

Protect Your Smart Device

The theft of wireless devices, particularly smartphones, is sharply on the rise across the country, according to many published reports. The high resale value of these high-tech phones and the personal information contained on the device that could be used by identity thieves has made smartphones a prime target for robbers. Here's how you can better protect yourself, your device and the data it contains, along with instructions on what to do if your device is lost or stolen.

How to safeguard yourself against smart device theft

- ✓ Consider your surroundings and use your device discreetly at locations in which you feel unsafe.
- ✓ Never leave your device unattended in a public place. Don't leave it visible in an unattended car; lock it up in the glove compartment or trunk.
- ✓ Write down the device's make, model number, serial number and unique device identification number (either the International Mobile Equipment Identifier (IMEI) or the Mobile Equipment Identifier (MEID) number or the Electronic Serial Number (ESN)), which you may find in your device settings or printed on a label affixed to your device underneath the battery. The police may need this information if the device is stolen or lost.
- ✓ Review your warranty or service agreement to find out what will happen if your phone is stolen or lost. If the policy is not satisfactory, you may wish to consider buying device insurance.

How to protect the data on your phone

- ✓ Establish a password to restrict access. Should your device be stolen or lost, this will help protect you from both unwanted usage charges and from theft and misuse of your personal data.
- ✓ Install and maintain anti-theft software. Apps are available that will:
 - Locate the device from any computer.
 - Lock the device to restrict access.
 - Wipe sensitive data from the device, including contacts, text messages, photos, emails, browser histories and user accounts such as Facebook and Twitter.
 - Make the device emit a loud sound ("scream") to help the police locate it.
- ✓ Make your lock screen display contact information, such as an e-mail address or alternative phone number, so that the phone may be returned to you if found. Avoid including sensitive information, such as your home address.

Be careful about what information you store. Social networking and other apps may allow unwanted access to your personal information.

What to do if your wireless device is stolen

- ✓ If you are not certain whether your device has been stolen or if you have simply misplaced it, attempt to locate the device by calling it or by using the anti-theft software's GPS locator. Even if you may have only lost the device, you should remotely lock it to be safe.
- ✓ If you have installed anti-theft software on your device, use it to lock the phone, wipe sensitive information, and/or activate the alarm.
- ✓ Immediately report the theft or loss to your carrier. (See service provider contact information at www.fcc.gov/stolen-phones-contact-numbers.) You will be responsible for any charges incurred prior to when you report the stolen or lost device. If you provide your carrier with the IMEI or MEID or ESN number, your carrier may be able to disable your device and block access to the information it carries. Request written confirmation from your carrier that you reported the device as missing and that the device was disabled.
- ✓ If the device was stolen, also immediately report the theft to the police, including the make and model, serial and IMEI or MEID or ESN number. Some carriers require proof that the device was stolen, and a police report would provide that documentation.

Consumer Help Center

For more information on consumer issues, visit the FCC's Consumer Help Center at www.fcc.gov/consumers.

Accessible formats

To request this article in an accessible format - braille, large print, Word or text document or audio - write or call us at the address or phone number at the bottom of the page, or send an email to fcc504@fcc.gov.

Last reviewed: 10/31/16

