Security Information for New Faculty/Staff

1. Choose strong passwords
   - Choose strong passwords with letters, numbers, and special characters to create a mental image or an acronym that is easy for you to remember.
   - Create a different password for each important account, and change passwords regularly.
2. Use email and the Internet safely.
   - Ignore unsolicited emails, and be wary of attachments, links and forms in emails that come from people you don't know, or which seem "phishy."
   - Avoid untrustworthy (often free) downloads from freeware or shareware sites.
3. Use secure connections.
   - When connected to the Internet, your data can be vulnerable while in transit. Use VPN and Remote Desktop/Screen Sharing for remote connectivity and secure file transfer options when off campus.
   - Never use free Wi-Fi to do any TCU business, banking or transferring other sensitive information as your text may be seen by others.
   - Never use a "public" computer to do any TCU business, banking or transferring other sensitive information as your text may be seen by others, even if using a VPN and Secure HTTPS session.
4. Control access to your machine.
   - The physical security of your machine is just as important as its technical security.
   - Don't leave your computer in an unsecured area, or unattended and logged on, especially in public places - including the TCU Library.
   - Lock your computer screen when you walk away from it.
   - Use a "pin" on smart phones, iPads and tablets.
5. Protect sensitive data (SPI) – Personal and TCU Data
   - Do not store SPI on Flash Drives, Hard Drives, CDs, DVDs or in the Cloud like Drop Box.
   - Use Identity Finder to remove or secure SPI
   - Protect yourself against identity theft.
   - Encrypt personal sensitive files.
   - Regularly backup your important files.

TCU INFORMATION TECHNOLOGY

Visit Our Website
Visit our site to learn more about the Information Technology division at TCU. Visit it.tcu.edu

Password Self Service
Use our password self-service tool to change/reset your password or to unlock your account. Visit password.tcu.edu

Technology Training
Get with our technology trainer and find out what you can learn about the services that we offer. Visit it.tcu.edu

6. Avoid spyware/malware.
    - Don't download unnecessary toolbars, add-ins, games, etc.
    - Don't click on links, instead copy and paste them into your browser.
    - Protect yourself against Keylogging software, Browser Re-directs and Drive-by downloads.
    - Even if you don't have SPI on your computer, your computer is in the TCU network and if compromised can be used to attack other computers.
7. Periodically, check the health of your computer.
    - TCU continually updates your computer, keeping your systems patched, but you will need to check to make sure everything is working. Regularly check – Windows updates, Apple Updates, Third Party Application Updates (Adobe, Java, Firefox etc.) and Sophos Anti-Virus.
    - Check desktop firewall to make sure it is enabled.
    - Inform IT Computer Help Desk if you notice Alerts or odd behaviors on your computer.
8. Most importantly, stay informed.
    - Find more TCU Security information at security.tcu.edu.

Security Information website
Visit security.tcu.edu to learn more about

- Password Security
- Email Security
- Secure Connections
- Control access to your machine
- Protect sensitive data (SPI)
- Avoid spyware/malware
- Check the health of your computer
- Stay Informed

Email: security@tcu.edu