



Tips for Protecting Your Smart Device from Theft

Record device information. Mobile devices have unique numbers (IMEI or MEID numbers) that can identify devices if they are stolen. You should record the IMEI or MEID number, serial number and MAC/Wi-Fi address and store it in a safe place. This information is usually found under the “Settings” menu on the “About” screen. Additionally, screenshot functions make it easy to capture this information and send it to an email account. Before you go out:

- [Find the IMEI or MEID number on your mobile device](#)
- Send yourself a screenshot of it: [iOS \(Apple\)](#), [Android](#), [Blackberry](#) and [Windows](#)

Be aware of your surroundings. Many mobile device thefts are crimes of opportunity. Using your device in public, particularly on public transit, or leaving it out in the open makes it easier for thieves to grab the device and run.

Treat mobile device theft like credit card theft. Mobile devices frequently contain sensitive financial and personal information.

Report all mobile device thefts immediately to your wireless carrier and local law enforcement.

Set a password/PIN and use the lock screen function. The password/PIN and lock screen functions on devices make it more difficult for thieves to use your stolen device and access your personal data. These functions should be set up as soon as you purchase a new device. (CTIA The Wireless Association has [instructions for setting up a password](#) on Android, Blackberry, Apple and Windows devices.)

Consider using mobile security apps. Mobile security apps can be useful in locating and recovering stolen devices. Common features include the ability to remotely track, lock or erase your personal data on your mobile devices. Some apps also allow you to remotely trigger an alarm on the device or take a photo of the thief. CTIA provides a [list of mobile security apps](#).

Regularly back up photos and data. Photos, videos, contacts, email and other data you would want to keep if your device is stolen should be backed up regularly on a computer, USB drive or cloud service.

Locate, lock and erase. You should inform law enforcement of your mobile security app that might help locate and recover the device. In addition, the remote lock feature can prevent thieves from using your stolen device. It may be best to remotely erase your personal data on the device if you believe it will not likely be recovered or if it contains sensitive financial, health or work information.

For More Information

Visit <http://www.fcc.gov/guides/stolen-and-lost-wireless-devices> and <http://www.ctia.org/your-wireless-life/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data> for more information about protecting your mobile devices.

