Mobile Device Safety Tips

Your mobile devices – smartphones, laptops, and tablets – are always at hand, whether you're working, traveling, or just entertaining yourself. These devices connect you to the world but also contain a lot of personal information about you, your family, and friends. It’s crucial to use your mobile device safely.

Key Safety Practices:

- **Secure Your Devices:** Use strong passwords or biometric security like touch ID to lock your devices. This helps protect your information if your devices are lost or stolen.
- **Enterprise Mobile Device Management:** If you're using your personal mobile device for work, it's essential to keep it secure. Enrolling your device in the enterprise mobile device management program is a must. [Click here](#) for more information.

- **Be App-Smart:** Personal information, such as your favorite games, contacts, shopping habits, and location, is valuable. Be selective about which apps you download and how they use your data.
- **Control WiFi and Bluetooth Use:** Some places track devices with WiFi or Bluetooth on. Turn these features off when not in use to avoid being tracked.
• **Be Careful with Public WiFi:** Public networks are not secure, making your activities visible to others. Avoid sensitive activities like accessing email or banking sites on public WiFi. Use a VPN or a personal hotspot for a more secure connection.

**Maintenance Tips:**

**Update Regularly:** Keep your mobile devices and apps up to date to protect against viruses, malware, and other online threats.

**Uninstall Unused Apps:** Regularly delete apps that you no longer use for better security.