vol.1 no.7 | January 2005

Information Technology Division | Bulletin

from the office of the CIO Texas Tech University

Looking to the Future

Message from the CIO

Happy New Year! The IT Division is planning for another productive spring semester. As we dust off the tinsel and locate our winter socks, we are preparing for a new semester full of activities and opportunities. In this issue, we are unveiling a new feature of our bulletin; we will highlight and recognize one of our **University IT partners.** Integrating technology to facilitate the mission and strategic plan of the University is a team effort, and we want to recognize those hard-working groups. As we evaluate our personal new year's resolutions, I encourage you to review the **educational opportunities** article and select an event to enhance your technology skills. For instance, we will be hosting a **lab security roundtable** on February 9th (details provided in article). For those that received or purchased a new computer system over the holiday period, the **safe computing tips** offer guidance for preparing your new computer system and connecting to the University network. For those who enjoy monitoring trends and facts, we included a few **2004 cyberfacts** for you to review. The IT Division wishes you a new year full of prosperity, productivity, and secure computing.

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

2004 Year in Review: CyberFacts

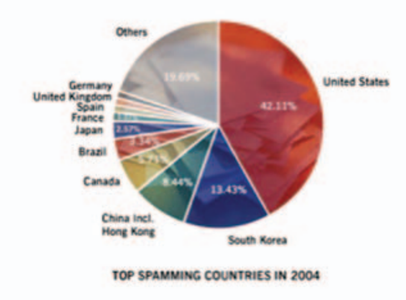
McAfee (2005) reports the following threats caused the most destruction and damage to consumers in 2004:

- Adware-180
- Adware-Gator
- Exploit-ByteVerify
- Exploit-MhtRedir
- JS/Noclose
- W32/Bagle
- W32/Mydoom
- W32/Netsky
- W32/Sasser
- W32/Sdbot (family including sdbot, gaobot, polybot, spybot)

"NetworkAdministrator.com" lists the top ten most common Spyware programs found in 2004:

- GAIN (commonly know as Gator)
- Claria
- GameSpy Arcade
- Hotbar
- Ezula
- BonziBuddy
- WeatherCast
- LinkGrabber 99
- TOPicks
- Cydoor

Sophos (2004) reports the United States continues to lead the world in spamming volume:



TOP SPAMMING COUNTRIES IN 2004

Hacking: A Means to What End?

In the last year, most of the University community has been either directly or indirectly impacted by the work of a hacker. As with "traditional" crime, we reflect on the work, time, and money lost during a hacking episode or event. While no one can purport to fully understand the criminal mind, we can help you understand what hackers are attempting to achieve. Michael Bruck, BIA Security Consultant, suggests that "the first step to protecting yourself is to understand your enemy."

Hackers are typically motivated by one of the following:

- **Revenge**
  A disgruntled employee or former employee looking to hack information as an act of revenge.
- **Money**
  Either by stealing credit card or account information or by conducting an Internet-based scam, many hackers are simply trying to earn a dishonest living. Additionally, hackers are hired to destroy, cover, hide, and exploit for a fee.
- **Large scale disruption – the challenge**
  Within the hacker community, the larger the disruption; the greater the bragging rights. Interrupting network service and traffic (Denial of Service Attacks) is an enticing challenge for many hackers. Similarly, massive data destruction is the mark of a seasoned hacker, while viruses, worms, and Trojan horses may be the product of the 17-year-old next door! When a hacker successfully destroys data or commandeers a server, they will often leave a "signature" as evidence of their conquest. The signature may be an image or text and typically identifies them to the hacker community.
- **Non-monetary personal gain**
  Some hackers are motivated by non-monetary, personal gain, such as access to information or functions that will satisfy some need or desire.

TTU Community Spotlight: IT Partners

Teaching, Learning, and Technology Center

The Teaching, Learning, and Technology Center partners with the Information Technology Division to provide the University high quality technical consulting and training. Pictured above from left to right are: David Faulkner, Karissa Greathouse, Dr. Ed Anderson, Ranjini Suryanarayanan, Tony Rando, Karen Humphreys, Charlotte Patterson, Morgan Mercer, Tom Heisey, Tina Sansom, Jon Early, Mark Nix, Bala Srinivasan, and Sharon Robinson.

Education Opportunities to Enhance Your Technology Skills

The TTU IT Division offers a host of educational opportunities to the University community. We invite you to take advantage of the following training:

- **Technology Skills ShortCourses** – instructor-led, hands-on courses; morning, afternoon, and evening courses are offered. Course topics include computing practices and guidelines, electronic mail, graphics, Internet tools, Microsoft Office, SAS/SPSS, and Web development. We offer basic and advanced training. http://www.itts.ttu.edu/training/shortcourses/
- **Computer-Based Training (CBT)** – 340 self-paced, interactive, online courses are available. Courses include basic technology skills, advanced technology topics, and management skills. http://www.cbt.ttu.edu/
- **Roundtables and Forums** – As part of the Safe Computing Practices campaign, the IT Division will be hosting roundtable events to foster collaboration and information sharing. For the spring semester, we will offer two basic roundtables, aimed at security basics for lab management and identity theft. In addition, we will offer an advanced roundtable designed to facilitate discussion on advanced security topics for Network Site Coordinators and other interested parties.
- **Specialty System Training:**
  - **GIS** - For those interested in map creation and architectural modeling, we offer specialized training and assistance with ESRI, which is a geographical information system. For further information, you can contact Ray Espinoza at 742-1650.
  - **Degree Audit** training within TechSIS and **Student Evaluation of Course and Instructor** training. For more information please call 742-2166.

Mission Security: Safe Computing Roundtable

Computer Lab Security

As a part of the Safe Computing initiative, the TTU IT Division invites you to attend a roundtable discussion on February 9, 2005, from 2:00-3:30 pm. A panel of IT professionals will discuss essential lab security. The panelist will be:

- Katherine Stalcup, Technology Support
- Brandie Anderson, Telecommunications
- Lori Gibler, IT Help Central
- Danny Mar, IT Help Central
- Tim Wolf, Technology Support
- Allen Young, Technology Support

The roundtable is intended for those that have an interest in computing and research lab security.
In order to make the roundtable more convenient for the TTU community, we will be delivering the session to several TTUNet interactive video rooms.

We will have a panelist in each of the following locations:

- Advanced Technology Learning Center Room 31
- Business Administration Room 152
- Education Room 201
- Holden Hall Room 38

We look forward to a productive session that will address critical lab security issues.

SAFE Computing TIPS

Setting Up a New Computer System:

- Install the most current version of Operating System (e.g. Windows XP). Visit http://eraider.ttu.edu
- Ensure all critical updates and patches are installed before connecting to the Internet.
  - IT Help Central has a current critical update and patch CD available.
  - Set up Microsoft Windows Critical Updates to automatically install. Go to http://helpdesk.ttu.edu/safecomputing. Under the heading of "Recommendations" click on "Automatically Install Critical Updates in Windows 2000/XP."
- Install an Antivirus software - TTU IT Division provides Norton AntiVirus to the TTU community for download at no charge. Visit http://eraider.ttu.edu

Verify That Your TTU Windows Domain Account is Active:

- Go to http://eraider.ttu.edu and log in using your eRaider username and password.
- Click on the "Manage your eRaider Account" link.
- Under the "eRaider Account Manager" banner, there will be a section on the right titled "Windows Domain Account." In this section, verify that you have an entry named "TTU.EDU – Active" (has a small bright green circle next to it). If you do, your Windows Domain Account is active, and you can proceed to the next section.
- If you see a small, dark green circle and an entry named "TTU.EDU – Inactive," you will need to activate your domain account before continuing. To do this, click on the entry named "TTU.EDU – Inactive," A new screen will appear with simple instructions that will guide you through activating your account.
- Once you have followed the instructions on the screen, click on the "General Information" button on the left, and verify that your account now appears as "TTU.EDU – Active" (with a small, bright, green circle next to it in the "Windows Domain Account" section on the right side of the page).

For questions or assistance with any of the above information, please contact IT Help Central at 742-HELP(4357).

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. Brandie Anderson, Eric Burrell, Lori Hefley, Tony Castle, Darrell Bateman with assistance from IT Division Directors and other staff.

TEXAS TECH UNIVERSITY™
Information Technology Division
Mail Stop 2008
Phone: 742-5151
Fax: 742-5155

TTU IT Division 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.depts.ttu.edu/itts/documentation/laws

Past copies of TTU IT Division Bulletins may be found online at http://www.infotech.ttu.edu/itbulletin