

# CONSUMER SECURITY & PRIVACY TIPS

Your mobile device is efficient, convenient and fun, which is why it's always with you. Today, mobile devices do everything from serve as your wallet to your health care monitor. It has never been more important to protect your device and the data. It has never been easier, either.

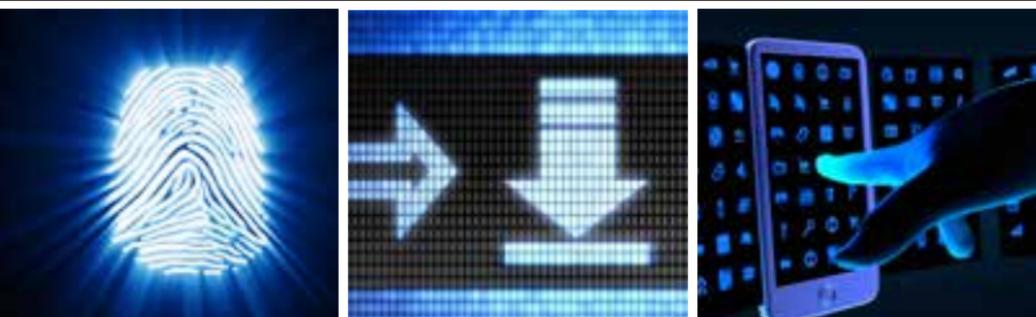
Here are **12 tips** from CTIA–The Wireless Association® to help you.

- 1 DO add a PIN or password to lock your device.** Access your phone's security settings and create a PIN or passcode. Make sure you change this PIN or passcode regularly.
- 2 DO use your phone's auto-lock features.** Enable the auto-lock feature in your phone's settings so that it requires a passcode when you're not actively using it. We recommend an auto-lock that activates after one to three minutes of inactivity.
- 3 DO install security software.** Just like you protect your PC with antivirus software, you should do the same with your smartphone.
- 4 DO set up phone tracking, lock and erase apps/features.** These apps or pre-installed features on your device enable you to track your smartphone's location, lock it and wipe its data in the event it is lost or stolen.
- 5 DO install operating system and app updates as they become available.** These updates often fix security glitches or bugs, so it's important to download updates as soon as they are available.
- 6 DO know what personal data your apps want to collect.** Check an app's permissions to understand what personal information it wants to collect and how it will be used. If you aren't using an app, delete it.

See **7** – **12** →



# CONSUMER SECURITY & PRIVACY TIPS



- 7 DO turn off Bluetooth® and Wi-Fi when you don't need it.** Security for public Wi-Fi networks varies. Plus, it will save battery life.
- 8 DO backup your data.** Routinely backup contacts, photos and messages to an external service, such as laptop or a cloud server so that you don't lose this valuable information if your device is lost or stolen.
- 9 DO evaluate the trade-off of "free."** Access to your device's information may enable some apps to be free, makes ad services more efficient and makes the ads you receive more relevant. When asked to share information with apps, decide whether these advantages are worth it.
- 10 DO read reviews of apps before you download.** App stores provide information on the app developer. If there is no contact information for the developer, download cautiously.
- 11 DON'T use unknown app stores.** Stick with the app stores 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.
- 12 DON'T open unknown links or files.** Links and files from unknown senders may contain harmful or malicious malware.

▶ Learn more by visiting: <http://ctia.it/1xv9Qli>

Last updated October 2015

