Message from TTU Chief Information Officer

Over the last few years there have been significant increases in worms, viruses, and hacking activities. The IT Division has a number of initiatives underway to address these issues. These initiatives include hardening the computing infrastructure, site licenses that allow the use of the latest versions of Windows and anti-virus software, and work in progress for a desktop management solution that could be extended to departments on campus. An important initiative is to provide IT information, especially tips on SAFE COMPUTING PRACTICES, to the University community. Our current communication methods to reach the University community are all electronic - Employee TechAnnounce, Student TechAnnounce, NSC/NSS mailing lists, and direct e-mails to TTU Administrators. We hope to use this bulletin as another way to communicate with the University community.

-Sam Segran
TTU Chief Information Officer

TTUnet Wireless

In 2002, the TTU IT Division applied for TIF grants to fund a Wireless (WiFi) Ethernet project at Texas Tech University. We received the funding in FY03. This grant provided the starter funds to begin the Campus Wireless Project for most of the academic buildings and some support buildings on the Lubbock campus.

WiFi will provide convenience and mobility to the TTU community. However, WiFi is not a replacement for desktop machines or labs. Students, faculty, and staff using wireless laptops at home and on TTU campus should be able to move easily between TTUnet wireless and other off-campus wireless locations.

The primary devices supported on the WiFi network are laptops and handheld devices through a secure and encrypted method using eRaider authentication and 802.1x security standard. Proper operation and security must be maintained on the WiFi network; therefore, no other wireless networks may be run on campus.

We understand that certain locations may have specialized needs for WiFi access, such as research areas and special applications. If you have a special WiFi need, please contact Carlos Casarez at 742-1648. WiFi access for special conferences and events can also be arranged. When making WiFi setup requests for such events, please allow at least five business days prior to the event date.

A list of buildings with WiFi capability (or work in progress) and connection instructions is listed at http://www.helpdesk.ttu.edu/general/wireless.php. For more information on the WiFi project please call the Network Operations Center at 742-4858.
Safe Computing Practices

Computing environments worldwide have changed drastically over the past year as a result of the continuous barrage of hacking attempts, viruses, and worms such as Blaster and Sasser. In the current environment, the breach of one PC by a worm or a hacker negatively impacts the usability and operations of other computers in the same network. The loss of data and productivity from each breach can range from serious to devastating to the user, depending on each incident.

Each computer must be protected to prevent outbound and inbound attacks. Safe computing practices at the desktop level are integral in ensuring stable network connectivity and productive computing on the part of the user. Three key elements to safe computing are discussed in the following articles.

Windows Critical Updates and Service Packs

All operating systems (OS) are subject to attacks due to unforeseen vulnerabilities, and the manufacturers, such as Microsoft, will release a critical update once they learn of the vulnerability. To ensure that patches and OS service packs are installed on your computer as soon as available, you should enable Automatic Windows Updates, and periodically visit http://windowsupdate.microsoft.com to install non-critical updates and Microsoft Office updates. It is also highly recommended that all Windows machines be upgraded to the latest version of OS available (currently XP). Because of the Microsoft Campus Agreement in place, Windows XP is available for free to the University community.

Password Security

- Use a combination of alpha and numeric characters.
- Use the computer-generated passwords given by eRaider.
- Do not use the same password on campus that you use for Yahoo!, Hotmail, or other off-campus log-ins.
- Change your password frequently (at least every 90 days).

Recommended E-mail Practices

Following the guidelines below will help reduce the chances of being a victim to identity theft, viruses, worms, and hackers:

- Never give out personal information, such as credit card numbers, routing numbers, or passwords, to untrusted or unknown sources.
- Do not open attachments from strangers or unsolicited attachments (including pictures). Depending on the type of worm/infection, even files from familiar e-mail addresses could be suspect.
- If you receive a suspicious e-mail, do not open it. Delete it.
- Recognize chain letters and scam e-mails, and do not forward them. Clues include big promises, prizes, high pressure tactics, and requests for money or help.
- Do not click on links on any of these e-mails. Such an action alone can cause you to get infected.
- If you are using the University's TechMail Server for your e-mail, turn on the SPAM filter feature on your Outlook 2003. Detailed instructions are available at: http://www.helpdesk.ttu.edu/general/O2K3JunkEmail.php

By following these guidelines, you can help to protect yourself and your computer from the dangers of today's computing environment. For more detailed information on safe computing, please visit www.helpdesk.ttu.edu/safecomputing; for specific questions, contact IT Help Central at 742-HELP.