Preparing for the Holidays

Message from the CIO
As the semester begins to wind down, our holiday preparations are gearing up. In this issue, we provide a few resources and important reminders during the hustle and bustle of the upcoming holiday season. 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!

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

Computer Discounts

Thanks to our partnership with Dell and Apple, you can do your holiday shopping anywhere, anytime! Texas Tech faculty, staff, and students can receive discounts on Dell and Apple products. For departmental and personal purchases: ithc.ttu.edu/recommend.

When To Dip Your Chip*

Many consumers now carry “chip-equipped” credit cards (metallic square on your card). Chip technology protects confidential information and reduces the threat of point-of-sale (POS) credit card fraud and data breaches.

**Chip-equipped card security:**
- Every time you use a new chip-equipped card, the chip adds a layer of security to the magnetic strip containing your card holder information by creating a unique transaction code associated with a particular purchase. Instead of transmitting personal and credit card information (name, credit card number, expiration date), a unique transaction code is sent; and
- In other countries where chip-compatible equipment has been put in place, chip-equipped cards have demonstrated promising results in reducing fraud.

**Purchasing with a chip-equipped card:**
- If the merchant has updated their equipment, you will insert the chip-equipped section of your card into the POS scanner.
- Some chip-equipped cards also support contact-less card reading. Instead of inserting your card, you tap the POS scanner for the transaction to take place; and
- Note that some of the new cards require a signature or to enter a PIN.

In the last year, many retailers have updated equipment and the technology has become more prevalent. Chip technology will not eliminate data breaches and credit card fraud, but it is a step in the right direction to protect consumers and make it tougher on fraudsters. Don’t let the Grinch steal your Christmas - practice safe computing!

*Information adapted from the creditcards.com organization website.
Online Shopping Checklist

As one of the peak seasons for Internet criminals draws near, the TTU IT Division recommends that you be vigilant and practice safe computing during this festive season:

- **Be prepared to shop online.** Be sure your computer has the latest security updates and is currently protected by antivirus software. When submitting your purchase, look for the lock icon on the browser's status bar and make sure that “https” appears in the address (https://...);
- **Be guarded while you shop online.** Limit online shopping to vendors you know and trust, and do not respond to pop-up notifications;
- **Track your online shopping activities.** Print and save records of your online transactions such as the online receipt and any electronic correspondence you had with the retailer or seller. Review your credit card and bank statements as you receive them and immediately report unauthorized charges;
- **Practice safe shopping.** Don’t use public computers or networks to shop online. We recommend that you not save your debit and credit card information with online vendors. As we have seen in the last several years, criminals target retailers to steal customer confidential information. The less you have stored with vendors, the less likely you are to become a victim;
- **Beware of online scams.** “Deals” that are too good to be true are probably not and could be a scam. Carefully review shipping, warranty, and other terms and conditions. Avoid high pressure sales offers or online vendors that market to your sympathies;
- **Consider a PO. Box as your return address.** For a modest cost, you can acquire a post office box and avoid providing your physical home address when possible; and
- **Think before you click!** An unwise click can lead to theft of your information, privacy, and resources.

With the hectic pace of our lives, online shopping is convenient, and the world becomes our shopping mall. The TTU IT Division encourages you to use these tips as you embark on your holiday shopping and activities.

Information About Wireless Connectivity On Campus

Wireless connectivity available on the Texas Tech University campus consists of WiFi and Cellular (4G, LTE, etc.). Cellular services are provided by AT&T, Verizon, Sprint, and T-Mobile. We partnered with AT&T to significantly improve the cellular infrastructure on campus. The enhanced AT&T cellular network already accommodates Verizon, and AT&T is currently working with the other carriers.

The TTUnet WiFi network is provided by the TTU IT Division and was deployed by Telecommunications several years ago. We upgraded the residence halls to the latest WiFi technology a couple of years ago, and are in the midst of a multi-year WiFi upgrade of academic buildings.

The quality of your WiFi experience can be negatively impacted by a variety of things, including the list below:

1. Installing consumer or non-University provided WiFi routers or extenders (e.g., Apple, Netgear, or Linksys) will cause serious interference with those attempting to connect their devices to TTUnet WiFi;
2. “Wireless” display devices (e.g. clicker technology and/or pointer devices) for conference and classrooms will interfere with WiFi devices in the vicinity;
3. Incorrectly configured WiFi devices may not connect reliably to TTUnet WiFi; and
4. WiFi enabled printers, consoles, and other devices (e.g., Roku, Apple TV, PlayStation, etc.), as well as some microwave ovens, will negatively impact WiFi performance and connectivity, especially in heavy use areas such as residence halls, classrooms, and during events.

Telecommunications staff monitor WiFi services closely, and are also working on mitigating some of the known interference issues. IT Help Central staff also regularly assist the campus community in configuring devices to connect to the TTUnet WiFi successfully. While we currently have only a few cases of WiFi issues reported to IT Help Central, we provide instructions on connecting to TTUnet WiFi at askit.ttu.edu/wifi. Should you experience problems using TTUnet WiFi, please contact IT Help Central at ithelpcentral@ttu.edu or (806) 742-4357 (HELP). We appreciate your partnership in helping us maintain a robust wireless infrastructure for all of us.

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.cbt.ttu.edu