InformationWeek
THE BUSINESS VALUE OF TECHNOLOGY

10 Steps To Smartphone Privacy

Smartphone owners, it's you versus bad guys and nosy apps. Follow these 10 tips to keep your data locked down.

By Eric Zeman, InformationWeek
February 18, 2012
URL: http://www.informationweek.com/news/security/mobile/232601089

10 iPad Problems, Solved
(click image for larger view and for slideshow)

Your smartphone is simultaneously your best friend and your worst enemy. It can help you find the nearest Starbucks for a caffeine fix, reach out to loved ones in times of need, or get the score of that vital play-off game. If it falls into the wrong hands, heck, even if it *doesn't* fall into the wrong hands, a smartphone can expose your contacts, location history, banking data, and more. Smartphone privacy was in the news again this week, due to a fresh Google and Apple iPhone privacy flap.

This all means smartphone owners need to be vigilant in order to protect themselves. Here are some essential tips to help keep your vital data under control.

1. Lock Your Phone

This may seem a simple and obvious step to take, but many people are too lazy to do it. Set up a screen lock so the phone can't be accessed or used without a password of some sort. Though four-number pins may foil street hoods, using a real alphanumeric password is much better. Make sure the screen locks automatically after 1 to 5 minutes of non-use.

2. Use 'Find My iPhone' Or Similar Services

It only takes a few moments to use today's smartphone tools to set up a free tracking/wiping service. Android, BlackBerry, iOS, and Windows Phone devices allow users to lock, track, or wipe their phones remotely if lost. Not only does this protect your data, it could help you recover a lost/stolen device. Do it.

3. Don't Leave Your Smartphone Unattended

Would you leave your social security card on a bar while you traipse off to use the bathroom? I didn't think so. Don't leave your phone sitting around in public where it can be grabbed by an opportunist. You may trust your coworkers in the meeting room, or friends you invite to your home, but don't be too quick to extend trust to people you don't know. Put it in your coat, pocket, desk (yes, even at the office), briefcase, purse, backpack, wherever. Keep it out of view.

4. Don't Give Your Phone to Strangers

That 'tourist' who needs to make an emergency call home and asks to use your phone? Dicey. It could certainly be someone in legitimate need of help--or not. Rather than give the person your phone, make the call yourself, and put it on speakerphone.

5. Keep Your Smartphone Up-to-Date

You know that system update you've been ignoring for a couple of weeks? Install it. Nearly all smartphone system updates include enhancements to device security. Smartphone makers and carriers often ship phones with buggy software that contains loopholes that can be used to circumvent security. When updates are provided by the manufacturer, install them.

6. Manage Location Settings

Most phones come with either GPS or carrier-aided location tracking features. These are meant to enhance the functionality of applications such as Google Maps or Foursquare (after all, maps are kind of useless if you don't know where you are.) Now, however, there are thousands of apps that want to access your location data, such as Google+, Facebook, Twitter, Instagram, and others. You can control location settings in these apps individually in most cases. If you want to make your location as secret as possible, turn off all forms of location assessment. This way, apps won't know where you are.

7. Do App Due Diligence

Speaking of apps, do your homework. If you value your privacy, read the "Permissions" screen when you download and install apps. Many apps will let you know that they are accessing your location, call history, contacts, and other data. Be sure to note if that data is going to be stored by the app, delivered by the app to the app vendor, or sent to third-party companies for other uses. If you're suspect about the permissions, do some research, look online to see if the app has been reviewed by reputable sources, and so on. Also, if you download an app and stop using it, get rid of it. Don't leave it on your phone.

8. Don't Download Apps From Untrusted Sources

Most smartphone manufacturers only want you to download apps from their stores, but there are plenty of ways to circumvent this control. In Android smartphones, for example, you can choose to enable a setting that allows non-Market apps to be installed. If you jailbreak our iPhone, you can install Cydia apps, etc. Don't do it. Apps that haven't been approved by an official app store are more likely to be invasive.

9. Watch Those Attachments!

Being able to access email on my phone is vital, especially when I am traveling for work. Be careful, however, about opening the attachments sent to you by people you don't know. Take the same precautions on your smartphone that you would on your home computer. Same goes for downloads from web sites, social networks, shortened URLs, etc.

10. Encrypt Smartphone Data

Today's smartphones make it relatively simple to encrypt the contents of the phone. This ensures that even if the phone does fall into the wrong hands and is accessed because the screen lock was bypassed, some level of protection remains. This is especially important for the memory cards of Android smartphones. The phone itself doesn't have to be stolen in order for you to lose all your documents, photos, songs, and other files.

The smartphone privacy bottom line is the same one your mother taught you when you were growing up: Don't trust strangers (or strange companies, apps, or networks.)