Message from the CIO

In observation of National Cyber Security Awareness month, the TTU Office of the CIO designated October as TTU Cyber Security Awareness month. During the month, the TTU Office of the CIO reinforced safe computing practices. Remember that cyber security is everyone’s responsibility. Our institutional IT security posture is a collaborative effort, and we depend on all faculty, staff, and students to practice safe cyber security habits to help protect institutional information resources, as well as your personal data. Featured in this issue is an article with general cyber security tips and the history of TTU cyber security written by James Hodgins, Section Coordinator of Internal Communications for TTU Communications & Marketing, and first published in RaiderWire, the Texas Tech faculty and staff newsletter. Additionally, there are password safety suggestions and tips. We appreciate the care that you take when you are online. We count on you — among other things — to think before you click!

-Sam Segran

Associate Vice President for IT and Chief Information Officer

LEARN HOW TO PROTECT YOURSELF ONLINE DURING CYBER SECURITY AWARENESS MONTH

Today, whether it’s at work or at home, on social networks or on a phone, we are connected more than ever before thanks to technology. IT systems and tools such as the Internet were created to improve communication and make it easier to share information, but they were never originally built with high-level security in mind.

Many people go online without knowing how to protect themselves, and that makes them all vulnerable targets, Chief Information Officer Sam Segran said. According to the 2012 Norton Cybercrime report, close to 18 people worldwide are victimized by computer crime every second. In the U.S. alone, people lost an estimated $20.7 billion to cybercrime last year.

This threat is why Texas Tech Information Technology (IT) formally launched the Safe Computing Practices Campaign in spring 2004, well before many other businesses and universities across the nation created similar programs, Segran said.

When October was dedicated as National Cyber Security Awareness Month (NCSAM) in 2005, he said they saw an opportunity to leverage the federal program and enhance their campaign with local events, activities and speakers, and the partnership continues this month.

The campaign originally started with safety tips in the IT Division Bulletin, which have evolved from talking about floppy disks to now putting information on social networking safety and emerging threats. Segran said the goal is to always keep the information current and relevant.

Cyber security dates back to before many of the students at Texas Tech University were even born. Starting in the ’80s, hackers ran small scams more for fun and prestige than anything else. In the ’90s, motivations turned from mischief to money, and with the advent of the World Wide Web, cybercrime exploded.

“The tools have changed, the people have changed, but the danger is still there,” Segran said.

Other efforts in NCSAM include spring cleaning for electronic data and holding Shred Days on campus. At the first Shred Day in April 2008, the Texas Tech community shredded nearly 8,000 pounds of paper. That amount has grown every year, and in 2011, almost 86,000 total pounds were shredded during two Shred Days.

In addition to Shred Day, this year’s programs for NCSAM include Cyber Security Awareness 101 on Oct. 10. This “lunch and learn” will cover the most common threats, scams and unsafe habits. Attendees will learn the basics of cyber security, while reaping the benefits of technology.

IT also will host three sessions on how to manage your online reputation on Oct. 18, 23 and 30. These discussions will cover what and what not to do online to protect your reputation and how to make a good impression online for a prospective employer, scholarship committee and many others.

Cyber security has become a lifestyle issue with how people live with technology all around them, Segran said. The hard distinctions between work-related and personal use with social networks are getting harder to distinguish.

“Safe computing behavior that is good for the university is also good for personal habits and vice versa,” he said. “When we teach employees about strong passwords and other good online practices, it protects them at home as well. We’re trying to raise the overall level of cyber security knowledge.”

Cyber security is a constant issue on campus, and IT is always looking to increase the preventative measures and controls in place to protect the university, faculty, staff and students. Segran said they have a general four-part strategy to improve cyber security at Texas Tech:

- Make systems less vulnerable
- Provide services and resources to protect data and infrastructure
- Educate the campus community
- Block cyber-attacks when they occur

In 2011, IT blocked 761,086 attacks and detected and fixed 2,179 issues. They also conducted hundreds of hours of training to thousands of participants.

(Continued...)
Cybersecurity begins with STOP THINK CONNECT. These three simple steps are the starting point for staying safer and more secure online.

STOP: Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your online actions could impact your safety or your family’s.

CONNECT: Enjoy the Internet with greater confidence, knowing you’ve taken the right steps to safeguard yourself and your computer.

- National Cyber Security Alliance, 2012

Password safety suggestions:

- Use different strong passwords for critical accounts, such as banking, credit, or investment accounts. You should not use your eRaider password for any other accounts other than eRaider.
- If you need to write down your passwords to remember them, write down a clue that will help you remember, but will be meaningless and undecipherable to others.

Suggestions for creating a strong password:

- Start with a sentence or phrase that is meaningful to you, but not a common sentence or phrase;
- Change the words into “shorthand” and/or intentionally misspell a word;
- Replace letters with numbers and/or symbols;
- Add length with additional numbers and/or symbols; and
- Be consistent in the scheme so you will remember it each time you create a new password/account.

The protection is extended beyond just the campus borders. IT has partnered with many area organizations including the Lubbock Chamber of Commerce to provide educational presentations to help promote safe computing practices to Lubbock and surrounding communities.

The university has official operating policies that outline the guidelines on dealing with data and information. To help employees, IT makes cyber security education a priority in its strategy to protect the campus community.

“The university can only do so many things to protect people, but ultimately, people have a huge responsibility,” Segran said. “How faculty and staff handle confidential and/or sensitive data is no longer a technology issue. At that point, it’s a people issue.”

Segran said there are several basic safety tips to protect yourself online, including:

- Set strong passwords
- Make password security questions harder to guess
- Keep your systems and software up to date
- Be careful what websites you visit and emails you open
- Delete old apps off your smartphone
- Wipe data from devices that are no longer used

IT also provides a safe computing website for the campus and Lubbock communities with information about best practices, threats and other educational materials.

 Contributors by: Katherine Austin Beltz Ph. D., James Hodging, Britta Tye and Kyle Parker.
Safe Computing Practices Committee: Sam Segran, Katherine Austin Beltz, Ph.D., Jeff Barrington, Darrell Bateman, Shannon Cepica, Scott Hall, Danny Mar, Ron Nail, Yung Ng, Randall Osborne, Mike Simmons, Phil Smith, Ph.D., J Stalcup, Britta Tye, John Vandygriff, Allen Young, and assistance from other IT Division leadership.

Printed with permission from James Hodgins, Section Coordinator of Internal Communications, Communications & Marketing, TTU. Originally published in RaiderWire October 2, 2012.