Message from the CIO
Technology has become far more than a business productivity tool; technology has become a means of communication, connection, and collaboration. At TTU, we have worked hard to provide and maintain the IT infrastructure to support such interaction for the TTU community. In this bulletin, we highlight several technologies that foster interaction: eLearning creates a community bridge for faculty and students; safe blogging provides a communication mechanism for students; and email fosters communication and transactions for all members of the Texas Tech community. In this edition, we also suggest tips to prevent identity theft as you explore and navigate technologies of today. Lastly, please join me in congratulating IT staff members who have recently received TTU awards.

Wishing you a safe and enjoyable summer!

- Sam Segran
  Associate Vice President for IT and Chief Information Officer

---

eLearning
TTU eLearning, located within the Raiderlink portal http://www.raiderlink.ttu.edu and created by the TTU IT Division, is a web-based course communication tool for faculty and students.

Intended as a course management tool, eLearning provides faculty with a web location to:

- create course assignments;
- upload course materials;
- set up and maintain a gradebook;
- publish final grades to the student information system; and
- add teaching assistants to help manage students, grades, and assignments.

From a student vantage point, eLearning offers the following features:

- quick access to assignments, grades, and course materials;
- ability to upload assignments; and
- obtain course materials and assignments posted by faculty.

When faculty, staff, and students access eLearning, the system automatically identifies the individual’s role (faculty/staff/student). Technology Support offers shortcourses for those interested in detailed functionality. http://webapps.itsd.ttu.edu/sc/ScheduledList.php

For additional information or technical questions, please contact IT Help Central, (806)742-HELP (4357).

Safe Blogging
Personal web spaces are a forum for communicating and posting ideas, photographs, videos, and other multimedia. Blogging is an online dynamic collection of one's thoughts, opinions, selected links, and personal information. Personal web spaces are used to communicate with “real-world” friends, as well as “cyber” friends. Popular sites, such as “MySpace” and “FaceBook,” cater to college communities. Bloggers can post and exchange their information, photographs, documents, and videos. Recent media coverage suggests that posting and communicating personal information may pose a risk for identity theft, stalking, or self-incrimination.

The TTU IT Division recommends the following practices:

- Be as anonymous as possible and carefully select information you post. Avoid postings that could enable a stranger to locate you. Never, under any circumstances, post your phone number or address;
- Read all privacy policies. Check to see if your service has a “friends” list that allows you to control who can visit your profile or blog;
- Carefully monitor your contact list; be aware of who can view your personal information. If possible, avoid allowing your “friends” contact lists to automatically view your information;
- Scrutinize third party information sharing policies. Some blog services may give your personal information (including your IP address) to other advertising companies in order to pay for the “free” service you are receiving;
- Avoid in-person meetings. Don’t get together with someone you “meet” online unless you are certain of their actual identity. If you do meet in person, don’t go alone and tell people where you will be meeting;
- Private and public companies review personal web space information. According to ExecuNet, a leading recruiting firm, 78% of executive recruiters routinely use Internet information to learn more about candidates and 35% have eliminated candidates based on the information they found;
- Information contained in a personal web space can be viewed as evidence of illegal or inappropriate behavior; and
- Avoid posting photos that allow people to identify you (street signs, license plates, school logo clothing, etc.), especially images that are sexually suggestive or display illegal activity (e.g. drinking under age, drug use, etc.).

Email Etiquette: Guidelines for Professionalism
Email has quickly become a primary means of communication in our digital world, with a majority of TTU faculty, staff, and students turning to electronic mail for communications once handled by phone, letter, or face-to-face meetings. While a simple method of communication for both the sender and recipient, email also has challenges. We suggest you consider these guidelines for professional communication with email:

- Email is permanent. It can be forwarded to other people easily and used to document activity;
- Use proper spelling, grammar, and formatting. Given that you never know who may view your correspondence, use proper grammar and spelling, even when sending a seemingly trivial email. Use conventional grammar standards, such as capitalizing letters that should be capitalized. If something is important enough for you to forward, copy the original author on the forward, if appropriate;
- Choose your words wisely. Make sure your email conveys the message you wish the recipient to receive. The tone of an email is challenging to convey and may be misinterpreted. There may be times when you may want to clarify your message in person. Avoid sending email while in emotional situations and remember to include only necessary information. As with all written communications, organize your email in a logical, clear manner that will help your reader understand your message;
- Use caution when using all CAPS in an email. According to Internet-based communication culture, using CAPS conveys the message that you are shouting at your recipient;
- Include the original text when you are replying to refresh correspondent's memory. Many times people forget details of their original message. This will help them to understand what you are referring to in your email, minimizing confusion and miscommunication. Also, be sure to read previous messages sent to you when you are replying;
Use humor sparingly. Not everyone has the same sense of humor. Make sure the email you are about to send is appropriate for the people to whom you are sending it. If you are unsure about your audience, either ask the individual or don’t include the humor;

Use a meaningful subject line. Meaningful subject lines will help gain the attention of the intended recipient. This will improve the likelihood that your email is read and given the proper attention. It will also help you organize your email for later use. Note that you should use the “urgent” email classification judiciously;

Respond to emails promptly. The nature of electronic communication causes people to have different response timeline expectations compared to traditional written correspondences. Be sensitive to this difference and respond as promptly as possible. If you are out of the office, be sure to use an automated response message, so your sender knows when you will return;

Follow-up when sending an important message. As appropriate, call your intended recipient to notify them that you have sent an important email; and

Consider the appropriateness of email signature lines. Email signature lines are a convenient place to display contact information, as well as to add a personal touch. Photos, long quotations, or large graphic files added as a signature line will increase the size of your message and likely irritate the recipient.

If you have questions about email use, please contact IT Help Central, (806) 742-HELP (4357).

Identity Theft Prevention Tips
Provided by Lieutenant David Parker, Texas Tech Police Department

- Destroy credit card applications, receipts, bank and billing statements;
- Avoid giving your SSN unless it’s absolutely necessary – use other identifiers;
- Pay attention to your billing cycles;
- Guard your postal mail from theft;
- Put passwords on credit card, bank, and phone accounts;
- Carry as little identification information as possible;
- Limit the number of credit cards you carry;
- Don’t give personal identification on the phone unless you initiate the call;
- Be cautious storing and managing your personal information at home;
- Check on who has access to your personal information at work;
- Don’t carry your Social Security card;
- Save ATM and credit card receipts to check against statements;
- Be informed about your financial institutions’ policies of sharing information; and
- Make sure your credit reports are accurate.

For additional safe computing information, please visit http://safecomputing.ttu.edu.