**REMEMBER**

- Never respond to any e-mail that requests personally identifiable information.

- Texas State does not solicit confidential information such as passwords or account numbers via e-mail or any other electronic communication.

**When in doubt, contact:**

**IT Security**

itsecurity@txstate.edu,
512-245-4225

or

**IT Assistance Center**

itac@txstate.edu

**KEEP YOUR INFORMATION SECURE**

- Never divulge your password to anyone. This includes family, friends, co-workers or even university IT staff.

- Use a different password for each online account you manage (e.g. Facebook, Twitter, NetID login, Banner, Amazon, banks, credit cards, etc.). Criminals know people often use the same password for all accounts. A breach of an account at one organization can lead to multiple breaches.

- Keep your computer up-to-date by applying operating system patches and anti-virus software updates.

- Do not change the security settings on university-owned devices.

Texas State University is a tobacco-free campus.
While phishing is effective, a relatively new type of attack has developed called spear phishing. The concept is the same: cyber attackers send e-mails to their victim, pretending to be an organization or a person the victim trusts. However, unlike traditional phishing e-mails, spear phishing messages are highly targeted.

Instead of sending an e-mail to millions of potential victims, cyber attackers send spear phishing messages to a few select individuals, perhaps only five or 10 targeted people. These messages are well-crafted and can be difficult to identify.

**WHAT IS PHISHING?**

Phishing attempts are e-mail messages sent by criminals to millions of potential victims around the world designed to “fish” for personal or financial information by tricking the recipient into providing a response.

Be aware, these messages are designed to fool the recipient by appearing authentic and coming from a trusted source: your bank, someone you know, or even an internal Texas State department such as ITAC or other IT department.

Be careful, these malicious attempts either ask you to respond to the e-mail or provide a link to a fake or “spoofed” website where you will be prompted for your credentials.

**HOW TO IDENTIFY A PHISHING ATTEMPT**

- These messages generally require you to take quick action, such as verifying your account to prevent it from being deactivated.
- It may, but not always:
  - claim that your account has been or will be suspended unless you take action
  - contain familiar branding associated with an unfamiliar website address
  - contain improper grammar and capitalization
  - contain misspellings

**HOW TO REDUCE YOUR RISK OF BEING PHISHED**

- Do not send your personally identifiable information or credentials (e.g. SSN, credit card number, NetID-password, Banner login, banking information, etc.) through e-mail or provide them in response to an unsolicited request.
- If other characteristics of the message indicate it could be a phishing attempt, do not click on links within the e-mail; never click on links in e-mails from unfamiliar sources.