Smartphone Security: Easier than your computer

Levi King

kingle@metrostate.edu

Got a new phone lately? I did. It’s nice to set things up and play with the new features. Perhaps you’re waiting to upgrade and you’ve still got an older phone.

Old or new, we tend to focus on the physical. You don’t want a cracked screen or a broken button, so you get a rubber bumper case and a plastic screen protector to save it from falls. Maybe you even buy an insurance policy. But what are you doing to protect the information stored on your phone?

In this column, we’ve covered many ways to improve your personal security, from using password management to securing your home Wi-Fi. Yet, every day I see people being careless with phones packed full of sensitive data such as email and Facebook accounts. These are all an identity thief needs to make a copy of your life.

You can stop them. At the very least, lock your screen; use a PIN, pattern, password, whatever, just turn it on. Otherwise, you’re leaving your whole life wide open.

**Theft Is Not the Problem**

Smartphone thefts are dropping. Pickpockets just want to flip them for a quick buck, which is hard thanks to built-in “kill switches” that let you wipe your phone from your computer and make it about as useful as a brick. Apple introduced this with iOS 7 and turned it on by default in 8, while Google brought it to Android 5 (Lollipop) and beyond. When you turn this on, the phone cannot be “factory reset” by a thief to make it like new and easy to sell again.

Obviously, phones still get stolen — the anti-theft warning signs in Metro’s own library are not a joke. Kill switches reduce theft because most don’t know how to bypass them, so few are willing to take the risk and end up with a device they can’t sell. More ambitious thieves will strip a phone for parts to sell them as “repair kits,” but this is difficult because the insides are so delicate, and few stores offer repairs even if you have the right pieces.

You have more options than ever for tracking a stolen phone! They can send GPS location, snap pictures, or just ring loudly and show a message on the screen. Users of iPhone should open iCloud settings and make sure Find My iPhone is turned on and set up. Android users can do the same using Device Manager, and Microsoft offers a Find My Phone system for Windows Phones. The steps vary, but none are complicated, and you’ll be glad you took the time. If your phone is an older model that doesn’t support any of these options, you might look into third-party apps like Prey Anti-Theft.

**Updates Are Important**

Each new smartphone operating system (OS) version is more secure than the last, but many people never upgrade. Almost 20 percent of iPhone users have not updated to iOS 9 yet, and very few Android users are on version 6 (Marshmallow) today. You can check for updates by looking in your settings app.

Sometimes you can’t update. Most iPhones get left behind after a couple generations, when the update becomes too big for their old hardware to handle. Android users are at the mercy of both manufacturers (like Samsung) and carriers (like AT&T); if they don’t push an update, your phone stays behind. There are ways around this, but most are too involved for the average person, and may introduce more vulnerabilities if done incorrectly — don’t attempt to “jailbreak” your phone on a whim. It’s not easy.

Even if you can’t update the OS, update your apps. Many people turn off automatic updates to save data, but you can open your app store settings and tell it “update only on Wi-Fi” to prevent this.

**Viruses? Unlikely**

Sometimes malicious apps slip into the Apple App Store or the Google Play Store. Never download an app without checking feedback. Scroll through user reviews, and sort them by “Most Recent” for real people. Malicious app developers might put a bunch of fake 5-star reviews up when they launch.

As long as you’re on a newer version of iOS or Android, you should get prompted for permission when an app asks for something, like a pop-up for using your contacts. This can be a red flag; a simple flashlight app shouldn’t need to see your contacts! On an older phone without these warnings, you can review permissions from the app’s page in the store.

Some phone features shouldn’t run 24/7. Maybe you use a Bluetooth speaker at home, but you should turn that off on the go. Near Field Communication (NFC) is handy for tap-to-pay apps, but there are ways to exploit this from a range up to several feet, so toggle that off too. Even Wi-Fi should be toggled on an off. I keep mine off when not at home, only turning it on to save data on networks I trust, like a local coffee shop. Letting it automatically connect to random networks is risky.

Finally, you might be wondering about antivirus. Apple forbids antivirus apps, so iPhone users can skip this. Android users have options, but you might as well avoid them. An antivirus app can’t control your whole device to keep it safe like it could on a PC. Most are just checking your phone for other apps that have been reported to be unsafe. This is unnecessary as long as you use common sense when installing them in the first place. Otherwise, antivirus apps are probably just draining your battery with background scans.

In the end, smartphones are both easier and harder to secure than a computer. They’re more locked-down to start, but their portability makes them risky. Keep a handle on your personal data by following these guidelines, and you’ll be a step ahead.