Message from the CIO

Summer is here, complete with vacations, hot weather, mosquitoes, barbeques, and Independence Day! Just as you use sunscreen to protect your skin from harmful sun rays, we encourage you to practice safe computing to protect your data, as you enjoy the summer months. Our bulletin this month provides information on keeping your mobile device secure, understanding the importance of “Patch Tuesday,” and protecting your identity while traveling. In addition, we also provide the campus with results from our spring Shred Day, accompanied by an article on wise shredding practices. We wish you a safe and fun summer, free from worms, viruses, and hackers!

-Sam Segran

Associate Vice President for IT and Chief Information Officer

“Bits” of Wisdom About Shredding

The TTU Office of the CIO, in partnership with the University Archivist and the Office of Records Management, sponsors Shred Day to encourage the campus community to shred unneeded confidential documents. Such practices promote information security and also contribute to a greener TTU.

The area businesses that provide shredding services at Shred Day use cross-cut or confetti-cut shredders. Cross-cut shredders have multiple shredding drums rotating in different directions, making a cutting pattern virtually impossible to reconstruct. As such, cross-cut shredding is a more secure alternative to traditional straight line shredding, because straight line shredded material can be reassembled with enough time, attention, and diligence.

If you are considering purchasing a shredder, be sure to check the type of shredding the unit performs prior to purchasing. Besides cross-cut shredders, other reliable shredding methods include: particle-cut; grinders; disintegrators; hammermills; and pierce-and-tear shredders. Each of these methods is a more secure shredding solution, compared to straight line shredding.

Before shredding TTU documents, please review the TTU Records Retention schedule at www.swco.ttu.edu/recordsmanagement/home.htm. University retention policy applies to the official “Master” copy. Note that Master document disposal requires the completion of a disposition log (see previous web address).

For additional information regarding TTU document retention policies and guidelines, please contact University Archivist Lynn Whitfield at (806)742-8675.

Keeping Your Mobile Device Secure

Mobile technology is rapidly developing, providing convenience and connectivity inherent in computing on-the-go. The TTU IT Division reminds you, that just as your desktop personal computer (PC) can be infected and overrun by malicious intruders, so can your mobile devices. Awareness of what you are doing and where you are visiting, as well as using safe computing practices, can help protect mobile device activity.

Many mobile devices offer services beyond making phone calls, texting, and receiving e-mail. With such a wide variety of mobile devices and options for connectivity, we strongly recommend that you exercise caution and be diligent about practicing safe computing. The United States Computer Emergency Readiness Team (US-CERT) recommends the following best practices to help protect mobile devices:

- Enable the personal identification number (PIN) or password to access the mobile device, if available;
- Encrypt personal and sensitive data, when possible;
- Disable features not currently in use such as Bluetooth, infrared, or Wi-Fi;
- Set Bluetooth-enabled devices to “non-discoverable,” so that unauthenticated devices cannot detect them;
- Use caution when opening e-mail and text message attachments;
- Use caution when clicking links contained in text messages and e-mail;
- Avoid opening files, clicking links, or calling numbers contained in unsolicited e-mail or text messages;
- Avoid joining unknown Wi-Fi networks;
- Delete all information stored in a device prior to discarding it; and
- Maintain situational awareness regarding mobile device threats.

Antivirus software exists for some mobile devices; however, it can only assist in protecting against known threats. We are all responsible for understanding the threats and proactively taking steps to avoid them. A high degree of vigilance is necessary to successfully prevent and mitigate future threats to mobile devices.

If you need assistance or would like more information, please contact IT Help Central at (806)742-HELP (4357) or via e-mail at ithelpcentral@ttu.edu.

Understanding “Patch Tuesday”

“Patch Tuesday” is the second Tuesday of each month when Microsoft releases updates or “patches” for Microsoft products, such as Windows operating systems and Microsoft Office. The released patches resolve vulnerabilities that have been identified within Microsoft software products. Keep in mind that these patches must be successfully installed before vulnerabilities are corrected. Many times you will be required to restart your system for the updates to finish installing. On the same Tuesday, Microsoft also publishes a monthly security bulletin that provides details for each patch that have been released.

Each patch is classified into a category, based on the ease of exploitation and the degree of impact they predict. Microsoft classifies each patch that have been released.

(continued on back)
The TTU IT Division recommends that you keep current on critical and important system updates. For detailed instructions to assist you in configuring your system to automatically update, you may access the following online TTU IT resources:

- For Windows XP: [http://www.ithelpcentral.ttu.edu/solutions/criticalupdate_win2KXP.php](http://www.ithelpcentral.ttu.edu/solutions/criticalupdate_win2KXP.php)

The TTU IT Division would also like to remind you to make sure you keep up-to-date on software that is important to your daily activities. Here are some examples for you to consider:

- Operating Systems – OS X, Linux
- Productivity Software – Microsoft Office, Adobe Acrobat, Adobe Acrobat Reader
- Antivirus Software – Symantec Antivirus Client, Antivirus definitions
- Web Browsers – Firefox, Safari, Internet Explorer

If you need assistance or would like more information, please contact IT Help Central at (806)742-HELP (4357) or via e-mail at ithelpcentral@ttu.edu.

### Shred Day Update

The IT Division would like to thank all 37 departments and those individuals who participated in spring Shred Day. The contracted vendors shredded 859 boxes of documents, generating 34,396 lbs of paper to be recycled. Since the TTU IT Division started hosting Shred Day in September 2007, the TTU Community has shredded 3,152 boxes of paper generating 86,122 total pounds to be recycled! Shred Day is just one way members of the TTU Community can begin to embrace a greener and safer IT environment at Texas Tech University. We appreciate our partnership with WesTex Documents and ShredIT, who provided shredding services for a discounted fee.

<table>
<thead>
<tr>
<th>Date</th>
<th>Boxes</th>
<th>Weight (lbs)</th>
<th>Shred IT</th>
<th>WesTex</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sept. 28, 2007</td>
<td>123.5</td>
<td>1,000</td>
<td>1,600</td>
<td>2,600</td>
<td></td>
</tr>
<tr>
<td>April 11, 2008</td>
<td>413.5</td>
<td>5,000</td>
<td>2,816</td>
<td>7,816</td>
<td></td>
</tr>
<tr>
<td>Oct. 24, 2008</td>
<td>336</td>
<td>4,680</td>
<td>5,500</td>
<td>10,360</td>
<td></td>
</tr>
<tr>
<td>May 1, 2009</td>
<td>775</td>
<td>5,920</td>
<td>8,500</td>
<td>14,420</td>
<td></td>
</tr>
<tr>
<td>Oct. 16, 2009</td>
<td>645</td>
<td>9,530</td>
<td>7,000</td>
<td>16,530</td>
<td></td>
</tr>
<tr>
<td>April 30, 2010</td>
<td>859</td>
<td>12,220</td>
<td>22,176</td>
<td>34,396</td>
<td></td>
</tr>
<tr>
<td>TOTAL</td>
<td>3,152</td>
<td></td>
<td>86,122</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Don’t Let Identity Theft Spoil Your Vacation

Tips for protecting your identity while vacationing:

- Ask a trusted neighbor to pick up your mail and newspaper or stop delivery. Identity thieves are on the lookout for signs that you are on vacation, in order to steal mail.
- Don’t travel with all your credit cards. Carrying limited credit cards reduces the chance of loss or theft.
- Don’t leave personal information in your hotel room. Consider storing items that contain financial or other confidential information in the hotel safe.
- Avoid accessing personal information from public computers. Most public wireless connections are not secure, so avoid using them for financial transactions.

Texas Tech University Web Site: [http://www.ttu.edu](http://www.ttu.edu)

Computer-Based Training (CBT): [http://cbt.ttu.edu](http://cbt.ttu.edu)

Safe Computing Practices: [http://safecomputing.ttu.edu](http://safecomputing.ttu.edu)

Contributions by: Katherine Austin Beltz, Ph.D., Shannon Cepica, Mark Holwerda, Danny Mar, Alvin Mills, Yung Ng, Ashley Raymond, J Stalcup, Britta Tye, Laura Webb, and Allen Young.

Safe Computing Practices Committee: Sam Segran, Katherine Austin Beltz, Ph.D., Darrell Bateman, Pulin Bhatt, Shannon Cepica, Paco Diaz, Scott Hall, Mark Holwerda, Michael Horton, Danny Mar, Alvin Mills, Yung Ng, Mike Simmons, Phil Smith, Ph.D., J Stalcup, Britta Tye, John Vandygriff, Allen Young, and assistance from IT Division leadership and staff.