ENJOY SAFER TECHNOLOGY®

# MOBILE DEVICE SECURITY AND BYOD FOR SMALL BUSINESSES

www.eset.com

# Mobile device security and BYOD for small businesses

By Cameron Camp, ESET Security Researcher

With mobile technology progressing at ever-more-breakneck speeds—the latest smartphones nearly rival the combined computing power that enabled the original moon walk—can scams be far behind? Is your mobile device a security risk? The latest wireless gadget in your pocket or purse right now has more in common with a laptop computer than the telephone that plugged into the wall when you were growing up, or even the flip phone you had a few years back. But unlike your laptop, your mobile phone goes everywhere and is always connected. For many of us that's also true of the tablets and book readers we love so much. All these digital traveling companions store, access and transmit all manner of personal and business information while far outside the safety of the office or home, or home office. And that exposes the information to thieves and scammers who would love to whisk it away to the dark markets where purloined data is bought and sold.

The use of personal devices for business purposes has been dubbed Bring Your Own Device (BYOD). But that also means you take the device out of the office, to wherever you need to go. Does that expose your business and networks to risk? And if you run a successful business from your kitchen table at home, could someone be monitoring everything you do on your smartphone? It's possible. That doesn't make it probable—many factors determine who gets targeted by the bad guys—but it certainly pays to think about it.

Here are some steps to strengthen your security and make sure unwanted folks don't have easy access to the crown jewels of your small business: your banking information, your contact list, your customer list, your latest emails about your latest invention, or that RFP you've worked so hard on.

## 1. Lock down your communication

Make sure you know how your mobile device is communicating. Are you on the phone company's 4G network—a relatively trustworthy communication channel—or has your device hopped onto a Wi-Fi connection? If so, who owns the access point? If you own it, see #2. If you are not sure, set your mobile device to only connect to wireless networks you trust. Out of the office that mainly means the 4G network, and it definitely excludes the "Free-Hacked-Wi-Fi" access point at the local hipster hangout.

## 2. Lock down your in-house Wi-Fi

If you have not password-protected the Wi-Fi access point at your office or home, others can snoop as you type, tap or gesture things out into the ether. They can possibly reconstruct those critical bits for later shenanigans. Select WPA2 if your home/office Wi-Fi router has that option. If necessary, get help from someone who's a little more tech savvy than you. Then set up your mobile device to remember and prefer that network to others that show up from neighboring offices or those with ill intent.

## 3. Lock down your devices

If someone swipes your phone or tablet right now and it is not at least password locked, you're setting yourself up for trouble. Nowadays there are numerous ways to secure access to your device, from passwords to gesture locks (swipes, tapping a certain sequence, etc.) to biometric security. Whichever you're the most comfortable with, use it. This way, if someone accidentally (or not) swipes one of your devices, he or she won't have access to the most important information by simply looking around at your private data.

## 4. Back up your devices and data

There is a lot to be said for having copies of all your files, photos, videos, messages and emails safely stored away somewhere other than your mobile device. Maybe in the cloud or on a hard drive in a desktop computer, or both, just to be on the safe side. Backups buy you peace of mind and give a last line of defense against thieves and that particularly nasty type of malicious code: ransomware. This is malware that encrypts the contents of your device and demands money to unlock it, and it has been seen on mobile devices (see blog: *Android/Simplocker using FBI child-abuse warnings to scare victims into paying $300*).

## 5. Use remote find/kill

Many mobile security suites (and sometimes the devices themselves) have “remote find” options. This means if your device comes up missing, you can issue a remote command to have the device tell you where it is. If you find it’s stuck in the couch cushions, you’ll likely have a very different response than if it’s in a car heading toward the mall. If you find it’s the latter, the remote wipe option can come in handy—just issue a command via SMS and it erases all your personal information (hopefully you read #4 before you have to do this).

## 6. Stick to official app sources

Google and Apple provide security-reviewed Android and iOS apps in the Play and App stores, respectively. Stick to these when downloading software to your Android and iOS devices. However, you still need to be vigilant as flaky apps sometimes slip past the reviewers (see blog: *Scareware: Fake Minecraft apps scare hundreds of thousands on Google Play*). Watch out for apps that offer a free version of games you normally have to pay for (and maybe ask yourself if you really need a game on a device you are using to build your real-world empire).

## 7. Use a good mobile security app

There are malicious apps and malicious links that target mobile devices. A good mobile security app will protect against these while offering additional protection, like device location. Corporate versions can be managed within the same console as the rest of your endpoints.

*For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted. For more information, visit www.eset.com.*

ESET®  ENJOY SAFER TECHNOLOGY®