PHISHING AWARENESS

MESSAGE FROM THE CIO

Phishing scams have become a mainstream method that Internet criminals use to gather account credentials, personal information, and institutional data. In this issue, we focus on information to help you avoid risking personal and institutional information. We count on your partnership to limit the damage these scams cause. While our TTU IT Security Team can block phishing schemes once detected, we rely on you to be vigilant, avoid falling prey, and report these costly attempts to steal information. Thank you for your continued partnership as we work together to secure TTU data and information resources.

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

BE VIGILANT: DON’T FALL VICTIM TO PHISHING SCAMS

Internet criminals and hackers often portray themselves as legitimate and trustworthy, in order to gain your trust. We all share a responsibility to Think Before You Click! Clues to help you spot a phishing scam:

• Requests for your username and/or password – credible institutions and organizations will not request personal information via email;
• A message telling you that your webmail or email account is about to expire and action is required – Texas Tech will never send you this type of message;
• A message telling you that your email account is full and that you should log in via the link provided to take action – Texas Tech will never send you this type of message;
• Time sensitive threats (e.g., your account will be closed if you do not respond immediately);
• Spelling and grammar mistakes;
• Vague or missing information in the “from” field or email signature;
• “To” field contains multiple random email addresses or is alphabetized;
• Impersonal or awkward greetings, such as “Dear Mr. account holder;”
• Unexpected files or downloads;
• Links that don't refer to the sender or sender’s organization;
• Emails about accounts that you don't have, such as eBay or PayPal, or banks that you don’t have accounts with;
• Emails “from” celebrities;
• Asks you to reply in order to “opt out” of a service; or
• Plays on human emotions to evoke sympathy, kindness, fear, worry, anxiety, or excitement.

CLEVER PHISHING ATTACKS AIMED AT TTU COMMUNITY

Internet criminals have become craftier in their attempt to impersonate legitimate Texas Tech University entities. Many attempt to portray a message from the “IT Help Desk,” such as the following that delivered to TTU mailboxes in March 2015:

From: it.desk@ttu.edu
Sent: Monday, March 02, 2015 4:34 PM
Subject: Service Violation - Urgent Action Required

Dear User,

We noticed a violation of our services on your E-mail account and for this reason, your E-mail account will be closed if you fail to resolve the issue within the next 48 hours.

This will only take a moment...Click the “RESOLVE” link below and enter the requested details to complete the process.

RESOLVE

© 2015 Texas Tech University.
All Rights Reserved

Typically, these messages will lead the reader to a carefully crafted website designed to steal personal information:

This particular website example, contained clear errors denoted above:

• Repeated references to texastech.com – our main campus website is ttu.edu, and texastech.com is our athletic site;
• References our network as “everyone.net” – our network is branded TTUNet; and
• No mention of eRaider, our official account management system – uses the generic “username.”
This document discusses the profitability of phishing attacks and the reasons why criminals continue to use phishing schemes. It highlights the potential financial losses from phishing attacks and emphasizes the importance of vigilance to prevent such attacks. The document also provides guidance on how to identify phishing attempts and what to do if one is encountered. Additionally, it encourages the use of safe computing practices to protect institutional data and information resources.