General Mobile Device Safety Tips

PROTECT YOUR DEVICE WITH A PASSWORD.

- Mobile devices are prime targets for thieves who can steal your device as well as your personal information. So, it's essential that you secure it with a password.

DISABLE SETTINGS WHEN THEY ARE NOT IN USE.

- Turning off Wi-Fi, Bluetooth, and location tracking (GPS) when you don't need them not only saves battery life, but also prevents anyone from tracking you and makes it harder for hackers to access your device.

INSTALL A SECURITY SUITE.

- Security suites address a wide range of issues that can protect you and your device.

JAILBREAKING: BE CAREFUL

- Jailbreaking – bypassing device limitations so you can install special software – can be fun. However, it voids your warranty and can be taxing on your device.

JAILBREAK ONLY WITH

CAUTION.

What we do:

Protect the citizens and economy of Florida by safeguarding our information systems, reduce our vulnerability to cyber attacks, and increase our responsiveness to any threat.

Contact us:

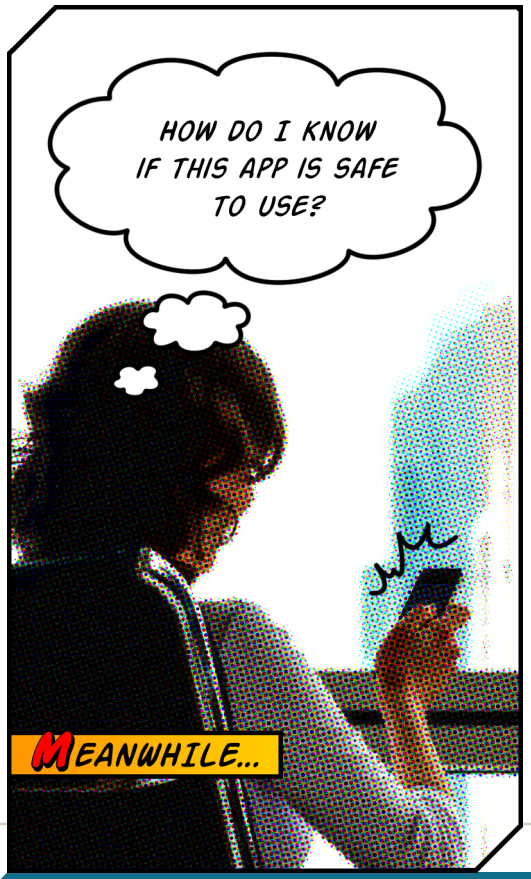
Phone: (850)410-7645
Email: admin@secureflorida.org
Website: www.secureflorida.org

Subscribe to **The Beacon** to stay informed and up-to-date on online security news. You can also sign up to receive Cyber Alerts from Secure Florida.

Secure Florida is funded through the Florida Department of Law Enforcement

Revised June 2016

Secure FLORIDA.org



Mobile Computing: Using Apps Safely

App Safety

Apps make our lives simpler, easier, and a lot more fun. However, you can't assume that all apps are safe to use: ***security may not have been a priority for the app developer, but it should be for you.***

Steps for using apps safely:

1

KNOW YOUR SOURCE.

- There are many places to download apps. Do your research!

2

CHECK PERMISSIONS.

- Many apps need permission to use other device features. Make sure you are comfortable with that.

3

READ THE RATINGS.

- Use the experience of others to help you make your decision. Pay special attention to the Parental Guidance ratings.

4

REVIEW ALL SETTINGS.

- Make sure you know how the app functions.

DETAILS INSIDE »»»

KNOW YOUR SOURCE.

- Apple's App Store and the Google Play Store are the most popular places, with millions of apps and billions of downloads. Although no source is completely free from malicious software, both Apple and Google have a thorough vetting process to keep their apps malware free.
- If you are considering an app from a lesser-known store, first do some research into both the store and the app.

CHECK PERMISSIONS.

- Before an app can access certain features such as the camera or microphone, or before it can use other apps, it requires *permission*.
- Android apps list their permissions when you download them; if you don't want to grant the permission, you can refuse the app. Newer versions allow you to choose which permissions to accept.
- Apple apps don't list the permissions when you download them, but ask you before each one they use; you can refuse permission any time.

READ THE RATINGS.

- Scan down the list of reviews to get a good idea of others' experiences with the app. Look for both the positive and the negative.

PARENTS: Pay special attention to the Parental Guidance ratings.

Apple App Store	Google Play Store
	E (Everyone)
4+	
9+	E10 (Everyone, 10+)
12+	T (Teen, 13+)
17+	M (Mature, 17+)
	AO (Adult Only, 18+)

REVIEW ALL SETTINGS.

- Check the settings carefully. Some are merely decorative; others govern benign functions such as the music volume. Still others deal with issues like privacy and location tracking.