**Message from the CIO**

As the semester begins winding down, our holiday preparations are gearing up. In this issue, we provide a few resources and important reminders for the upcoming holiday shopping season on how to stay mindful and secure while looking for gifts online and completing online purchases. For those of you who have computer equipment on your shopping list, TTU has negotiated many computer and technology discounts available to members of the Texas Tech community, and these discounts are also available for personal purchases. As you may have seen in various campus announcements, the TTU IT Division is upgrading (to ServiceNow) our IT service management system that was used for handling customer requests. Remember that the winter holiday season is prime time for Internet criminals. We urge you to practice safe computing, stay vigilant, and think before you click! Happy Thanksgiving Wishes to All!

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

**ServiceNow**

The IT Division is transitioning to a new IT support platform, replacing FootPrints with ServiceNow. This new platform will provide more self-service options (askIT) for our customers, while offering additional tools to meet the needs of our campus community.

**Key Updates:**
- **More personalization options, including issue subscription options:** Sign up to receive text/email alerts when a change has been made to your issue.
- **New email address:** Support emails from IT Help Central will come from servicenow@ttu.edu instead of ithelpcentral@ttu.edu. (You may preview example communications from ServiceNow in askIT)

**Online Shopping Tips**

This holiday season, the TTU IT Division encourages you to be mindful while shopping online:
- Type in the URL instead of clicking on links in emails, social media posts, or SMS. Also, when you are planning on purchasing items, be extra careful when clicking on short URLs or scanning QR codes as those are favorite methods used by cyber criminals to redirect you to another site;
- Look for the lock icon on the browser’s status bar, and make sure that “https” appears in the address before completing your purchase. The “https” in the address indicates that the connection is secure and your credit card information is encrypted. If you don’t see a lock icon or https://, then your connection is not secure, and your information could be at risk;
- Install, enable, and regularly update anti-malware/anti-virus software on your computers and devices;
- Regularly update operating systems, application software, and mobile OS (iOS, iPadOS, and Android) and apps. Instructions for updating your operating systems may be found below:
  - Windows: [https://www.askit.ttu.edu/windowsupdate](https://www.askit.ttu.edu/windowsupdate)
  - Mac: [https://www.askit.ttu.edu/macupdate](https://www.askit.ttu.edu/macupdate)
- Pay with a credit card instead of a debit card. With credit card transactions, you have a period of time before money is transferred to the seller, but debit transactions are immediately withdrawn from your account. You may also consider paying via a one-time use credit card, a gift card, or reputable payment systems such as Apple Pay, Google Pay, Venmo, etc;
- Shop through reputable online stores. Be cautious of sellers in online marketplaces like Etsy, eBay, and Craigslist. Many of the sellers that post on these services are individuals, so your risk of online fraud or not getting the gift you purchased is much higher;
- Save emails regarding your online transactions, especially online receipts, and any electronic correspondence you have with the retailer or seller; and
- Review your credit card and bank statements as soon as you receive them, and immediately report unauthorized charges. Set alerts on your credit cards for expenditure so that you are immediately notified when your credit card is used.

We encourage you to be vigilant in practicing cybersecurity and invite you to learn more cybersecurity tips online at [http://www.ttu.edu/cybersecurity](http://www.ttu.edu/cybersecurity).

For more information or questions, please contact IT Help Central at (806) 742-4357 (HELP) or via email at ithelpcentral@ttu.edu.
Social media companies refer to platform manipulation as the unauthorized use of their platforms by criminals who employ deceptive or aggressive activity to disrupt or mislead other users. In common terms, actions like spam, fake accounts, or automated accounts all fall under this rubric.

Platform manipulation can be hard to detect. Every year, social media giants hone their algorithms to identify unscrupulous behavior. To root out fake accounts, social media companies employ algorithms to comb through user accounts, looking for:

- Accounts created in large batches at the same time or from the same geographic region;
- Profiles that engage with narrow bands of very targeted content, often with identical posts;
- Dormant social media accounts with a sudden surge in posting; and
- Unusual activity patterns in the time of posts.

Social Media Companies Take Action

Social media companies are aggressively curating their user base. Relying on algorithms to identify manipulative accounts, these companies purge a staggering number of fake or compromised accounts each year.

Recent examples:

- Facebook Inc took down 1.3 billion fake accounts between October 2021 and December 2021 and employs 35,000 to remove fake accounts and stamp out misinformation on its platform.

How to Spot Fake Accounts:

- Check to see if the account is verified. Facebook, Twitter, and Instagram all have verification for prominent accounts;
- Review the account name for random numbers and letters; this might suggest the account was computer generated and not a real person;
- Look at account activity; accounts that simply posts links and comments without engaging with other may be suspect; and
- Spoofed or fraudulent accounts typically have a small number of followers compared to the authentic celebrity or company they are impersonating.

Tips to Remember:

- Be wary of offers that seem too good to be true;
- Look for computer generated accounts operating with the express intent to influence behavior or opinion; and
- Verify information from social media with other news sources.

Sam Segran Named Higher Education IT Executive of the Year

Sam Segran, CIO and Vice President for Information Technology, has been designated one of the "Higher Education IT Executive of the Year" winners in the inaugural 2022 EdScoop 50 Awards!

From EdScoop - Announcing the winners of the 2022 EdScoop 50 Awards, November 1, 2022:

"The awards, in their first year, honor the most influential people in the higher education technology community, along with the most innovative projects that make a positive impact across universities."

"Starting in July, members of the higher education IT community nominated more than 200 leaders and projects for the awards. The EdScoop team narrowed the list to the top 80, and readers cast more than 200,000 votes to select this year’s winners."

The national IT community selected 50 top executives to be awarded, representing 40 institutions, two university systems, seven private sector companies, and one professional organization.