaster, or media event has resulted in an increase in email scams and other cyber threats.

**Examples of common email scams:**

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

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.

**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 a message’s legitimacy, 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 [https://www.cisa.gov/shields-up](https://www.cisa.gov/shields-up). You can find additional tips online at [http://cybersecurity.ttu.edu](http://cybersecurity.ttu.edu). For more information or questions, please contact IT Help Central at (806) 742-4357 (HELP) or [ithelpcentral@ttu.edu](mailto:ithelpcentral@ttu.edu).
With Internet criminal activity continuing to rise, 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: Prevents unauthorized account access by sending a code to the account owner when their account is accessed.
  
  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 askit.ttu.edu/2fa.

- Microsoft Advanced Threat Protection: Checks links and attachments contained in all incoming email to determine if they are malicious.

Microsoft Advanced Threat Protection (ATP) Details:

In an effort to protect users from malicious websites, links will appear slightly different:

- Links will be prepended with "https://na01.safelinks.protection.outlook.com/?url=" when you hold your mouse pointer over them.

- 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 ATP, 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.

- ATP 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.

Recommended Cybersecurity Practices:

As a reminder, the TTU IT Division recommends the following cybersecurity practices to protect yourself and TTU information resources and data:

- Do not click on links contained within an email or SMS, 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.

- Keep current on critical system updates:

  Windows: https://www.askit.ttu.edu/windowsupdate

  macOS: https://www.askit.ttu.edu/macupdate

  iOS: https://www.askit.ttu.edu/iosupdate

  Android: https://www.askit.ttu.edu/androidupdate

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

- Enroll with a credit monitoring service.

- 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 identitytheft.gov.

- Consider registering for fraud alerts with all credit bureaus (Equifax, Innovis, Experian, and TransUnion).

- 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 annualcreditreport.com.

We encourage you to be vigilant in practicing cybersecurity. You can find additional cybersecurity tips online at 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.
Natural disasters and severe weather can create opportunities for fraud in their wake, occurring at a time when people may be especially vulnerable, or targeting charitable intentions.

Scammers use phone, text, mail, email, and even go door-to-door to target residents of affected areas following hurricanes and damaging storms.

Watch Out for Red Flags

First, know that officials with government disaster assistance agencies do not call or text asking for financial account information, and that there is no fee required to apply for or get disaster assistance from FEMA or the Small Business Administration. Anyone claiming to be a federal official who asks for money is an imposter.

Remember that phone scams often use spoofing techniques to deliberately falsify the information transmitted to your caller ID display to disguise their identity or make the call appear to be official.

If someone calling to be a government official, hang up and call the number listed on that government agency’s official website. Never reveal any personal information unless you’ve confirmed you’re dealing with a legitimate official. Workers and agents who knock on doors of residences are required to carry official identification and show it upon request, and they may not ask for or accept money.

Steps for Avoiding Post-Disaster Insurance Scams

If you get a phone call about an insurance claim or policy, don’t give out any personal information or agree to any payment until you can independently verify that the call is legitimate. If the caller says they’re from your insurance company, hang up and contact your agent or the company directly using the number on your account statement. Policyholders with the National Flood Insurance Program (NFIP Direct) can call 1-800-638-6620.

Contractors and home improvement companies may also call claiming to be partners with your insurance provider. Never give policy numbers, coverage details, or other personal information out to companies with whom you have not entered into a contract. If your state requires licensing, verify that any contractor you are considering is licensed and carries adequate insurance. Many states have online databases you can check.

Disaster Relief Charity Scams

Consumers should also be aware of scammers posing as representatives of charities seeking donations for disaster relief. There are several steps you can take to protect yourself from this type of fraud:

- Donate to trusted, well-known charities. Beware of scammers who create fake charities during natural disasters. Always verify a charity’s legitimacy through its official website. If you have doubts, you can check with Better Business Bureau’s Wise Giving Alliance, Charity Navigator, Charity Watch, or GuideStar. You can also check with the National Association of State Charity Officials whether charities must be registered in your state and if the charity contacting you is on file with your state.
- Verify all phone numbers for charities. If you need to contact a charity by phone, check the charity’s official website to see if the number you have is legitimate. If you’re using text-to-donate, check with the charity to ensure the number is legitimate before donating.
- Do not open suspicious emails. If you receive a suspicious email requesting donations or other assistance, do not click on any links or open any attachments. Scammers regularly use email for phishing attacks and to spread malware.
- Verify information in social media posts. Double-check any solicitation for charitable donations before you give. Crowd-funding websites often host fake charities during natural disasters. Always verify a charity’s legitimacy through its official website. If you have doubts, you can check with State Charity Officials or following a natural disaster, please notify FEMA at 1-866-720-5721 or disaster@leo.gov.

To report suspected fraud, call the FEMA Disaster Fraud Hotline toll free at 1-866-720-5721. If you need to report other fraudulent activities during or following a natural disaster, please notify FEMA at 1-866-720-5721 or disaster@leo.gov.

You can also file a complaint with the FCC about phone scams, or with the FTC about fraud.

Consumer Help Center

FCC consumer guides provide tips on avoiding caller ID spoofing and robocalls that may help you avoid being scammed. To learn more about scams and how to avoid them, check out the FCC Scam Glossary or visit the FCC Consumer Help Center at fcc.gov/consumers.
Securing Online Meetings

We provide the information and guidelines below to assist TTU students, faculty, and staff in successfully participating in online meetings in Collaborate, Skype, Teams, and Zoom.

Best Practices for Scheduling Online Meetings and Courses

Many of the options/settings for the online meeting experience are established when the meeting is being scheduled. It is very important that these settings are correct.

- **Waiting Rooms:** When participants are known, trusted, and authenticated, waiting rooms are generally not necessary. However, they are recommended in public presentations when participants include representatives from outside entities, such as a guest lecture or a collaborative research meeting with other institutions. If a waiting room is being used, the meeting host should begin admitting participants a few minutes early and pay close attention to latecomers. Meetings that are in progress can also be locked to prevent additional attendees from joining or rejoining.

- **Recurring Meeting Invitations:** When calendar invitations are updated, always send the update to all participants so that everyone joins the same online meeting. It is also a good idea to periodically end a recurring series and begin a new series with all participants. For example, schedule monthly recurring meetings on an annual basis.

- **For those platforms that have a designated host, designate at least one additional co-host on every meeting who can admit participants, enable screen sharing, etc. This is particularly important in Zoom and Collaborate meetings. Ensure that the hosts are familiar with these features. For more information, please see the Additional Help and Support section below.**

- **While always joining meetings on time, consider starting online meetings a few minutes after the scheduled start time and ending meetings promptly a few minutes before the scheduled end time to allow participants to transition between back-to-back-to-back online meetings.**

Best Practices for Secure Online Meetings and Course Sessions

When meeting online, be sure to practice safe computing and avoid unwanted guests (Zoombombing). General tips for hosting secure online meetings:

- **Check for updates for your conferencing app at least once a month.** When possible, configure applications for automatic updates and install updates upon notice;

- **Do not publicly post meeting links to social media unless you intend to invite all those that can read your social media feed;**

- **Use unique meeting identifiers so that your meeting is only available to those with that code;**

- **Use a waiting room to manage participants joining prior to the host or rejoining after leaving the meeting;**

- **Manage disruptions and unexpected participants by locking meetings from late or returning participants after all expected participants have joined;**

- **Limit who can join meetings as a presenter; enable only specific individuals to help co-host the meeting;**

- **Disable file sharing, if not needed; and**

- **Mute participants who do not need to speak.**

Best Practices for Participating in Online Meetings and Courses

- **Sign into your conferencing app (Zoom, Teams, etc.) every week.**

- **Arrive to meetings early (especially in hybrid meetings in conference rooms and classrooms) in case there are technical difficulties.**

- **Remember to mute and unmute yourself, as appropriate.**

- **Ensure that you have a quality Internet connection.**

- **In general, most TTU resources, such as email, Blackboard Collaborate, Skype for Business, Microsoft Teams, and Zoom, do not need a large amount of bandwidth.**

- **Remember that other activities, such as streaming audio and video, may impact your meeting experience.**

- **When possible, use audio for online activities that do not require video. Note that most online meeting tools will automatically prioritize audio over video if sufficient bandwidth is unavailable.**

- **eLearning & Academic Partnerships offers a helpful video with great strategies for effective participation in online environments:**

  - **Treat your online course and work as if it were face-to-face;**

  - **Use a schedule;**

  - **Create a dedicated physical and virtual learning/working space; and**

  - **Just as you would in a traditional environment, focus your attention and communicate effectively.**

Additional Help and Support

- **We have compiled technical instructions for securing TTU’s supported platforms—Zoom, Skype for Business, Blackboard Collaborate, and Teams—at [https://askit.ttu.edu/onlinemeetings](https://askit.ttu.edu/onlinemeetings).**

- **For instructional assistance, eLearning & Academic Partnerships has created a resource for faculty; the resource includes guidance from the Teaching, Learning, & Professional Development Center - [https://www.depts.ttu.edu/elearning/blackboard/collaborate](https://www.depts.ttu.edu/elearning/blackboard/collaborate)**

- **For instructor-led trainings, Technology Support offers free ShortCourses. Visit [https://www.depts.ttu.edu/itts/training/shortcourses](https://www.depts.ttu.edu/itts/training/shortcourses) to sign up!**

- **Teams: [9 Tips for having the Best Online Meeting Experience](https://www.depts.ttu.edu/itts/training/shortcourses)**

- **Zoom: [Zoom Meetings Training - Reference Guide](https://www.depts.ttu.edu/itts/training/shortcourses)**

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.
According to Texas Government Code §2054 and TTU OP 52.04, Texas Tech University information resources and data are considered critical institutional resources and must be protected with an appropriate level of security. Mobile computing devices are generally less secure and inherently at risk for data loss. As such, they should not be used for the storage of sensitive or confidential data (See Mobile Computing Policy).

The TTU IT Division provides and supports several free online file storage solutions. In addition to being more secure than saving data locally on your device or on removable media, these systems are backed up regularly so that files can easily be restored if lost or accidentally deleted.

**Type of Data Storage Solution**

<table>
<thead>
<tr>
<th>Type of Data</th>
<th>Storage Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Institutional Data - Mission Critical*</td>
<td>TechShare (100 GB free to departments), SharePoint (via the web or through Microsoft Teams)</td>
</tr>
<tr>
<td>Institutional Data - Non-Mission Critical**</td>
<td>OneDrive for Business (FERPA Certified)</td>
</tr>
<tr>
<td>Personal Documents</td>
<td>OneDrive (consumer version)</td>
</tr>
</tbody>
</table>

* Mission critical information is any information or data that is critical to the academic, research, or administrative operation of TTU.

** Non-mission critical information is any information or data that is considered non-essential to the function(s) of TTU, a TTU business unit, or a TTU official research project.

### Additional Notes:

- SharePoint is ideal for files that many people may own or need to access. SharePoint is also conducive for collaboration.
- Microsoft Teams provides a popular, collaborative environment that includes SharePoint storage and rich Office 365 integration.
- TechShare is another resource for archiving large files or folders but does not afford easy collaboration.
- OneDrive for Business is best for storing files that you need to retain as the sole user. OneDrive does allow for live collaboration and sharing during the document editing process.
- Please review Texas Tech University Operating Policy 10.10, to make sure that file retention complies with the institutional retention schedule.

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

---

**Survey Tool Options for Researchers, Faculty, and Staff**

To assist the academic and research communities on campus, we continuously evaluate IT products and services in support of institutional strategic priorities. For the last several years, the TTU IT Division has worked collaboratively with the Institutional Review Board, Office of the Vice President for Research and Innovation, Colleges, and the Office of the Provost to identify suitable survey data collection tools for our campus.

We provide a brief outline of tools available to faculty and staff, below.

**SurveyMonkey**

TTU provides a SurveyMonkey enterprise license for faculty and staff. Please note that the enterprise license is available to faculty and staff at no cost and includes data protections and IT security features not available in the free platform or in other survey tools. We can assist you with migrating any materials needed. Visit [https://www.depts.ttu.edu/itts/software/surveymonkey.php](https://www.depts.ttu.edu/itts/software/surveymonkey.php) for more details.

**REDCap**

REDCap is a free, secure, web application for researchers, faculty, and staff at Texas Tech to build and manage online surveys and databases. While REDCap can be used to collect virtually any type of data in any environment, it is specifically geared to support online and offline data capture for research studies and operations. The REDCap Consortium, a vast support network of collaborators, is composed of thousands of active institutional partners in over one hundred countries who utilize and support their own individual REDCap systems. Visit [https://evaluate.ttu.edu/](https://evaluate.ttu.edu/) for more details. First time users may request access by contacting the ITTS Licensing Team.

**Qualtrics**

Qualtrics is a popular survey tool used by many organizations. Qualtrics may be used at TTU using departmental or other available funding. Note that State and TTU procurement processes will apply. Qualtrics supports campus users directly through email and web tools ([https://www.qualtrics.com/support/](https://www.qualtrics.com/support/)).

---

Copyright 2022 Texas Tech University

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

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