SMART DEVICE THEFT PREVENTION
LOCK • WIPE • REPORT

Tips for Protecting Your Smart Device

Record device information. Mobile devices have unique numbers (IMEI or MEID or ESN numbers) that can identify devices if they are stolen. You should record the unique 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, and also appears on the phone. Additionally, screenshot functions make it easy to capture this information and send it to an email account.

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.

Be aware of your surroundings. Many smart 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**.**

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

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

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 smart devices. Some apps also allow you to remotely trigger an alarm on the device or take a photo of the thief.

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

Lock, wipe, report. 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/smartdevice 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.

Federal Communications Commission
Consumer and Governmental Affairs Bureau
445 12th St. SW. Washington, DC 20554

1-888-CALL-FCC (1-888-225-5322)
TTY: 1-888-TELL-FCC (1-888-835-5322)
Videophone: 1-844-432-2275

www.fcc.gov/SmartDevice