TTU IT Security Awareness

New Spam and Phishing Containment Strategies

Despite continued warnings from the TTU IT Division, a small number of TTU faculty, staff, and students have responded to “phishing” e-mails with their eRaider usernames and passwords, as well as other confidential information. As a result, spammers have been able to use these accounts to generate large quantities of spam. Subsequently, major e-mail providers have placed the TTU mail domain on their “black list”, causing legitimate e-mails sent to those providers (Yahoo, MSN, HotMail, Google, etc.) to be rejected and not delivered. In order to address this problem, the TTU IT Division has implemented two new e-mail strategies:

• **Blocking Spam Sent from TechMail Accounts**
  The first strategy will reduce the amount of outbound spam sent from TechMail addresses. Just as inbound messages are scored based on the likelihood of being spam, outbound messages are now scored as well. If a message is scored high enough, it will not be delivered, and the sender will receive a notice stating the following:

  TechMail unable to deliver because message was scored as spam. Please alter message and resend; for assistance contact (806)742-HELP.

• **Delivering Potential Phishing Messages to Junk Mail**
  The second strategy identifies likely incoming phishing schemes and automatically places them in your Junk E-mail folder. Phishing messages typically include the word “password” in the text; the TechMail server currently preends a warning message onto the message scored as potential spam, warning you not to respond. Messages containing the word “password” are now delivered to your Junk E-mail folder, unless they are already on your safe senders list. Please note that authenticated, internal TechMail messages will not be affected.

  Further, if a TechMail customer moves the message containing the word “password” from their Junk E-mail folder into their Inbox and replies to that message, the outgoing message will not be delivered. The sender will receive a notice stating the following:

  Unable to send messages flagged with security warnings. Contact (806)742-HELP for assistance.

Note that for legitimate external messages that contain the word “password”, TechMail customers must move the message to their Inbox and remove the warning text from their reply for the message to be sent. Customers are cautioned to carefully review the message content before removing the warning text and sending the message onwards to ensure that the security exposures are not perpetuated.

As a reminder, no one (including TTU employees) should ask for your eRaider password, and you should **never** share your password with anyone for any reason!

For more information or questions, please contact IT Help Central at (806)742-HELP (4357), via e-mail at ithelpcentral@ttu.edu, or online at www.ithelpcentral.ttu.edu.

Acclimating to the New TechMail Filters

As we continue to come up with methods to manage spam and phishing issues, the following tips will help you adjust to the new security requirements:

1. **Communications with Journal Editors**
   For those of you who review and submit articles to journals, add the appropriate mail domain (ex. @ttu.edu, @yahoo.com) to your safe senders list (http://www.depts.ttu.edu/ithelpcentral/solutions/email/safe_senders_list.php). Note that when the editor sends you login credentials to access materials electronically, the message will be filtered to your Junk E-mail folder, unless you have added that sender to your safe senders list. With criminals targeting compromised journal accounts to relay spam, carefully review every message you receive!

2. **Mailing List Servers**
   For active mailing list memberships, add the domain to your safe senders list (see resource above).

3. **General Correspondence**
   Avoid the following to reduce the likelihood of a legitimate message being tagged as spam (at TTU or receiving mail servers):
   - Misspelled words in the subject line and body;
   - Use of words and acronyms not likely to be found in a common dictionary, including scientific and technical terms, particularly in the subject line;
   - Sending mass mailings, unless using a listserv;
   - Inclusion of words and characters typically found in spam. Microsoft offers these words as general examples of what spam filtering may look for: http://office.microsoft.com/en-us/help/ha010450051033.aspx.

4. **General Safe Computing Tips**
   Please assist us in combating spam by following these safe computing practices:
   - Do not click on links contained within an e-mail unless you are certain of the sender’s identity and expecting the information;
   - Do not open attachments unless you are certain of the sender’s identity and expecting the information;
   - Delete and do not reply to any e-mails asking for private information, especially your password;
   - Update your anti-virus software; Symantec AntiVirus is available for download at http://eraider.ttu.edu at no cost to the University community; and
   - Keep current on critical system updates:
     - Windows Users: http://windowsupdate.microsoft.com
     - For instructions to set up Automatic Updates, visit http://safecomputing.ttu.edu/criticalupdates.php
     - Mac Users: Use Software Update in System Preferences

TTU IT Security Awareness

Message from the CIO

The Department of Homeland Security’s National Cybersecurity Division (NCSD) has designated the month of October as the fifth annual “Cybersecurity Awareness Month.” As part of this initiative to raise awareness and minimize risks associated with cyber crime, the TTU Office of the CIO has designated the week of October 12th, 2009, as “TTU Cybersecurity Awareness Week.” We are dedicating this issue to key IT security topics: Data Loss Prevention, Records Retention, and Data Encryption Tips. In addition, we highlight the recent improvement in our e-mail security initiative with Outbound Spam and Phishing Filtering. As part of our security week, we will host a Symantec presentation, post educational materials, and culminate the week with our fall semester Shred Day. Throughout the year, we work diligently to inform faculty, staff, and students about safe computing practices and security threats. Please join us in helping to further raise IT security awareness on our campus and we invite you to participate in our events the week of October 12th. IT security posture is strengthened through collaboration and coordination – thanks to all of you for your efforts in helping to secure TTU data and IT resources!

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

For more information or questions, please contact IT Help Central at (806)742-HELP (4357), via e-mail at ithelpcentral@ttu.edu.
Data Loss Due to Carelessness: A Problem in Higher Education

The latest statistics on data loss breaches – the unauthorized exposure of personal or confidential data that could lead to identity theft – reveal some alarming facts regarding higher education. According to data available from the Open Security Foundation’s Data Loss Database[1], the Education Sector accounted for 27% of all known data loss breaches. The Educational Security Incidents[2] (ESI) website provides a more detailed breakdown of these incidents, focusing specifically on higher education institutions. ESI concluded that 49% of all data loss breaches in 2008 were due to “employee mistakes”, i.e. carelessness, or “unintended actions by employees” that exposed personally identifiable information (PII) to identity theft. This percentage outnumbered the incidence of hacker attacks by a 2-to-1 margin. The message for the nation’s colleges and universities is clear: faculty and staff who have a business need to access the PII of students and employees must exercise diligent care to avoid unintentionally exposing that information to identity thieves.

Here are some ways to practice diligent care:

- Never post student grades on bulletin boards, websites, or in other public places using Social Security Numbers (or any portion of this number) or Texas Tech Banner ID’s (“R” Number);
- Do not store reports or data containing student or employee PII on individual desktops, laptops, portable computing devices, or removable media (CD-ROM’s, CD-RW’s, DVD’s, USB Memory sticks, etc.);
- Do not needlessly e-mail files or data containing PII, as this information can become a part of personal e-mail archive files or be inadvertently forwarded to unauthorized individuals;
- Faculty and staff with a business need to store or e-mail data containing PII must use encryption technology and take appropriate measures to safeguard this information. For more information or questions, please contact IT Help Central at (806)742-HELP (4357), via e-mail at ithelpcentral@ttu.edu, or online at http://www.ithelpcentral.ttu.edu; and
- All university faculty and staff must observe TTU IT Security Policies and use industry standard security best practices when developing application code and websites.


Records Retention Tips
TTU Archivist Lynn Whitfield

The volume of mail, e-mail, and files we deal with on a daily basis can easily bog an office down with unnecessary documents. The field of Records Management grew out of this common institutional need to differentiate which records to keep, which to dispose, and which to archive for posterity. In 1992, Texas Tech University began its Records Retention Project in accordance with Texas law requiring all state agencies, colleges, and universities to implement and adhere to a records retention schedule. TTU’s Records Management Office conducts a survey of all TTU departments and campuses once every three years in order to compile a complete records retention schedule. The schedule, located online at http://www.swco.ttu.edu/recordsmanagement/home.htm, lists every recognized classification of university record type, length of required retention, and proper disposal methods. The next records survey will be conducted in the spring of 2010.

Confidential and Sensitive Data: Tips for Encryption and Data Protection

As Texas Tech University faculty and staff, we are responsible for exercising due diligence in protecting confidential and sensitive data. Encryption is one way to protect such data; we offer the following tips:

- When you have no other alternative and must store sensitive or confidential information on a portable device, TTU Portable Computing Security Policy requires that you encrypt the data on the device to meet state mandate;
- Install and maintain anti-virus software;
- Do not share your passwords or encryption keys with anyone;
- Dispose of sensitive information properly. To ensure deleted files cannot be accessed, make sure that you permanently erase sensitive files by emptying your system “trash bin”;
- Lock or turn off your computer any time you are away from it. An encrypted hard drive may still be vulnerable to a skilled attacker who has direct access; and
- Never leave a portable device unattended!

For more information or questions, please contact IT Help Central at (806)742-HELP (4357), via e-mail at ithelpcentral@ttu.edu, or online at www.ithelpcentral.ttu.edu.

Fall Shred Day October 16

The TTU IT Division, in partnership with the Office of Records Management and University Parking Services, will host TTU Shred Day on Friday, October 16, from 9am-3pm in the United Spirit Arena north parking lot. Shred Day is a component of the TTU Office of the CIO Safe Computing Practices Campaign. Since the inception of Shred Day, we have assisted the TTU Community with shredding and safely recycling over 35,000 pounds of documents! We appreciate your effort in making the initiative a success and invite you to participate this year.

Note: Custodial Services, (806)742-9777, provides shredding services for the Texas Tech community throughout the year for a fee.

Contributions by: Katherine Austin, Ph.D., Darrell Bateman, Logan Beatty, Pulin Bhatt, Gary Burns, Shannon Cepica, Scott Hall, Mark Holwerda, Randall King, Danny Mar, Yung Ng, J Stalcup, Britta Tye, John Vandygriff, Allen Young, and assistance from IT Division leadership and staff.

Fall Shred Day October 16

The TTU IT Division, in partnership with the Office of Records Management and University Parking Services, will host TTU Shred Day on Friday, October 16, from 9am-3pm in the United Spirit Arena north parking lot. Shred Day is a component of the TTU Office of the CIO Safe Computing Practices Campaign. Since the inception of Shred Day, we have assisted the TTU Community with shredding and safely recycling over 35,000 pounds of documents! We appreciate your effort in making the initiative a success and invite you to participate this year.

Note: Custodial Services, (806)742-9777, provides shredding services for the Texas Tech community throughout the year for a fee.

Contributions by: Katherine Austin, Ph.D., Darrell Bateman, Logan Beatty, Pulin Bhatt, Gary Burns, Shannon Cepica, Scott Hall, Mark Holwerda, Randall King, Danny Mar, Yung Ng, J Stalcup, Britta Tye, John Vandygriff, Allen Young, and assistance from IT Division leadership and staff.

Fall Shred Day October 16

The TTU IT Division, in partnership with the Office of Records Management and University Parking Services, will host TTU Shred Day on Friday, October 16, from 9am-3pm in the United Spirit Arena north parking lot. Shred Day is a component of the TTU Office of the CIO Safe Computing Practices Campaign. Since the inception of Shred Day, we have assisted the TTU Community with shredding and safely recycling over 35,000 pounds of documents! We appreciate your effort in making the initiative a success and invite you to participate this year.

Note: Custodial Services, (806)742-9777, provides shredding services for the Texas Tech community throughout the year for a fee.

Contributions by: Katherine Austin, Ph.D., Darrell Bateman, Logan Beatty, Pulin Bhatt, Gary Burns, Shannon Cepica, Scott Hall, Mark Holwerda, Randall King, Danny Mar, Yung Ng, J Stalcup, Britta Tye, John Vandygriff, Allen Young, and assistance from IT Division leadership and staff.

Fall Shred Day October 16

The TTU IT Division, in partnership with the Office of Records Management and University Parking Services, will host TTU Shred Day on Friday, October 16, from 9am-3pm in the United Spirit Arena north parking lot. Shred Day is a component of the TTU Office of the CIO Safe Computing Practices Campaign. Since the inception of Shred Day, we have assisted the TTU Community with shredding and safely recycling over 35,000 pounds of documents! We appreciate your effort in making the initiative a success and invite you to participate this year.

Note: Custodial Services, (806)742-9777, provides shredding services for the Texas Tech community throughout the year for a fee.

Contributions by: Katherine Austin, Ph.D., Darrell Bateman, Logan Beatty, Pulin Bhatt, Gary Burns, Shannon Cepica, Scott Hall, Mark Holwerda, Randall King, Danny Mar, Yung Ng, J Stalcup, Britta Tye, John Vandygriff, Allen Young, and assistance from IT Division leadership and staff.

Fall Shred Day October 16

The TTU IT Division, in partnership with the Office of Records Management and University Parking Services, will host TTU Shred Day on Friday, October 16, from 9am-3pm in the United Spirit Arena north parking lot. Shred Day is a component of the TTU Office of the CIO Safe Computing Practices Campaign. Since the inception of Shred Day, we have assisted the TTU Community with shredding and safely recycling over 35,000 pounds of documents! We appreciate your effort in making the initiative a success and invite you to participate this year.

Note: Custodial Services, (806)742-9777, provides shredding services for the Texas Tech community throughout the year for a fee.

Contributions by: Katherine Austin, Ph.D., Darrell Bateman, Logan Beatty, Pulin Bhatt, Gary Burns, Shannon Cepica, Scott Hall, Mark Holwerda, Randall King, Danny Mar, Yung Ng, J Stalcup, Britta Tye, John Vandygriff, Allen Young, and assistance from IT Division leadership and staff.