Message from the CIO

Seasons greetings to the TTU community! In preparation for the holiday break, we have prepared a special issue to address two timely topics: guidelines for shopping online and special safe computing tips for your work and home computing systems. As we depart to enjoy the festivities of the holiday season, remember that November and December are "prime-time" for hacker activity. Verisign, a trusted digital certificate authority, reports that hacker attempts increased by 176% during November and December 2003, compared to the previous year during the same time period (http://www.itfacts.biz/index.php?id=P691). Given the increase in hacker tools and creativity in the last year, I anticipate a larger increase in security threats this year. While we wish you a restful holiday break, we also encourage you to exercise safe computing practices.

The holiday photo above includes the TTU Office of the CIO staff and my senior management team:

**Standing:**
- Dr. Phil Smith, Senior Director - High Performance Computing Center;
- Eric Burrell, IT Policies and Planning Officer - TTU Office of the CIO;
- Sam Segran, Associate Vice President for IT and CIO;
- Darrell Bateman, Managing Director - Technology Assessment;
- J Stalcup, Managing Director - Telecommunications;
- Vickie Gustafson, Assistant Vice President for IT Customer Support;
- Scott Hall, Managing Director - IT Help Central;
- Kathy Stalcup, Managing Director - Technology Support

**Seated:**
- Vicki West, Managing Director - Institutional Research and Information Management;
- Lori Hefley, IT Event and Education Coordinator - Technology Support;
- Cynthia Cantu, Administrative Assistant - TTU Office of the CIO;
- Mary Scott, Senior Administrative Assistant - TTU Office of the CIO

Happy New Year!

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

Contributions by: Vickie Gustafson, Katherine Stalcup, Lori Hefley, Joshua Harrison, Edie Temple, Ray Espinoza, Amy Boren, Jamie Adie, J Stalcup, Carlene Van Stone, and Scott Hall.
Safe Computing Practices Committee: Vickie Gustafson, Katherine Stalcup, Scott Hall, J Stalcup, Brandi Anderson, Eric Burrell, Lori Hefley, Tony Castle, Darrell Bateman, Lori Gibler, with assistance from IT Division Directors and other staff.
The National Fraud Information Center (http://www.fraud.org) reports that 19% of all Internet fraud from January to June of 2004 occurred with general merchandise purchases. Texas ranked the third highest location in the United States for fraud victims, with 6% of Internet fraud victims reporting Texas residency. In terms of victim age, 73% were 20-49 and 16% were 50-59. These statistics are a stark reminder that hackers and Internet criminals target all online shoppers; no one profile can be described as high-risk group. We recommend the following online shopping practices:

### The Smart Shopper: Recommended Practices for Online Shopping

- **Know the seller** - Before buying online, investigate the company! We suggest that you obtain a physical address and phone number. For large purchases, check with the Better Business Bureau for information concerning any prior complaints.

- **Know the terms and conditions** - Carefully review the product return information and read the fine print. Evaluate the process for damaged or unwanted merchandise. Obtain all product details and purchase arrangements before ordering. For instance, know the total price, tax, delivery time, shipping charges, and order tracking procedures.

- **Use a credit card** - The Federal Trade Commission suggests that, "If you pay by credit or charge card online, your transaction will be protected by the Fair Credit Billing Act. Under this law, you have the right to dispute charges under certain circumstances and temporarily withhold payment while the creditor is investigating them. In the event of unauthorized use of your credit or charge card, you generally would be held liable only for the first $50 in charges. Some companies offer an online shopping guarantee that ensures you will not be held responsible for any unauthorized charges made online, and some cards may provide additional warranty, return and/or purchase protection benefits.”

- **Shop at secure e-commerce sites** - Look for company security and privacy statements and guarantees; read them carefully. When you are in an order form or shopping cart, review the Internet address and make sure that it begins with “https://” or “shttp://”, which indicates a scrambled.

- **Use secure passwords** - Most online retailers require you to create an account with the company and provide your own password to access your account and order information. Use the recommended tips for password creation: use an alpha-numeric combination, avoid words contained in the dictionary, and use at least nine characters. We strongly suggest that you avoid using personal information (birthday, social security number, TTU eRaider account passwords, pet names, etc.).

- **Keep records** - Print the order confirmation and purchase order; file with your financial records for future reference. Most online companies guarantee delivery within thirty days; mark your calendar and check on your order periodically.

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

**Office computer:**
- 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 locking file cabinet or other secure location.
- Check your e-mail periodically during the break to avoid going over the mailbox quota, which will prevent sending and receiving e-mails.

**Home/mobile computer:**
- Update Windows XP to Service Pack 2. Visit www.windowsupdate.com and scan for updates. If using a dial-up connection, contact IT Help Central to obtain a CD of the latest patches.
- Set Windows to update automatically during times the computer is on and has Internet access.
- To modify Norton AntiVirus to update automatically on a daily basis, right mouse click the Norton Shield in the lower right corner of your screen. Select “Open Symantec AntiVirus,” go to “File,” then “Schedule Updates.” A pop-up box will appear with “Enable scheduled automatic updates.” The selected text box shows the schedule. To modify, 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” on 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 your PC is secure from theft while traveling or in hotels and airports. 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

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