Blogging
With the popularity of blogging and personal networking sites among college-age students, the TTU IT Division encourages the TTU community to be aware of the risks associated with blogging and steps that can be taken to minimize those risks. Blogging can be a powerful communication and collaboration tool and, with a few simple precautions, can be a safe and productive part of the educational process.

We recommend the following safe practices for blogging:

• **Be as anonymous as possible.** Avoid posting information that could enable a stranger to locate you. Such information includes your last name, school name, cell phone number, and physical location. You should also be careful about posting your favorite locations, your class schedules, your cell phone number, and your friends;

• **Protect your information.** Check to see if your blogging service has a “friends list” (privacy controls) that allows you to control who can visit your blog. If so, be sure to allow only people you know and trust. Remember that for many services, once you add someone to your “friends” list, you also grant access to their “friends” list. As your list grows, the likelihood increases that your information may be viewed by someone with ill-intent;

• **Photos: Think before posting.** It’s best to avoid photos that can make it easy for people to recognize you. We strongly recommend that you do not post photos that are suggestive or sexual in nature. What you post on the Internet becomes public and can be downloaded by others. Before uploading a photo, ask yourself how you would feel if that picture were seen by the world;

• **Check comments regularly.** If you allow people to comment on your profile or blog, review your comments regularly. Don’t respond to negative or embarrassing comments. Never allow messages that are degrading, threatening, offensive, or embarrassing to yourself or others. Delete them and, if possible, block offensive writers from commenting further;

• **Be honest about your age.** Membership rules are there to protect people. Misrepresenting your age could expose you to serious trouble and risk;

• **Read between the “lines.”** It may be fun to check out new people for friendship/romance, but be aware that many people act nice because they have motives that are malicious. Plattering/supportive messages may be more about manipulation than friendship or romance;

• **Change your passwords.** Change the passwords you use to access online services at least once every three months and do not share your password. Remember a good password consists of at least eight characters, utilizing upper- and lower-case letters, as well as numbers and/or special characters; and

• ** Routinely conduct searches on your name.** Use Google and other search engines to search for your name. Try searching for your nicknames, phone numbers, and addresses; you might be surprised at what you find. Many blogging sites have instructions on how to exclude your posts from appearing in search engine results.

One of the best ways to protect yourself as you participate in blogging and social networking is to be aware of the following risks that you may face:

• **You have little control over who may access your information.** The fact is that people can find ways to bypass privacy measures and gain access to your information. Your readers may include potential or current employers, coworkers and professional colleagues, neighbors, your spouse or partner, your family, and anyone else curious enough to type your name, email address, or screen name into Google or another search engine;

• **You may be held accountable for information you post on your blog.** For example, employers might object to confidential items, employer-related information, and postings that point to illegal or unethical behavior. In addition, bankers, insurance brokers, police departments, public safety, and college admissions officers are increasingly using social networking and blogging sites to gain information about individuals;

• **If your real identity is tied to your blog, anyone can eventually read your information.** Once something is posted on the Internet it is effectively permanent and public. Even if you subsequently delete the post, it may have been cached in a search engine archive, a company server, or an individual computer. As a result, your information may remain in a browser cache or on the hard drive of anyone that visited your blog; and

• **You may expose yourself to Internet criminals.** Any popular online destination invariably draws criminals looking for an easy target. Hackers and spammers have begun using blogging and social networking sites to lure you to malicious web pages that could install destructive software to your computer without your knowledge. Hackers can easily post a malicious link on the anonymous posting page of your blogging site.

Ultimately, posting your personal information on a blogging site may result in problems at work, trouble with law enforcement, financial risks, reputation risks, privacy risks, as well as physical risk to you or your family from on-line predators. As with any endeavor, the more informed you are about the processes, risks, and protections, the more likely you are to have a safe and successful blogging experience. For more information on a wide variety of security topics related to online safety, visit the website for the TTU Office of the CIO Safe Computing Practices Campaign at www.safecomputing.ttu.edu.

---

Message from the CIO
To members of the TTU community, *Strive for Honor* means much more than simply lyrics to our school song. *Strive for Honor* instills a sense of pride, a sense of integrity that stretches from the classroom to the athletic field to the daily responsibilities of TTU community members. TTU is working diligently to raise campus awareness of ethics and integrity in every aspect of our organization. To further encourage each member of the TTU family to *Strive for Honor*, this bulletin issue highlights specific topics and recommended **safe practices for blogging, downloading files, and recognizing an infected computer**. We also provide information on **reporting a security incident** to the proper TTU IT Security professional. Used safely and with integrity, technology tools support the aim to *Strive for Honor*. Early this semester, we will be inviting the TTU community to participate in an online **data security survey** to help TTU IT provide appropriate security tools and services for you. Stay tuned for another fall full of IT educational opportunities and activities. Get your guns up!

-Sam Segran
Associate Vice President for IT and Chief Information Officer
Is Your Computer Infected?
Viruses, worms, Trojan Horses, and spyware can infect your computer systems without your knowledge. The following symptoms can be a sign that your computer has been infected:
- Slower than normal operating system response time;
- Warning messages or dialogue boxes that suddenly appear in an application;
- Slower than normal application response time; and
- Sudden changes in the look of application windows
  - an additional search bar in browser
  - your browser home page changes
  - a new icon appears in the lower right task tray.

Most people inadvertently infect their systems by opening an infected email attachment, by clicking on a link contained in an email message, or visiting a questionable web site. The malicious application will either install immediately or at a designated time after it has been downloaded onto your system. You will not be aware that the program is installing on your system; your first warning will be the symptoms noted above. If you experience any of these symptoms please contact IT Help Central at (806) 742-HELP (4357).

Reporting a Computer Security Incident
While we all know that we should protect our workstations, laptops, servers, and applications by using safe computing practices, many of us do not know that should a security issue arise we should report it promptly to the appropriate TTU IT security staff. Texas Tech University has procedures in place for reporting computer security incidents as outlined in the Incident Management Security Policy which is part of the TTU OP 52.04. To view our policy, visit http://www.infotech.ttu.edu/security/docs/incident_management.php.

There are a wide variety of data security incidents that must be reported which include, but are not limited to: virus, worm, and Trojan horse infections; unauthorized use of computer accounts and systems; complaints of improper use of Information Resources; data theft and fraud; and computer system compromises. Should you become aware of a data security issue, please follow the appropriate procedure:
1. Immediately report the incident to the Information Security Officer (ISO) or his designees.
2. For virus & worm infections, compromised systems, or improper use complaints, contact the IT Security Team at security@ttu.edu or 742-0840.
3. To report an incident that may involve a criminal act (data theft, fraud, etc.); the exposure of confidential information, or a threat to personal or homeland security, directly contact the TTU Information Security Officer, J Stalcup, at 742-8000 x7000 or J.Stalcup@ttu.edu.
4. Perform appropriate remedial action in accordance with the ISO’s instructions and IT guidelines.

Serious incidents will require some investigation to assess the severity of the incident and to determine whether further forensics are required. Please contact the security staff above before altering the computing system or attempting to “fix the problem”. Typically virus and worm infections can be cleaned up without further investigation and IT Help Central, (806) 742-HELP (4357) or ithelpdesk@ttu.edu, can provide assistance.

TTU IT Data Security Survey
In the next few weeks, the TTU Office of the CIO will be surveying the University community concerning the access, use, and storage of confidential or sensitive data. The brief online survey will help us to further improve our security posture and to provide tools and suggestions for securing confidential and sensitive data. State regulations, TTU IT Security Policies, and TTU Operating Policies provide the following definitions:

Confidential Information - information that is exempt from disclosure requirements under the provisions of applicable state or federal law, e.g. the Texas Public Information Act, because the disclosure of which may harm the institution or individual. (Examples include Social Security Number, Credit Card Numbers, etc.)

Sensitive Information - information or knowledge that might result in a loss of security if revealed or disclosed to others who might have low or unknown trust ability and/or indeterminable or hostile intentions. (Examples include home addresses, cell phone numbers, birth dates, etc.)

Look for the email invitation to participate in the online survey in the next week! Thank you in advance for your participation and contribution.

Above: Srirangam Addepalli holds his guns up with the Masked Rider and Raider Red.
Right: Michael Horton and his daughter, Greenli Kate, show off their TTU Spirit.

Contributions by: Katherine Austin, Ph.D., Shannon Cepica, Alvin Mills, Yung Ng, Ric Ramon, J Stalcup, Britta Tyé, Nicole Weatherly, and Allen Young.
Safe Computing Practices Committee: Sam Seyran, Katherine Austin, Ph.D., Darrell Bateman, Pulin Bhatt, Shannon Cepica, Scott Hall, Mark Holwerda, Michael Horton, Danny Mar, Alvin Mills, Yung Ng, Mike Simmons, J Stalcup, John Vandygriff, Allen Young, and assistance from IT Division leadership and staff.