Information Technology Division Bulletin

vol. 16 no. 8 | June 2020

Message from the CIO

As we head into summer, we reflect on how vastly different this year has been. Learning, teaching, and working remotely while providing flexibility in processes and deadlines has been an unprecedented challenge. The IT Division has prioritized transitioning quickly and effectively to meet the needs of our campus community, and we successfully met that goal with collaboration, hard work, dedication, and commitment to excellence. In addition to the changes required to maintain operations during this time, the IT staff has continued to provide online training, critical updates, and valuable support to ensure students, staff, and faculty can continue to excel in all academic and professional areas. Stay safe and Go Tech!

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

Reminder: Microsoft O365 Voicemail

This past spring, Microsoft transitioned Texas Tech University's Office 365 (O365) voicemail services to their modern Cloud Voicemail service. Users experienced minimal impact, and voicemail messages are still accessible in email and Microsoft Teams software.

If you are receiving notifications in your Skype for Business (SfB) software to upgrade to Microsoft Teams, these notifications can be dismissed or avoided altogether by upgrading to the latest O365 SfB software (recommended), as SfB is still required for telephony at TTU. To upgrade your Skype for Business software, follow the instructions at www.askit.ttu.edu/skypeforbusiness.

As a reminder, Microsoft no longer supports mailbox features such as calendar, contacts, and voicemail directly on older telephone handsets, such as Polycom CX500, CX600, or CX3000 IP phones.

Please contact IT Help Central at (806) 742-4357 (HELP) or ithelpcentral@ttu.edu if you require assistance with voicemail services.

Beware of COVID-19 Stimulus Scams

Since the news of the Coronavirus gained international attention in early January, we have seen an astronomical amount of phishing and malware emails connected to COVID-19. Google reported 18 million daily malicious emails specifically related to COVID-19 in the month of April. Once the U.S. Government released their proposal for the national stimulus package in mid-March, cybercriminals then shifted their focus to individuals' stimulus checks. Knowing many individuals are desperate for financial assistance, cybercriminals have abused these fears through stimulus-related attacks. As a second stimulus package appears to be on the horizon, we remind you to stay vigilant.

Cybercriminals are sending phishing emails that appear to provide legitimate stimulus-related information but actually contain malicious attachments. In addition to phishing emails, cybercriminals are also creating domains to target consumers. While many of these domains are in fact legitimate, a substantial percentage are malicious. Year-to-date, 30% of the domains created were considered either malicious or suspect.

To best protect yourself and TTU information resources from stimulus-related cyberattacks, please follow the recommendations below:

- Examine domains closely, particularly links in emails and supposed "government" sites;
- Use extreme caution when receiving files via email;
- Do not click promotional links within emails and be wary of "special" offers; and
- Never reuse passwords.

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

Coronavirus update: As economic stimulus payments start to flow, cyber-attackers want to get their share too. (2020, April). Retrieved from HERE.

Whitney, L. (2020, April 20). Scammers exploiting stimulus payments with phishing attacks and malicious domains. Retrieved from HERE.

New Version of Symantec Endpoint Protection

The TTU IT Division recently released a new version of Symantec Endpoint Protection software (Version 14.2.2) for both Windows and macOS, available to download on the eRaider Software Download site – https://www.eraider.ttu.edu/. We strongly recommend that you install the new version, as Symantec is addressing known vulnerabilities with the previous version. Note that our testing determined there is no change to the customer experience.

Notes for Downloading the New Version:

After you navigate to the eRaider site, click on "Manage Your Account" and then select "Software Download" from the left navigation pane. Once you select your operating system(s), you will see the option to select either "unmanaged" or "managed" versions.

All university-owned Windows and Apple computers must use the managed package, which allows the Symantec software to check our centrally managed server for updates. Apple computers running macOS 10.15 (Catalina) will need to use a browser other than Safari (e.g. Chrome or Firefox) to download the managed package.

Personally-owned computers should use the unmanaged package, which requires the owner to update the Symantec software themselves. Once you select the appropriate Symantec software, an installation program will walk you through the simple process of installing.

The following table provides further information about each version:

	Managed (University-owned)	**Unmanaged (Personally-owned)**
Antivirus Live Updates	Critical updates can be automatically installed on all Managed Clients in the event of a serious IT security threat.	The computer owner must obtain updates from the Symantec Live Update server through the Internet.
Release/ Version Updates	Can be pushed out to all clients for automatic install/update.	The computer owner must obtain the updates from eRaider Software Download and install them on the computer.
Monitoring and Reporting	Active attacks and malware infections can be monitored and proactively corrected. **NOTE: User activity and content are NOT monitored by this software.**	None.

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

PARENTS' CORNER

Entertainment Resources

We know this is a stressful and confusing time as you attempt to acclimate yourselves to learning, teaching, and working remotely. Due to the extension of the social distancing period, you may also find yourself struggling to provide quality educational and entertainment resources for your family. While there are many activities that can still be done outside - such as gardening, a backyard cookout, and home projects - there may still be weeks of quarantine in your future. To help you adjust to these unusual times, we have combined a list of free virtual tours to fill your nights and weekends with family fun. We hope you enjoy!

Disclaimer: Texas Tech University does not endorse or recommend any of the specific locations/resources listed below. This article is simply provided as an informational resource and community service.

VIRTUAL TOURS

Google Arts and Culture

The Louvre

The Solomon R. Guggenheim Museum

The National Gallery of Art

The British Museum

Museum of the American Revolution

Smithsonian National Museum Of Natural History

The National Museum Of The United States Air Force

Yellowstone National Park

The Metropolitan Museum of Art

The National Women's History Museum