Cyber Security on the Go

How to protect your laptop, smartphone and other mobile devices

TCU faculty, staff and students frequently rely on mobile computing devices such as ***laptop computers***, ***smartphones***, ***portable storage devices*** (i.e., USB memory sticks, thumb/flash drives, removable hard drives), ***PDAs*** (Personal Digital Assistants), etc. These devices offer convenience but also include risks. This document will supply you with some security guidelines to protect you on the go.

What are the risks?

Mobile computing devices can store a large amount of data, are portable, often unprotected and are easy to lose or steal. It is relatively simple for an unauthorized person to gain access to all the data stored on them. Even if the device is not lost or stolen, the data may be "sniffed" during unprotected wireless communications. The results can include broken devices, infection from a virus, spyware or malware that allowed capturing of your keystrokes (including passwords and credit card numbers) and/or theft of sensitive personal information. Additionally, many mobile devices offer location-aware technologies which raise concerns about privacy and security.

Best Practices

Good habits

- Keep it in sight, within reach, on your person.
- For laptops, use cable locks.
- Avoid opening files, clicking links or calling numbers contained in unsolicited emails or text messages.
- Know what you are downloading. Make sure you download apps from reputable developers.
- Never store sensitive or confidential information on a mobile device.

Configure device securely

- Enable auto-lock – set an idle timeout that will automatically lock the device when not in use.
- Enable password protection – configure a password to gain access and use the device.
- Keep all system/application patches up-to-date, including mobile OS and installed apps.
- Install anti-virus if available and keep it up-to-date.
- Remote wipe – You can wipe out the data on a lost iPhone or smartphone with Windows Mobile if the phone uses ActiveSync to synch email. Open Outlook Web Access (OWA), go to Options.

Wi-fi

- Disable features not in use such as Bluetooth, infrared or Wi-fi. Set Bluetooth devices to non-discoverable to render them invisible to unauthenticated devices.
- Avoid joining unknown Wi-fi networks (disable any "autoconnect" feature).
- When using a public wireless hotspots for surfing the Internet only type in or view information you would not mind being public unless you create a TCU VPN session first.

USB memory sticks, thumb/flash drives, removable hard drives

- Configure with a username and password.
- Encrypt any data that you would not want exposed.

Data Protection

The best way to protect sensitive personal information (SPI) is to never store it on a mobile device.

- SPI is defined as an individual's name, address, or telephone number combined with any of the following:
  - Social security number or taxpayer ID number
  - Credit or debit card number
  - Financial/salary data
  - Driver's license number
  - Date of birth
  - Medical or health information protected under HIPAA
  - Student related data protected under FERPA
  - See the TCU Sensitive Personal Information (SPI) Policy https://security.tcu.edu/SecuringSPI.htm

- Store your important files on your M: drive and use VPN with Remote Desktop (Windows) or Screensharing (Mac) to access it (see http://www.tr.tcu.edu/RDP_VPN.htm for instructions on setting up VPN).

- While it is against TCU Policy to store SPI on a mobile device, if you must store your own personal information, encrypt it.
  - Use Microsoft Office file encryption, or
  - PGP's Whole Disk Encryption

- Only transmit SPI when required for TCU business and then only in an encrypted manner such as through a TCU VPN session.

Location-Sharing Technologies

Location-aware applications deliver online content to users based on their physical location. Technologies employ GPS, cell phone infrastructure or wireless access points to identify where cell phones or laptops are located and users can share that information with location-aware applications.

What are they used for? Apps might provide you with information on nearby restaurants, notify you of traffic jams, or let your friends in a social network know where you are, prompting increased social connectivity. Additionally there are highly targeted marketing opportunities for retailers. Unfortunately these services can make users "human homing beacons". They increase the chances of being stalked, of revealing where you live and when you are home or not.

Most location apps do have privacy controls; however they are not always easy to access. Know what applications you have and research the privacy controls.