Message From the CIO

The Information Technology Division wishes the University community a happy and healthy holiday season. We extend our warmest wishes for the season. In this issue, we have included online shopping tips for consumers from the National Consumers League, the National Cyber Security Alliance, and the Better Business Bureau. While you are looking for gifts online, hackers are looking for their next victim; be aware and be safe!

Remember to be vigilant during this “prime-time” for computer related criminal activity and practice safe computing.

Merry Christmas, Happy Holidays, 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 my senior management team:

Standing: Mary Scott, Senior Administrative Assistant; Eric Burrell, IT Policies and Planning Officer; Whitney Norman, Analyst II; Sam Segran, Chief Information Officer; Katherine Austin, Ph.D., Assistant Vice President; Dr. Phil Smith, Senior Director - High Performance Computing; Shannon Cepica, Managing Director - IT Help Central; Vicki West, Managing Director - Institutional Research and Information Management.

Seated: J Stalcup, Managing Director - Telecommunications; Darrell Bateman, Managing Director - Technology Assessment; Lori Dudley, Coordinator, Divisional Events and Training - Technology Support.

Texas Tech University
Office of the Chief Information Officer

Contributions by: Katherine Austin Ph.D., Lori Dudley, Joshua Harrison, Tiffany Naylor, Amy Boren, and Carlene Van Stone.
Safe Computing Practices Committee: Katherine Austin Ph.D., Shannon Cepica, J Stalcup, Darrell Bateman, Scott Hall, Eric Burrell, Lori Dudley, Tony Castle, and assistance from IT Division Directors and other staff.
SHOPPING ONLINE FOR THE HOLIDAYS:
TWELVE TIPS TO PROTECT YOURSELF FROM
CYBER GRINCHES, SCAMS AND SCHEMES

The National Consumers League, the National Cyber Security Alliance and the Better Business Bureau Provide Joint Advice on Safe Online Shopping Do’s and Don’ts

Media Contact:
National Cyber Security Alliance:
Julie Han, 415-975-3327
jhan@porternovelli.com

WASHINGTON, DC –November 17, 2005

The holiday season is a busy time as people hunt for the perfect gifts for family and friends. The Internet can make your shopping faster and easier, but there can also be pitfalls if you’re not careful. The National Consumers League, the Better Business Bureau and the National Cyber Security Alliance offer key advice to ensure you have a safe online shopping experience, so that your gift-giving is a joyous occasion, not an opportunity for cyber thieves:

1. **Know who you’re dealing with.**
   Check out unfamiliar sellers with the Better Business Bureau and your state or local consumer protection agency. If you’re buying gifts on an online auction site that provides a feedback forum, check the track record of the seller before you bid. Don’t buy things in response to unsolicited e-mails from unknown companies, since these may be fraudulent.

2. **Get all the details.**
   Get the name and physical address of the seller; how much the product or service costs; what is included for that price; whether there are shipping charges; the delivery time, if any; the seller’s privacy policy; and the cancellation and return policy.

3. **Look for signs that online purchases are secure.**
   At the point that you are providing your payment information, the beginning of the Web site address should change from http to shttp or https, indicating that the information is being encrypted – turned into code that can only be read by the seller. Your browser may also signal that the information is secure with a symbol, such as a broken key that becomes whole or a padlock that closes.

4. **Pay the safest way.**
   It’s best to use a credit card, especially when you’re purchasing something that will be delivered later, because under federal law you can dispute the charges if you don’t get what you were promised. You also have dispute rights if there are unauthorized charges on your credit card, and many card issues have “zero liability” policies under which you pay nothing if someone steals your credit card number and uses it.

5. **Never enter your personal information in a pop-up screen.**
   When you visit a company’s Web site, an unauthorized pop-up screen created by an identity thief could appear, with blanks for your personal information. Legitimate companies don’t ask for personal information via pop-up screens. Install pop-up blocking software to avoid this type of scam.

6. **Keep documentation of your order.**
   When you’ve completed the online order process, there may be a final confirmation page and/or you might receive confirmation by e-mail. Print that information and keep it handy in case you need it later.

7. **Know your rights.**
   Federal law requires orders made by mail, phone or online to be shipped by the date promised or, if no delivery time was stated, within 30 days. If the goods aren’t shipped on time, you can cancel and demand a refund. There is no general three-day cancellation right, but you do have the right to reject merchandise if it’s defective or was misrepresented. Otherwise, it’s the company’s policies that determine if you can cancel the purchase and whether you can get a refund or credit.

8. **Be suspicious if someone contacts you unexpectedly and asks for your personal information.**
   Identity thieves send out bogus e-mails about problems with consumers’ accounts to lure them into providing their personal information. Legitimate companies don’t operate that way.

9. **Check your credit card and bank statements carefully.**
   Notify the bank immediately if there are unauthorized charges on your credit card, and many card issues have “zero liability” policies under which you pay nothing if someone steals your credit card number and uses it.

10. **Keep your computer secure for safe shopping and other online activities.**
    Protect your computer with spam filters, anti-virus and anti-spyware software, and a firewall, and keep them up to date. Go to http://www.staysafeonline.org and http://www.onguardonline.gov/ to learn more about how to keep your computer secure.

11. **Beware of e-mails offering loans or credit, even if you have credit problems.**
    Con artists take advantage of cash-strapped consumers during the holidays to offer personal loans or credit cards for a fee upfront. These scammers simply take the money and run.

12. **Contact the seller promptly about any problems with your order.**
    Check the company’s Web site for a customer service page, “contact us” link, e-mail address, or phone number to get your complaint addressed or questions answered. If you can’t resolve the problem, contact the Better Business Bureau or your state or local consumer protection agency for help.