Information Technology Division Bulletin

vol. 15 no. 2 | October 2018

We Are All Responsible

Cyber Security Awareness Month Special Edition

Acceptable Use Policy | Facebook Security | Microsoft Deploys Improved Security for O365 Services | Encryption | Beware of Natural Disaster Scams | Are You a Target? | Protecting Personal and Institutional Data

Message from the CIO

October is designated as "Cyber Security Awareness Month" by the National Cyber Security Awareness Alliance. For the past 14 years, Texas Tech University has participated, hosting a number of educational activities for faculty, staff, and students. As cyber crime continues to proliferate and cyber criminals become more savvy, your partnership is critical in our efforts to protect institutional information resources and data. In this issue, we focus on key articles to help you practice safe computing, and be on guard against attempts to steal or exploit TTU information resources and data. Many of these tips will also help you protect your personal devices and data. Remember to think before you click. . . **we are all responsible**. Go Tech!

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

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 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 security measures;
- Information on safe computing practices is available for the campus community at cybersecurity.ttu.edu;
- Be respectful, courteous, and ethical in the use of information resources;
- Do not share information resources login information (e.g., eRaider user name or 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/commercial gain or for political activity; and
- All use of information resources is governed by local policies and applicable state/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!

Facebook Security

Facebook users may unknowingly be promoting malicious content due to a new trend amongst internet scammers called "like-farming." The act of Facebook "liking" may now have unintended consequences. Seemingly benign Facebook posts that appeal to one's emotions can potentially be ploys for scammers to accumulate "likes" and "shares" from these posts.

Once a post has gained enough popularity, the scammers modify the content, replacing the promotional content with malware, and infecting those that "like" and "share" the page. Common characteristics of "like-farming" attempts:

- Posts that promise to raffle off expensive gifts if it is "shared" and "liked;"
- Invitations that ask a user to "like" or "share" to show appreciation;
- Any solicitations that thrive on the good nature of people and play to their emotions; and
- Sites that appear on your news feed identifying people that have also "liked."

TTU IT recommends that you routinely review your activity log by clicking "Activity Log" on the right-hand side of your Facebook page, and select "Likes and Reactions" under "Filters" on the left-hand side of the screen. If any of the activities in your log look suspicious, you can delete, "unlike," and report the incident to Facebook.

Help spread "like awareness" and understand that not every Facebook page is an accurate representation of the true owner, and criminal motives are often well disguised. As you participate in social networking tools, we strongly recommend that you limit your "likes" and savvy your "shares." For more information on security and social media, please visit cybersecurity.ttu.edu.

Microsoft Deploys Improved Security for O365 Services

In order to increase security and better protect information resources, Microsoft will end Office 365 support for TLS encryption protocol versions earlier than 1.2 on October 31, 2018. After this date, all client-server/browser-server combinations must use TLS 1.2 or later to connect to Office 365 services. Transport Layer Security (TLS) is a protocol used to establish secure communications over a network. TLS 1.2 has been available since 2008 and is widely supported by most applications. While Microsoft's analysis indicates TLS 1.0 and 1.1 usage is low, please read the known impacts below to determine whether you need to act to prepare for this change. For any questions or additional information, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

Known impacts (detailed information for each follows the list):

- Operating systems and browsers without native TLS 1.2 support
- Exchange mailbox integration in Skype for Business and Lync clients
- Exchange mailbox integration on Polycom CX500, CX600, & CX3000 IP phones

Operating systems and browsers without native TLS 1.2 support:

Customers who have the most recent operating system and browser versions should not experience any service interruptions following the October 31st deadline. The minimum software requirements are as follows:

Minimum Operating System Requirements:
- Windows 7 with KB3140245 installed
- Windows Server 2008 (R2) with KB3140245 installed
- OS X Mountain Lion with 10.8.5 update
- iOS 5
- Android 5

Minimum Web Browser Requirements:
- Internet Explorer 11
- Microsoft Edge (any version)
- Chrome 30
- Firefox 27
- Safari 7

Previous operating system and browser software may be unable to use the improved security. Please update your software to ensure uninterrupted access to the service.

Exchange mailbox integration in Skype for Business and Lync clients:

Customers running updated Microsoft Office 2016 with Skype for Business for PC or Skype for Business on Mac software should not experience any service interruptions following the October 31st deadline.

While basic chat, voice, and video features will be unaffected, mailbox features such as calendar, Outlook contacts, and voicemail will be inaccessible within the following Skype for Business and legacy Lync clients:

- Skype for Business 2016 for Windows without update KB4018323
- Skype for Business 2015/Lync 2013 for Windows without update KB4018334
- Lync for Mac 2011 and Lync 2010 Attendant

Upgrade (recommended) to Skype for Business on PC or Mac or apply updates to avoid a loss of functionality and to take advantage of the latest features.

Exchange mailbox integration on Polycom CX500, CX600, & CX3000 IP phones:

USB devices, such as headsets and Polycom CX300 [R2] handsets, are not affected. Nor are Polycom CX5000, CX5500, Trio, or VVX phones.

While basic phone calling will be unaffected on Polycom CX500, CX600, & CX3000 IP phones and mailbox features such as calendar, Outlook contacts, and voicemail can still be accessed on your computer, users will see the following notification indicating Microsoft Exchange integration is unavailable when attempting to access these functions directly on affected IP phones.

To avoid a loss of functionality, please consider replacing any phones in your area on which these advanced features are required with a supported device. You can view pictures of the affected phones in askIT.

Encryption

Mobile computing devices are easy targets for theft. When mobile devices containing confidential and sensitive data are stolen or compromised, institutional data, information resources, and individual identity are placed at risk. If you have a business need to store and/or transfer confidential or sensitive information on your mobile device and have no viable alternative, the TTU IT Division offers the following resources for the TTU Community:

- Mobile Phones/Tablets: Use one of the devices with internal security features. Enabling a non-simple passcode/passphrase or biometric form of authentication on mobile devices is the best way to protect mobile devices, stored data, and apps because it usually automatically encrypts the device as well.
- Laptops/Desktops: TTU IT recommends using the native operating system encryption, BitLocker and FileVault for Windows and macOS, respectively.

Contact your departmental IT support or IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.

Beware of Scams Related to Natural Disasters

The United States Computer Emergency Readiness Team (US-CERT) warns citizens to remain vigilant for malicious cyber activity seeking to capitalize on interest in and devastation from natural disasters*. Emails and social media posts requesting donations from duplicitous charitable organizations commonly appear after major natural disasters. We advise TTU students, faculty, and staff, as well as the community at large to exercise caution in handling any email with subject line, attachments, or hyperlinks related to natural disaster relief, even if it appears to originate from a trusted source. Fraudulent communication will often contain links or attachments that direct users to phishing or malware-infected websites. In some cases, these attempts to steal your identity are very sophisticated, complete with professional logos and good grammar.

The TTU IT Division and US-CERT recommend the following cybersecurity practices to protect yourself and TTU resources from this and other email scams:

- Verify the legitimacy of any email solicitation by contacting the organization directly through a trusted contact number. You can find trusted contact information for many charities. The following are examples from Hurricane Florence relief efforts:
  - http://give.org/charity-reviews/national
  - https://www.usa.gov/hurricane-florence
  - https://www.fema.gov/volunteer-donate-responsibly
  - https://www.nvoad.org/
  - https://www.consumer.ftc.gov/blog/2018/09/wise-giving-after-hurricane
- 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; and
- Keep current on critical system updates:
  - Windows Users:
    https://support.microsoft.com/en-us/help/12373/windows-update-faq
  - Mac Users:
    https://support.apple.com/en-us/HT201541
  - iOS Users:
    https://support.apple.com/en-us/HT204204
  - Android Users:
    https://support.google.com/android/answer/7680439?hl=en

We encourage you to practice cybersecurity, and to be aware of these activities designed to steal institutional and personal data. You can find additional cybersecurity tips online at cybersecurity.ttu.edu.

*Source: https://www.us-cert.gov/ncas/current-activity/2018/09/14/Potential-Hurricane-Florence-Phishing-Scams

Are You a Target?

Your mother's maiden name . . .
Your first car . . .
Your pet's name . . .
Place of your birth . . .
Your favorite color . . .
Your High School mascot . . .
Your anniversary date . . .
Name of your first born . . .

Is any of that information about you posted on Facebook? Twitter? LinkedIn? Instagram? Any public website? Is any of this information used as a password to your banking accounts? Other financial accounts? eCommerce sites? PayPal? Internet criminals are getting more creative in mining personal data in order to guess password reset questions and passwords. Once they can reset your password, then they can access your account and information. These exploits continue to grow because people use common information for reset questions and/or passwords, and criminals continue to profit from personal information theft.

We suggest the following safe computing practices:

- Review all the information you have published on websites and in social media, and remove anything that answers any of your password reset questions;
- Change any password reset questions that use information you had previously published publicly;
- Use different strong passwords for accounts, such as banking, credit, or investment accounts. You should not use your eRaider password for any accounts other than eRaider; and
- If you need to write down your passwords to remember them, write down a clue that will help you remember, but will be meaningless and undecipherable to others.

Working together, we can protect institutional and personal data, and make these strategies less lucrative for criminals. For information about improving your own personal cybersecurity, please visit 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.

Protecting Personal and Institutional Data

Historically, Internet criminals leverage our tax season to launch various campaigns to steal confidential data and resources. In the context of the massive Equifax data breach that was announced last year that potentially affected 143 million U.S. consumers (source: https://www.equifaxsecurity2017.com), the TTU IT Division strongly recommends that faculty, staff, and students be vigilant in protecting institutional and personal data and information resources. Recently, TTUHSC discovered that criminals likely used data stolen from Equifax to pose as TTUHSC employees, and petitioned the Texas Workforce Commission for unemployment pay. Be on the lookout for any unexpected communication of this type and report suspicious activity involving the Texas Workforce Commission to TTU Human Resources at hr.talent.management@ttu.edu or (806) 742-3650.

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 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://www.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, and selecting "Software Download" on the left menu.
- Microsoft Advanced Threat Protection: ATP checks links and attachments contained in all incoming email to determine if they are malicious. Additional information about ATP:

  As part of protecting 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.

As a reminder, the TTU IT Division recommends the following cybersecurity practices to protect yourself and TTU resources from this and other email scams:

- 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; and
- Keep current on critical system updates:
  - Windows Users:
    https://support.microsoft.com/en-us/help/12373/windows-update-faq
  - Mac Users:
    https://support.apple.com/en-us/HT201541
  - iOS Users:
    https://support.apple.com/en-us/HT204204
  - Android Users:
    https://support.google.com/android/answer/7680439?hl=en

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; and
- The Federal Trade Commission recommends filing your tax returns early to help prevent fraudulent filings.

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