10 Tips to Help Better Secure Your Mobile Device(s):

The use of mobile devices continues to climb. We rely on our mobile devices for communication, banking, shopping, and storage of personal information. However, it is important to remember that the more we rely on our mobile devices, the more we are exposed to security threats. Smart phones and tablets are computers, and any device that connects to the internet needs to be protected.
Here are 10 tips to help better secure your mobile device(s):

1. **Use a passcode lock on your home screen.** A passcode will make it more difficult for thieves to access information on your device if it is lost or stolen. Without a password, anyone who has your device can easily access the data inside.
2. **Keep your software and apps up-to-date.** Updating your mobile operating system and apps give you the latest and greatest features and typically closes security holes and other vulnerabilities.
3. **Only download apps from trusted sources.** There are countless apps on the market, and some are offered through independent, unmonitored sources. Only download apps from an App Store, after reading the reviews and ratings.
4. **Review the privacy settings on apps before you download them.** Some apps request access to personal information on your device, including access to your contacts, text messages, camera, and location. If the requested access is outside of the purpose of the app, and you can't control the access settings, don't download it.
5. **Install mobile security software.** As mentioned, your mobile device is a computer and can be vulnerable to hackers and cyber criminals. A security app helps safeguard your personal data, and protects your phone from viruses and malware.
6. **Be cautious when using unsecured Wi-Fi hotspots.** Wi-Fi hotspots transmit your data over-the-air, so if you enter a password or credit card details while using a public, or unsecured network, you run the risk of someone stealing your information. Criminals can also set up "evil twin" Wi-Fi hotspots. These networks are setup with the same name as ones used by major hotels and stores, in close proximity to the real ones, to trick you into connecting with them. If you need to access a website or app with a password, or use a credit card online, disconnect from the public Wi-Fi and use your mobile network.
7. **Do not allow automatic connections.** Your mobile device may be set to automatically connect with available Wi-Fi networks and Bluetooth devices. Disabling this option will prevent your mobile device from connecting and transmitting data without you realizing it.
8. **Use a "find my phone" tool.** Device location apps make it easy to locate your mobile device if it is lost, and helps anyone who finds it connect with you. Your device may offer the options of locking your device and wiping your data remotely if necessary.
9. **Avoid storing sensitive information.** Don't store information like passwords, credit card numbers, or social security numbers on your phone. If someone gains access to your device, you do not want them to have this information.
10. **Wipe your mobile device clean before you discard it.** Follow the manufacturer's recommended technique for removing the data from your device before you donate, sell, or trade it in. If you don't, you leave yourself vulnerable to someone accessing your personal information.