Information Technology Division Bulletin

vol. 14 no. 7 | February 2018

Message from the CIO

While Internet criminals remain busy throughout the year, we experience a higher volume of threats during certain holidays and time periods. We typically see a high level of phishing attacks and email scams during tax season. In this edition, we provide information to help you be vigilant in protecting institutional and personal data. In addition, we also provide information on a Mac operating system vulnerability, including instructions for mitigating the problem. Finally, we provide tips for using the new focused inbox feature of Outlook—a handy tool that may help you manage your electronic correspondences. We thank you again for your partnership, as we work together to protect institutional data and information resources. Go Tech!

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

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, 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 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://www.askit.ttu.edu/windowsupdate
  - Mac Users: https://www.askit.ttu.edu/macupdate

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 https://www.identitytheft.gov;
- Consider registering for fraud alerts with all credit bureaus (Equifax, Innovis, Experian, and TransUnion). These free alerts must be renewed every 90 days. An extended fraud alert can be set for a longer time period. With fraud alerts, you will be contacted before any credit applications are approved;
- 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 https://www.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 http://www.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.

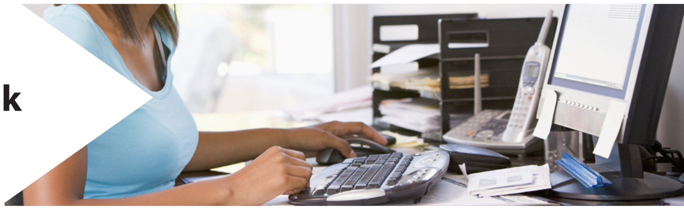
Vulnerability in macOS High Sierra

It has been reported by news outlets recently that a vulnerability in macOS High Sierra exists in which an attacker may be able to bypass administrator authentication by accessing the system as "root" without entering the administrator's password. Apple announced the release of "Security Update 2017-001" that resolves the issue. It is important to note that the "root" account within macOS High Sierra is disabled by default. Users of macOS High Sierra will not be affected unless this account has been manually enabled.

The TTU IT Division recommends, if you are using macOS High Sierra, that you apply the security update at your earliest convenience. Updates can be applied by opening the App Store app on your Mac. Click 'Updates' in the App Store toolbar, then use the Update buttons to download and install any updates listed. Please note that "Security Update 2017-001" is only available for systems running macOS High Sierra 10.13.1. If you are running 10.13 you will need to update to 10.13.1 first, then update the latest security release.

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

Focused Inbox for Outlook



The "Focused Inbox" is a new feature that Microsoft has implemented for the Office 365 version of Outlook and Outlook Web App to help manage a busy mailbox. "Focused Inbox" intelligently separates your inbox into two tabs, "Focused" and "Other."

"Focused Inbox" is intended to make the process of email management easier by helping you focus on the emails that matter most to you. This feature is not meant to take control of your email, but rather works to prioritize what is most important for you. Email directed to your "Focused Inbox" is determined automatically by taking into account the people you interact with most often, and the content of the email itself (e.g., newsletters, machine generated mail, etc.). You can switch between tabs at any time to take a quick look. You can easily reclassify emails between "Focused" and "Other." The more you use the "Focused Inbox," the more you train the software.

Options are available to fine tune your "Focused Inbox," by allowing control to which tab email messages are delivered. In order to ensure important emails are not missed, the IT Division recommends you check both tabs regularly, or disable the Focused Inbox feature. We encourage you to try using the "Focused Inbox," but if you wish to disable the feature, please see the following instructions:

https://www.askit.ttu.edu/focusedinbox.

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

Mail | Mail Stop 2008
Phone | 742-5151
Fax | 742-5155

TTU IT

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

Need IT assistance?
IT Help Central
(806) 742-4357 (HELP)
ithelpcentral@ttu.edu
askit.ttu.edu

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