

Information Technology Division Bulletin

vol. 13 no. 9 | July 2017



Cybersecurity
Travel Tips

Faculty &
Staff Discounts

HR Training
Catalog

Limit Likes
Savvy Shares

Message from the CIO

We hope this bulletin finds you enjoying the summer months, and personal time to relax. For those traveling, we provide **tips on protecting your personal information** and data while vacationing. For those who “travel” via Facebook, beware of criminal tactics that target the simple practice of “**sharing**” and “**liking**.” Summer is also a time that many devote to learning and preparing, so we have included information on our new **HR online training catalog**—a collaborative endeavor with Jodi Billingsley and her staff. For those looking to invest in a new system before the fall, we provide information on **faculty and staff hardware discounts**. Go Tech!

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



Cybersecurity Travel Tips

Vacationers are at an increased risk for identity theft because they often carry credit cards, passports, and other official forms of personal identification. As a result, tourists are routinely targeted by criminals, who are just as likely to target your personal information as your expensive camera or laptop. Travelers should be careful to protect themselves and take extra precaution with personally identifiable information; for instance:

- Don't travel with all your credit cards—carrying a limited number of credit cards reduces the magnitude of loss or theft;
- Take advantage of the hotel safe, rather than leaving personal information in your hotel room;
- If you make travel arrangements using a mobile

device, avoid storing transaction information; such as, login information, credit card number, or billing address. Remember that saved information could be stolen along with your phone;

- Protect your computers and mobile devices (including phones) with passwords;
- Public wireless connections are not secure, so avoid using them for secure transactions, such as transactions requiring a login; and
- Stay alert! It is easy to let your guard down while relaxing on vacation, but it's important to be aware of your surroundings and the people around you.

For more cybersecurity awareness information, please visit cybersecurity.ttu.edu.

TTU Faculty & Staff Discounts

TTU faculty and staff are eligible to receive discounts on hardware and software products. Visit the IT Help Central website at www.ithelpcentral.ttu.edu, and click on “Buying the Right Computer” for recommendations, as well as links to the Apple and Dell online stores. You may also visit www.itts.ttu.edu/software for detailed information about a variety of software, such as Symantec Endpoint Protection and Adobe products that are provided at no cost to faculty and staff.

For additional questions, contact IT Help Central at (806) 742-4357 (HELP), ithelpcentral@ttu.edu, or visit our self-service resources at www.askIT.ttu.edu. For departmental purchases, the TTU IT Division and TTU Procurement Services have streamlined the process to obtain the best pricing possible on technology hardware purchases through partnerships with Apple and Dell. For your department's convenience, online purchase orders can be pre-populated through the Procurement Services website, techbuy.ttu.edu.





HR Training Catalog

cbit.ttu.edu

Skillsoft Online Training (cbit.ttu.edu) is an online, self-paced, interactive training system. TTU hosts an inventory of over 4,000 courses, covering basic to advanced technology skills, customer service, project management, and general management skills. The TTU IT Division has partnered with Human Resources to construct an HR Training Catalog available to faculty, staff, and students. The catalog includes courses in:

- Ethics;
- HR Certifications;

- Interviewing and Hiring;
- Organizational Behavior;
- Recruitment and Retention;
- HR Leadership Program;
- Strategies for Successful Employee On-Boarding;
- The Role of HR as a Business Partner;
- Communicating in a Diverse Environment; and
- Customer Service.

CBT modules can be used as professional development for a wide variety of skills. Please visit www.cbit.ttu.edu.

Limit Your Likes & Savvy Your Shares



Facebook users may unknowingly be promoting malicious content due to a recent 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 the “View Activity Log” button on the bottom right-hand side of your profile cover photo. If any of the activities in your log look suspicious, you can delete, “unlike,” or report the incident to Facebook.

Spread awareness 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.”

Mail | Mail Stop 2008

Phone | 742-5151

Fax | 742-5155

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

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

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

