Message from the CIO
IT security continues to be a major initiative for the TTU IT Division. Whether it is fighting e-mail intrusions or protecting information, our staff are constantly working to improve our IT security posture. In this issue, we summarize the recent Identity Theft Roundtable discussion that includes valuable information for all faculty, staff, and students. In our Safe Computing Tips section, Lt. Parker, Texas Tech Police Department, provides some simple tips to prevent identity theft, based on his experience in law enforcement. In addition to the junk mail strategies that we deploy centrally, we have also included an article highlighting strategies for further managing junk e-mail at your desktop. Effective strategic IT security plans require collaboration between the TTU IT Division and the TTU areas and units; we appreciate the partnerships that we have fostered here at Texas Tech University.

Sam Segran
Associate Vice President for IT and Chief Information Officer

Strategies for Junk Mail Filtering
TechMail, the TTU e-mail service, provides sophisticated levels of filtering to all customers. When an individual outside TTU sends e-mail to a TTU individual using TechMail, the filter evaluates each messages for recognizable spam patterns and assigns the message a rating based on the probability that the message is unsolicited commercial e-mail or spam. This rating is called the Spam Confidence Level (SCL). Messages scored 0-2 will be delivered to the recipient's inbox; those scored 3-7 will be deliver to the recipient's junk e-mail folder; and those scored 8 and 9 are refused and returned to the sender. In addition to this automatic filtering, TechMail offers customer-managed filtering options at the client level to help manage unwanted and unsolicited e-mail.

General recommendations for customer-managed TechMail junk e-mail filtering:

- **Enable filtering through Outlook Web Access (OWA)** at [http://mail.ttu.edu](http://mail.ttu.edu) by choosing “Options” and then selecting “Filter Junk E-mail” and “Save”. This step must be completed in order for junk messages to be filtered to your Junk E-mail folder.
  - Outlook Clients: If you have enabled filtering in OWA, then your Outlook junk e-mail lists will automatically synchronize with OWA. Once enabled, there is no additional management necessary through OWA.
  - Non-Outlook Clients (including some data devices): Depending on your client, you may need to manage your junk e-mail lists through OWA to control unwanted and unsolicited messages.

- **Enable Outlook client-side filtering** by going to “Tools,” then choose “Options,” click on the “Preferences” tab, and click on the “Junk E-mail” button, select your choices, and click “OK.”
  - Microsoft Outlook (2003 and 2007) offers four levels of junk e-mail filtering: None, Low, High, and Safe List Only. Select “Safe List Only” for the highest level of filtering available in both server-side and client-side processing. For detailed instructions, please visit [http://www.depts.ttu.edu/helpcentral/info/antispam.php](http://www.depts.ttu.edu/helpcentral/info/antispam.php).
  - Enable International top-level domain blocking in Outlook (visit the address above for detailed instructions).

- **Manage your Junk E-mail Lists** - Safe Senders, Safe Recipients, and Blocked Senders.
  - Lists can be managed by choosing “Options” in the Outlook web client (OWA – [http://mail.ttu.edu](http://mail.ttu.edu)) or from within your Outlook client.
  - For spam delivered to your TechMail Inbox, right click on the message, select “Junk E-mail”, and “Add Sender to Blocked Senders List”.

- For legitimate messages delivered to Junk E-mail folder, right click on the message, select “Junk E-mail”, and “Add Sender to Safe Senders List”.
- Add the domains commonly used by spammers (such as paypal.com and chasebanking.com) to your Blocked Senders list.
- Consider carefully which e-mail addresses/domains you add to your Safe Senders list. Adding the ttu.edu domain to your list may seem like a good idea, but this will also allow e-mails with “spoofed” ttu.edu addresses to reach your inbox. TechMail is configured so mail sent from within the TechMail system itself will not be filtered into your junk e-mail folder; adding the ttu.edu domain to your safe senders list is not necessary. Also, please be aware that e-mails from some TTU systems, such as HR Express, ePO, and Lyris are sent from non-TechMail and could possibly filter to junk e-mail depending on your filtering levels (These addresses should be explicitly added to your Safe Senders List).

IT Help Central will be glad to assist with your TechMail Junk e-mail settings. Instructions for setting up your spam filters are available at [http://www.depts.ttu.edu/helpcentral/info/antispam.php](http://www.depts.ttu.edu/helpcentral/info/antispam.php). If you have any questions or need additional assistance, please contact IT Help Central at 806-742-HELP (4357).

Currently Enrolled Student Survey is on the way
It is survey time at Institutional Research & Information Management! But, then again, it’s always that time of year at IRIM! Look for the Currently Enrolled Student Survey where students can give feedback regarding their academic department, Student Business Services, Financial Aid, Parking Services and many other administrative units -- even I.T.

This survey has been conducted every fall for the last seven years. It is sent to all students enrolled for the fall semester. Past results for this survey and others appear on the IRIM website [http://www.irs.ttu.edu/](http://www.irs.ttu.edu/) in the Data Warehouse. Sign in and look for “Surveys on the Web.” If there is something you need to know, we probably already have some information for you, but we are always happy to work with you to explore new areas of opinion research. For more information, please contact IRIM staff at 806-742-2166.
Your Identity. . . Priceless
On September 19, 2007, the TTU Office of the CIO hosted a roundtable discussion on identity theft. We received positive feedback on the event, as well as several requests to share the information that our guest panelists presented. We have posted the full presentation at http://www.safecomputing.ttu.edu. After you sign-in with your eRaider account, click on “Event Educational Materials.” For your convenience, this article highlights some of the key information.

Magnitude of the Problem
Dr. Katherine Austin and Mr. Alvin Mills provided details on the scope and severity of identity theft in the United States. Referencing the National Criminal Justice Reference Service (2007) and the Federal Trade Commission (2006), they presented some startling statistics:

- “Electronic Fund Transfer” related identity theft was the most frequently reported type of identity theft bank fraud during calendar year 2006.
- In 2004, approx. 3.6 million U.S. households were victimized by identity theft. According to federal authorities, 10 million citizens were victimized in 2006.
- Total consumer loss was $1.1 billion dollars in 2006 (approximately $500 per customer).
- About 1 in 6 victimized households had to pay higher interest rates as the result of identity theft, and 1 in 9 households were denied phone or utility service.

In addition, the Better Business Bureau (2007) has identified the top 10 ways that your personal information is obtained: lost/stolen wallet, checkbook, or credit card; friends/acquaintances/relatives; corrupt employees; online transactions; stolen paper mail/fraudulent change of address; computer spyware; garbage can; online transactions; computer viruses/hackers; and e-mail.

Legal Process
Lt. David Parker discussed common identity theft scams and discussed the Texas Tech Police Department’s active involvement in identity theft cases. Lt. Parker noted that Medicare-approved drug discount cards as the latest ploy that he has experienced. Typically, the criminals contact elderly citizens through the telephone, e-mail, or door-to-door contact. After obtaining the individual’s Social Security Number under the guise of submitting a drug card approval application, the information is used for identity theft crimes and Medicare fraud crimes. Lt. Parker encouraged everyone to check their credit reports and be sure to report any suspected fraud to the following authorities:

- Equifax (www.equifax.com)
- Experian (www.experian.com)
- Trans Union (www.tuc.com)

Financial Institution Perspective
Ellen Hein, Manager of the Texas Tech Federal Credit Union, discussed the responsibility of financial institutions to protect customer information. She outlined information protection guidelines expressed in the Graham Leach Bliley Act (1999), the Bank Secrecy Act, (1970), the USA Patriot Act (2001), and the Fair and Accurate Credit Transactions Act (FACT, 2003). For instance, Ms. Hein highlighted the primary results of the 2003 FACT legislation: required merchants to delete all but the last five digits of a credit card number on store receipts; created a national system of fraud detections so that consumers could issue a nationwide alert with one phone call; and granted consumers the right to receive one free credit report per year from each of the nationwide credit reporting agencies. Ms. Hein also recommended “opting-out” of pre-screened credit card offers by contacting 1-888-567-8688 (reaches all three credit bureaus).

One clear message emerged: your identity is priceless and valuable! Given the attendance and positive feedback we received, the TTU IT Division plans to host another identity theft roundtable discussion in the next year.

Identity Theft Prevention Tips
Provided by Lieutenant David Parker, Texas Tech Police Department

- Destroy credit card applications, receipts, bank and billing statements;
- Avoid giving your SSN unless it’s absolutely necessary – use other identifiers;
- Pay attention to billing cycles;
- Guard your postal mail from theft;
- Put passwords on credit card, bank, and phone accounts;
- Carry as little identification information as possible;
- Limit the number of credit cards you carry;
- Don’t give personal identification on the phone unless you initiate the call;
- Be cautious storing and managing your personal information at home;
- Check on who has access to your personal information at work;
- Don’t carry your Social Security card;
- Save ATM and credit card receipts to check against statements;
- Be informed about your financial institutions’ policies of sharing information; and
- Make sure your credit reports are accurate.

For additional safe computing information, please visit http://safecomputing.ttu.edu.

Contributions by: Katherine Austin, Ph.D., Alvin Mills, Lt. David Parker, Ellen Hein, Vicki West, Ric Ramon and Jake Reed.
Safe Computing Practices Committee: Sam Segran, Katherine Austin, Ph.D., Darrell Bateman, Eric Burrell, Kathleen Burrell, J.D., Tony Castle, Shannon Codics, 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

Past copies of TTU IT Division Bulletins may be found online at http://www.infotech.ttu.edu/itbulletin
Copyright 2007 Texas Tech University