Message From the CIO

The TTU Information Technology Division extends our best wishes for a safe, relaxing and festive holiday season to the University community. In this issue, we will focus on reminders and suggestions as you prepare for the holiday break. Remember that the holiday season is “prime time” for hackers and we must all be on guard and protect ourselves and our computers. In the January issue, we will review our accomplishments for 2007 and our goals for 2008.

Merry Christmas, Happy Holidays, Seasons Greetings, and Happy New Year!

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

The holiday photo above includes the TTU Office of the CIO Staff and IT senior management:

Front Row: Sam Segran, CIO; Shelly Walraven, Analyst II, TTU Office of the CIO; and Katherine Austin, Ph.D., Assistant Vice President, TTU Office of the CIO
Second Row: Philip Smith, Ph.D., Senior Director, High Performance Computer Center; Mary Scott, Senior Administrative Assistant, TTU Office of the CIO
Third Row: Vicki West, Managing Director, Institutional Research and Information Management; Kathleen Burrell, J.D., Education Services Manager, Technology Support; Shannon Cepica, Managing Director, IT Help Central
Fourth Row: Adrienne Daniels, Administrative Assistant, TTU Office of the CIO; Darrell Bateman, Assistant Vice President, TTU Office of the CIO; Eric Burrell, Assistant Managing Director, IT Policy and Planning, TTU Office of the CIO
Back Row: J Stalcup, Managing Director, Telecommunications; Allen Young, Managing Director, Technology Support
Preparing for the Holiday Break

Preparing Office and Home Computers for the Holiday Break

Here are some steps to take to protect your office computer and home/mobile computer over the Holiday break:

Office computer:
• Update Windows XP to Service Pack 2 or higher. Visit www.windowsupdate.com and scan for updates.
• Update to the newest version of Norton AntiVirus by visiting www.eraider.ttu.edu, then use Norton’s Live Update feature to obtain the very latest Virus definition files.
• Turn off your office computer over the break.
• Enable password protection on all computers and handheld devices.
• Lock any mobile/handheld devices left in the office in a cabinet or other secure location.
• Check your e-mail periodically during the break to avoid going over the mailbox quota, which could prevent sending and receiving e-mails.

Home/Mobile computer:
• Update Windows XP to Service Pack 2 or higher. Visit www.windowsupdate.com and scan for updates. If you are using a dial-up connection, you may contact IT Help Central to obtain a CD of the latest patches.
• Download all Windows OS and Microsoft Office Critical Updates at www.windowsupdate.com and www.officeupdate.com
• Set Windows to update automatically during times the computer is on and has Internet access.
• Set your AntiVirus to update automatically. For those with Symantec AntiVirus:
  ◦ Right mouse select the Norton Shield in the lower right hand corner of your screen.
  ◦ Select “Open Symantec Antivirus” and go to “File”, then “Schedule Updates”, and a pop-up box will appear with “Enable scheduled updates”. The selected text box below shows the schedule.
  ◦ To modify these settings, select the “Schedule” button and change the frequency to daily; be sure to select a time when the computer is on and has Internet access.
  ◦ To finish, select “OK” through all the dialog boxes and close Symantec Antivirus Console.
• Connect your PC to the Internet periodically during the Holiday break to obtain OS patches and update Norton’s virus definitions.
• Ensure that your PC is physically secure from theft while in hotels, airports, or traveling. Do not leave computing equipment in unattended vehicles.

When you return from the holiday break, we recommend:
1. Obtain Windows updates at www.windowsupdate.com
2. Run Norton LiveUpdate; then scan your computer
3. Obtain Office updates at www.officeupdate.com
4. Clean out your e-mail inbox and junk mail folder.

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

Preparing for the Holiday Break: Your eRaider Password

Changing your eRaider password before the break can save you time and effort upon your return. eRaider passwords expire every 90 days. If you last changed your password in September, it will likely expire over the Christmas break. To prevent login issues when you return in January, the TTU IT Division recommends you change your eRaider password before leaving for the semester.

Instructions for changing your eRaider password:
1. Navigate to http://eraider.ttu.edu
2. Sign in with your eRaider credentials, then click the “Manage your eRaider Account” link.
3. Click the “eRaider Password” link in the left column.
4. Enter a new password, or select a randomly generated password, then click the “Set Password” button.
5. You will now see a message asking you to confirm your password change. Click the “Set Password” to change your eRaider password.
6. You will see a verification message next, indicating that your password has been accepted. At this time, you may close the eRaider account manager.

Your new password should take effect within about 5 minutes.

Please note that if your password has expired, you can still set a new one from the eRaider website. Simply sign in with your eRaider username and old password, and the system will prompt you to set a new password.

IT Help Central will be glad to assist you with any questions or concerns you may have regarding your eRaider account. You may contact them at (806) 742-HELP (4357) or ithelpdesk@ttu.edu.

Consumer Beware: ‘Tis the Season for Hackers

The holiday season is a prime time for hackers to attack computer systems and prey on Internet shoppers. Hacking tools have become so sophisticated, allowing anyone with an interest to build and deploy malicious tools. Beware that December is a target time for identity theft ploys. Hackers take advantage of the increase in online shopping and the stress of the season. We strongly suggest that you be vigilant in protecting your personal information, especially when purchasing online:
• Shop online with established, reputable vendors;
• Read the privacy and security statements before purchasing with a store online;
• Use a credit card when purchasing online; credit card companies are prepared to assist you in disputing any fraudulent charges;
• Do not enter your personal information in a “pop-up” screen;
• Make sure that the online transaction page is secure – look for “https:” on the address line in your browser;
• Keep records of your online purchases;
• Be wary of any unsolicited holiday specials or deals; and
• Contact the store immediately if you experience problems with your order.

We also suggest that you be very careful about purchasing gifts from online auction sites, such as eBay. Carefully inspect all information posted about merchandise on these sites. Enjoy the convenience of online shopping, but be careful to practice safe computing!

Contributions by: Katherine Austin, Ph.D., Lisa Mills, Ric Ramon, Josh Humphreys, and Troy Watson.
Safe Computing Practices Committee: Sam Segran, Katherine Austin, Ph.D., Darrell Bateman, Eric Burrell, Kathleen Burrell, J.D., Tony Castle, Shannon Cepica, Scott Hall, Alvin Mills, J Stalcup, Allen Young, and assistance from IT Division leadership and staff.

Information Technology Division

Mail Stop 2008
Phone: 742-5151
Fax: 742-5155

IT Web Site: http://www.infotech.ttu.edu
Texas Tech University Web Site: http://www.ttu.edu
Computer-Based Training (CBT): http://cbt.ttu.edu
Laws and Texas Tech Policies: http://www.itts.ttu.edu/documentation/laws