Mobile Device Threats

Threats to mobile device users include:

- **Theft:** Thieves target mobile users so that they can resell the devices to make a profit and because they contain personal information that can be used by identity thieves and other criminals.
- **Malware:** Malicious individuals can create mobile apps to distribute malware and access users' personal information.
- **Social Engineering Attacks:** Phishing attacks are just as much of a threat on internet-equipped mobile devices. Social engineers may also target victims over the phone, via text message, or even on social networking sites.

Securing Information on Mobile Devices

To help to safeguard personal and company information on mobile devices:

- Ensure the physical security of your device.
- Choose a secure device.
- Keep your operating system up-to-date.
- Turn on device authentication.
- Use discretion when choosing mobile apps.
- Be mindful of the information you store on your device.
- Back up your data regularly.

Wi-Fi hotspots also pose risks to your information security. To protect yourself when using a public Wi-Fi network:

- Use a VPN to encrypt data.
- Don't use mobile apps that access personal or sensitive information.
- Only provide sensitive information to secure websites that are fully encrypted (look for "https" rather than "http" in the URL).
- Don't use the same password for multiple accounts.
- Once you're done using an account, log out.

If your device is lost or stolen:

- Report it to your institution immediately, if it contains company data.
- Notify your service provider.
- Contact local law enforcement, if your device was stolen.