CTIA Consumer Security & Privacy Tips

You love your mobile device. It's so efficient, so convenient and so much fun. No wonder it's virtually always with you, always on and always has just what you want.

With its ever-expanding array of features and functions, it has never been more important to protect your device and the data it stores. It has never been easier, either.

Here are timely tips from CTIA–The Wireless Association® to help you get started:

Setting up security for your device

1. **Set up security software.** This will back up your personal data, locate your device if it's lost or stolen and run a security scan on the apps you download to detect malware and spyware. In many cases this software may be part of the device operating system or may be a preloaded app. You can download other security software options.

2. **Set a short inactivity timer.** Security-wise, one to three minutes is best. While you're at it, set a passcode for your device to protect your data if your device is lost or stolen.

3. **Enable or install features that can lock, locate and erase your device remotely.** If you lose your device, ask your provider to put your account on "hold." It protects your device from unauthorized use – and protects you from having to pay charges incurred if the device turns up stolen. If you know the device has been stolen, call your provider and the local police to report it.

Maintaining security for your device

1. **Install updates to your operating system as soon as they're available.** Updates often improve security.

2. **Update your settings for your apps regularly.** It's the most efficient way to manage access to – and use of – your personal information by individual apps. Delete apps you don't use because some collect information even when you're not using them.

3. **Leave your device's unique identification numbers alone.** Those numbers are similar to a serial number that your wireless network uses to authenticate each device. Messing with them – sometimes called rooting or jailbreaking – opens the door to hacks and may violate your warranty.

4. **Turn off Bluetooth® and Wi-Fi when you don't need it.** Security for public Wi-Fi networks varies, so always use a secure connection or an encryption service when you're dealing with transactions that involve sensitive information.

5. **Before you recycle, trade in or sell your phone, erase all information associated with apps and all personal information.** If possible, keep the SIM card and any removable storage, and use the "factory reset" option.

Downloading Apps

1. **Stick with well-known app stores.** For example, the ones connected to your device's operating system or another well-known third-party. Most app stores evaluate apps to find and remove any that might be malicious. Spam email and texts also are sometimes used as a trick to install malware and spyware on your device, so delete those messages.

2. **Read reviews about an app and a developer before you download.** You can check out the developer's reputation through the app store or a search engine. If there's no contact information for the developer, download with great caution.

3. **Check the permissions for an app before you download.** What information will the app access and how will it will be used? Some apps access only the information they need to function best, but others may access data that may not seem to have anything to do with the app's purpose.

4. **Decide whether free services and relevant ads are a convenient trade-off for information accessed from your device.** Access to your device's information may enable some apps to be free, makes ad services more efficient and makes the ads you get more relevant.

For more information about keeping your device and your data secure and private, visit **CTIA.org**, **StaySafeOnline.org** *and* **OnGuardOnline.gov**

For more information about keeping your device and your data secure and private,

visit **CTIA.org**, **StaySafeOnline.org** *and* **OnGuardOnline.gov**