Emergency Preparedness

Deter Smartphone Thefts and Protect Your Data

(NAPSA)—As Americans increasingly prefer mobile-first lifestyles, our mobile devices hold personal data that must be protected. That's why the wireless industry is proactively working to help you protect your smartphones and your information.

CTIA and participating wireless companies developed the "Smartphone Anti-Theft Voluntary Commitment" that will, at no cost to consumers:

- Remote wipe the owner's data in the event it is lost or stolen;
- Render the smartphone inoperable to an unauthorized user; and
- Prevent reactivation without the owner's permission.

Yet if the smartphone is recovered by the owner, the data on the smartphone can be restored to the extent feasible.

In addition to the voluntary commitment, CTIA and its member companies are individually and collectively developing consumer education campaigns to remind consumers about the numerous apps and features—many for free—available today to help deter theft and protect your personal information. These efforts are clearly working; there was a more than 20 percent increase in PIN and password usage from 2012 to 2015 according to a recent survey.

While the wireless industry is actively helping protect consumers, it's important that users also take some important and simple steps to protect their smartphones and their personal information.

BEFORE your smartphone is lost or stolen:

1. Be Aware. Know your surroundings and be cognizant of your smartphone use behavior. Try not to call attention to your smartphone, leave it lying around or let strangers "borrow" it.

2. Lock It. Set a hard-to-guess password to protect your device and change it regularly.

3. Add Apps. A number of apps can remotely track, lock or erase/wipe personal information on your smartphone. In addition, some remotely trigger an alarm so people know their smartphone is stolen or photograph the thief so you can send it to police. CTIA developed a list of apps available on Apple (iOS), Android, BlackBerry, and Windows platforms so you can choose the best one(s) for you.

Even if your smartphone gets lost or stolen, you can keep your data safe.

4. Save It (Again). If you have photos, e-mails, contacts, videos or anything else that you want to make sure is available if your smartphone is ever lost or stolen, save it somewhere else, such as a computer, USB drive or cloud service.

5. Insure It. Consider insuring your device through your wireless provider or a third-party entity so if it is lost or stolen, replacement is covered.

AFTER your smartphone is lost or stolen:

1. Report It. Immediately notify your wireless provider to avoid incurring charges. Tell the police what tracking or similar apps you have installed that may help them. If your device is lost, instruct your provider to put a "hold" on your account.

2. Locate It. Never attempt to recover your smartphone on your own, warns CTIA,; your safety should always be your No. 1 priority. If you've installed apps to remotely track your smartphone, however, activate them from a safe location and remotely lock your smartphone.

3. Erase It. If you have sensitive information relating to finances, health or work, or you believe your smartphone won't be returned, "remote wipe" it—similar to resetting it to its default settings. If you stored any passwords on your smartphone for email, financial accounts or remote work access, make sure you change them.

Learn More

For more information on how you can deter smartphone thefts and protect your personal information, visit http://ctia.it/1d1V99p.