Information Technology Division Bulletin

vol. 18 no. 2 | October 2021

We Are All Responsible
Cybersecurity Awareness Month Special Edition

Message from the CIO

October is "Cybersecurity Awareness Month" and was launched in October 2004, by the National Cyber Security Alliance and the U.S. Department of Homeland Security (DHS) in an effort to raise awareness across the nation about the importance of cybersecurity. Texas Tech University has participated in "Cybersecurity Awareness Month" since inception as it highlights an important goal in the TTU IT Division's strategic plan. Our commitment to maintaining a secure, reliable, and sophisticated information technology infrastructure, and continuously addressing the cybersecurity challenges that we face in higher education, only succeeds when we are all vigilant and practice safe computing. In this issue, we provide relevant and timely news on COVID-19 scam statistics and protecting yourself from healthcare fraud, as well as education and best practices for protecting institutional and personal information resources and data. Your partnership is critical in protecting institutional information resources. Go Tech!

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

FBI Releases the Internet Crime Complaint Center 2020 Internet Crime Report

(FBI released the Internet Crime Complaint Center 2020 report on March 17, 2021; Article adapted from Security Magazine, March 18, 2021, and is reprinted in full accordance with the FBI information and public awareness policy, and with educational fair use, Security Magazine, 2021.)

The FBI's Internet Crime Complaint Center has released its annual report. The 2020 Internet Crime Report includes information from 791,790 complaints of suspected internet crime—an increase of more than 300,000 complaints from 2019—and reported losses exceeding $4.2 billion. State-specific statistics have also been released and can be found within the 2020 Internet Crime Report and in the accompanying 2020 State Reports.

The top three crimes reported by victims in 2020 were phishing scams, non-payment/non-delivery scams, and extortion. Victims lost the most money to business email compromise scams, romance and confidence schemes, and investment fraud. Notably, 2020 saw the emergence of scams exploiting the COVID-19 pandemic. The IC3 received over 28,500 complaints related to COVID-19, with fraudsters targeting both businesses and individuals.

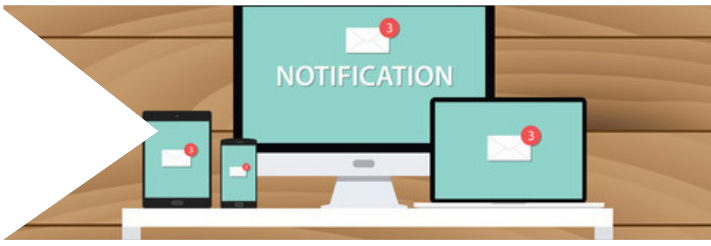
In addition to statistics, the IC3's 2020 Internet Crime Report contains information about the most prevalent internet scams affecting the public and offers guidance for prevention and protection. It also highlights the FBI's work combating internet crime, including recent case examples. Finally, the 2020 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 2020 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.

Resources:
2020 Internet Crime Report (pdf)
2020 State Reports (pdf)
More IC3 annual reports

External Email Notification



Cyber criminals continue to attack higher education institutions, often masquerading as TTU officials and sending email messages that appear to be sent from a TTU.EDU email address (spoofing). Responding to these scams can result in account compromise or the loss of sensitive information such as financial account data, credit card information, personal data, and passwords.

As an additional security measure to protect institutional data and information resources, a notification banner now automatically appears in any email message that originates from outside the university. The banner will be similar in appearance to the following text:

This email originated outside TTU. Exercise caution!

When receiving messages with this cautionary note, please validate the legitimacy of the sender and message before responding, clicking links, or opening attachments. Thank you for helping to protect our institutional information resources. If a message is not flagged accurately, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

Protecting Yourself from Healthcare Fraud

(FBI Tech Tuesday: Protecting Yourself from Healthcare Fraud, September 7, 2021), FBI Tech Tuesday: Protecting Yourself from Healthcare Fraud reprinted in full accordance with FBI informational and public awareness purpose policy, copyright FBI.

According to the FBI's Internet Crime Complaint Center (IC3), healthcare related fraud saw a 110% increase in victims nationally from 2019 to 2020, rising from 657 victims to 1,383. The reported losses saw an even more significant increase, rising from 1.1 million dollars in 2019 to 29 million dollars in 2020.

Healthcare fraud is a scheme that attempts to defraud private or government healthcare programs. Schemes may include offers for fake insurance cards, stolen health information, and various other scams involving medications, supplements, or diversion practices.

Healthcare fraud can be committed by medical providers, patients, and others who intentionally deceive the healthcare system to receive unlawful benefits or payments. These scams are often initiated through spam email, internet advertisements, links in forums/social media, and fraudulent websites.

The FBI suggests these tips to help protect yourself from healthcare related scams:

Protect your health insurance information. Don't share your personal or health information with anyone other than known and trusted medical professionals.

Beware of "free" services. If you're asked to provide your health insurance information for a "free" service, it's most likely not free and could be fraudulently charged to your insurance company.

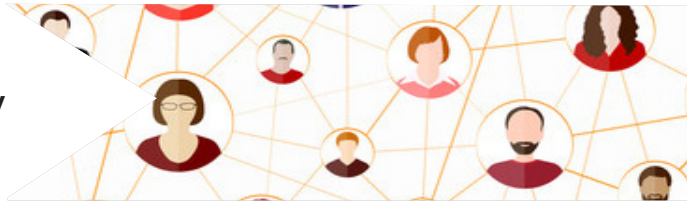
Check your explanation of benefits (EOB) regularly. Make sure the dates, locations, and services billed match what you actually received. If there is a concern, contact your health insurance provider.

If you believe you have been the victim of a healthcare related scam, please contact FBI Phoenix at (623)466-1999. Victims are also highly encouraged to file a complaint with the FBI at ic3.gov.

For more information on healthcare fraud, visit:
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/health-care-fraud

For information on healthcare fraud in relation to COVID 19, visit:
https://www.fbi.gov/coronavirus.

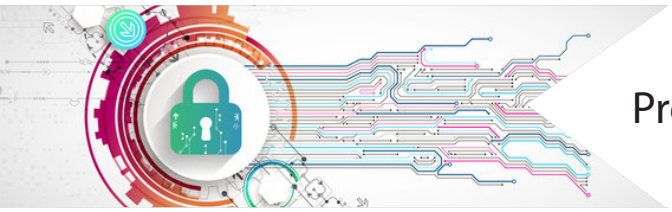
IT Security and Network Connectivity



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; Symantec Endpoint Protection is free for home use – just download from https://eraider.ttu.edu by selecting "Manage Your Account" – "Software Download".
- Update operating systems, anti-malware/anti-virus software, application software, and mobile apps:

  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
- 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
  - IT Security Policies: https://www.depts.ttu.edu/infotech/security/
  - Cybersecurity Awareness Program: http://www.ttu.edu/cybersecurity/
  - TTU Software Download: www.eraider.ttu.edu
  - Symantec: www.askit.ttu.edu/symantec by selecting "Manage Your Account" – "Software Download"



Protecting Personal and Institutional Data

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.

- Symantec Endpoint Protection: Capable of detecting and removing most keylogger software and malware. You may download Symantec at no cost by visiting eraider.ttu.edu, selecting "Manage Your Account," and then choosing "Software Download" on the left menu.

- 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.

Visit **cybersecurity.ttu.edu** for more information

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 matters!

October Cybersecurity Events

2021 marks the 18th year of National Cybersecurity Awareness Month (sponsored by The National Cyber Security Awareness Alliance), and the 17th year that TTU has participated with campus events and education. Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. Common sense, accountability, and responsibility are the cornerstones of cybersecurity. We are all responsible for practicing and promoting cybersecurity.

In conjunction with National Cybersecurity Awareness month, the TTU Office of the CIO will be providing educational materials and sessions for the TTU community. Please visit cybersecurity.ttu.edu for tips and information on a variety of cybersecurity topics. The National Cyber Security Awareness Alliance also provides tips at www.staysafeonline.org.

Our October lineup of events is provided for your convenience with more information to follow. If you have questions or need assistance, please contact IT Events at itevents@ttu.edu.

Date	Time	Event	Location
October 6	2:00pm-4:00pm	Dell Presentation	Zoom
October 13	10:00am – 12:00pm	Apple Presentation	Zoom
October 21	10:00am – 12:00pm	Microsoft Presentation	Zoom
October 27	10:00am – 12:00pm	Palo Alto Presentation	Zoom

TTU IT

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

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