1919 INVESTMENT COUNSEL

Mobile Device Security

June 2017

Brett Kozloski,
Business Systems Analyst

Nowadays, most people, whether they are in school, working or retired, carry and/or use a mobile device during their day-to-day activities. Although most are aware of the risk and inconvenience involved should their mobile device be stolen, the correlation of mobile device theft and identity theft often goes overlooked.

In order to obtain a baseline understanding of how your mobile device relates to your personal identity, perform this quick exercise and ask yourself the following questions:

- Does my phone lock with a PIN?
- Do I use all applications installed on my phone?
- For applications containing my name, email address, bank account information or other personally identifiable information, am I asked to enter an additional password after launching the application?
- Are my pictures, music, emails and other files saved outside of the mobile device (i.e. cloud or external hard-drive)?

If you answered, "Yes" to all of the above questions, then you at least have some knowledge of how to protect personal information contained on your mobile device. If you answered, "No" to any of the questions, then you need to carefully review how you use your mobile device. This could include reviewing the strength of your PIN/password, using two-factor authentication when accessing an application that contains private information, backing up important files and assessing which applications you actually need and use. Mobile applications, unbeknownst to the user, can run in the background of your mobile device and track data such as GPS location. It is imperative to uninstall mobile applications you do not need nor use and fully understand the data points involved to run applications you require.

On June 8, 2017, the Federal Trade Commission (FTC) released an official alert about the theft of mobile phones and the best way to prepare for and recover from this kind of theft.

The FTC offered four (4) distinct pieces of advice when it comes to securing your mobile device and thwarting identity theft:

1. Lock your phone. Use at least a 6-digit passcode on your device, or use the fingerprint scanner if it is available. Set the device to lock whenever it is not in use.
2. Update and back-up your phone when prompted and on your own time. Back up your device regularly and ensure automatic updates are turned on. Most cell phone service providers and/or manufacturers offer a free and automatically scheduled back-up of subscribers' mobile devices. Take note of where your data is being backed up, obtain the required login information and review how your data is stored outside of your mobile device. It should, at a minimum, be password protected. However, the FTC recommends that private information backed up to a cloud service be encrypted and any data stored on an external hard-drive be physically secured and only accessible by the owner of the information.

3. **Get help finding your phone.** Install and turn on 'Find my iPhone' (for iPhone users) or 'Find My Device' (for Android users). These applications could help you locate your device if you lose it. In the event your mobile device is stolen, these applications also allow you to remotely issue a command to wipe your device – even if the thief powers it off.
4. **Alert your mobile device service provider if your phone is missing.** Make the call as soon as you know your device is missing. Service providers and manufacturers can permanently or temporarily disable the SIM card to stop someone from using the stolen device (for calls, texts, Internet access, etc.). It is also helpful to keep a separate record of your IMEI number – you can typically find this on the original packaging of your mobile device or by contacting your mobile device service provider and/or manufacturer.

Regarding personal accounts on your mobile device (financial, corporate/personal email, shopping, etc.), the FTC highlighted three (3) tips to keep you and your mobile device secure:

1. **Turn on two-factor authentication whenever possible.** Turning on this feature on any application will require the entry of a password as well as a second piece of information to prove that it is you accessing the account (i.e. first pet's name, mother's maiden name, etc.). This added layer of security makes it harder for thieves to hack your accounts should one get ahold of your mobile device.
2. **Know which devices have access to your accounts.** Keep a list of all of your electronic devices and what specific accounts you access from each device. Most accounts offer a service to alert you when a login has taken place with a new device. If this option is available to you, enable it and check to see where you logged in and if it was actually you.
3. **When in doubt, change your passwords.** If you've lost your device, change all of your passwords. Focus immediately on changing passwords tied to email, online banking, social media and shopping accounts if your device is lost/stolen.

If you are a confirmed victim of identity theft or concerned about the possibility after losing your mobile device, the FTC recommends utilizing https://www.identitytheft.gov/ to file a formal report. After filing a report, you will receive clear instruction on how to prevent further damage, safeguard the balance of your accounts and information as well as a personalized recovery plan. Some recovery plans may involve putting alerts on credit reports, notifying your bank(s), cancelling all debit and credit cards and getting a new driver's license.

At 1919 Investment Counsel (1919ic), we're here to help guide you through the recovery process in the event your mobile device and/or personal information are compromised. Of course, if you lose your phone or think it may have been stolen, please feel free to contact your 1919ic Team. We will help you navigate the steps outlined in this document to best protect your personal identity and relevant data in a timely manner.

For more information on managing your cyber privacy and 1919ic's preferred cyber threat mitigation tools, please visit our website, download and read an article prepared by our Research and Information Technology Team's at this link: Managing Online Privacy: Do you know where your data is?

Citations

Roth, Sheryl. "An Identity Thief Stole My Phone!" *Federal Trade Commission - Consumer Information*. Federal Trade Commission, 08 June 2017. Web. 13 June 2017. <https://www.consumer.ftc.gov/blog/identity-thief-stole-my-phone>.

The views expressed are subject to change. Any data cited have been obtained from sources believed to be reliable. The accuracy and completeness of data cannot be guaranteed. **Past performance is no guarantee of future results.**