Keep Your Information Secure

- **Never** share your password with anyone, this includes everyone
- Use a **different** password for **each** online account you manage
- Keep your computer and mobile devices **up-to-date** by applying operating system patches and anti-virus software updates
- **Do not** lower the security settings on university owned devices
- Report any possible phishing emails utilizing the Report Phishing button in Outlook for Windows or Office 365 or forward any phishing or suspicious emails you received in your TXST email, *as an attachment,* to **abuse@txstate.edu.**

Think Before You Click!

Remember!

- **Never** respond to any emails that request personally identifiable information
- Texas State **does not** solicit confidential information such as passwords or account numbers via email or any other electronic communications
- **Always** be wary of offers that sound too good to be true, or ask for too much information

TEXAS STATE®
INFORMATION SECURITY

infosecurity.txstate.edu
512.245.4225

TEXAS STATE®
INFORMATION SECURITY

Don't fall for the phish!

What is Phishing?

Phishing attacks are email messages, text messages or anonymous phone calls sent by criminals to millions of potential victims around the world designed to "fish" for personal or financial information by tricking the recipient into divulging personal information.

Be aware! These messages or phone calls are designed to fool the recipient by appearing authentic and coming from a legitimate source, i.e. your bank, software provider, someone you know, or even an internal Texas State department such as ITAC or other IT departments.

Be careful! These malicious attempts either ask you to respond to the email or provide a link to a fake "spoofed" website where you will be prompted to log in using your credentials.

How to Identify a Phishing Attempt

These messages generally have a sense of urgency and require you to take quick action, such as verifying your account to prevent it from being deactivated.

In most cases, but not all, it:

- Claims that your account has been or will be suspended
- Contains familiar branding associated with an unfamiliar website address
- Contains misspellings or improper grammar and capitalization

Spear Phishing Attacks

While phishing attacks are effective, a relatively new type of attack has developed called spear phishing. The concept is the same: cyber criminals send emails, text messages or make a phone call, pretending to be an organization or a person the victim trusts. However, unlike traditional phishing emails, spear phishing messages are highly targeted.

Instead of sending an email to millions of potential victims, cyber criminals send spear phishing messages to a *few* select individuals, perhaps only 5 or 10 targeted people. These messages are well-crafted and can be difficult to identify.

How to Reduce Your Risk of Being Phished

- **Do not** send your personally identifiable information or login credentials through email or provide them in response to an unsolicited request.

  Examples of personally identifiable information.

  - SSN
  - NetID
  - Credit card numbers
  - Banking information

- DO NOT click on links in emails from unfamiliar sources

* **Make sure to routinely change your passwords**
* **Send any malicious emails to abuse@txstate.edu**