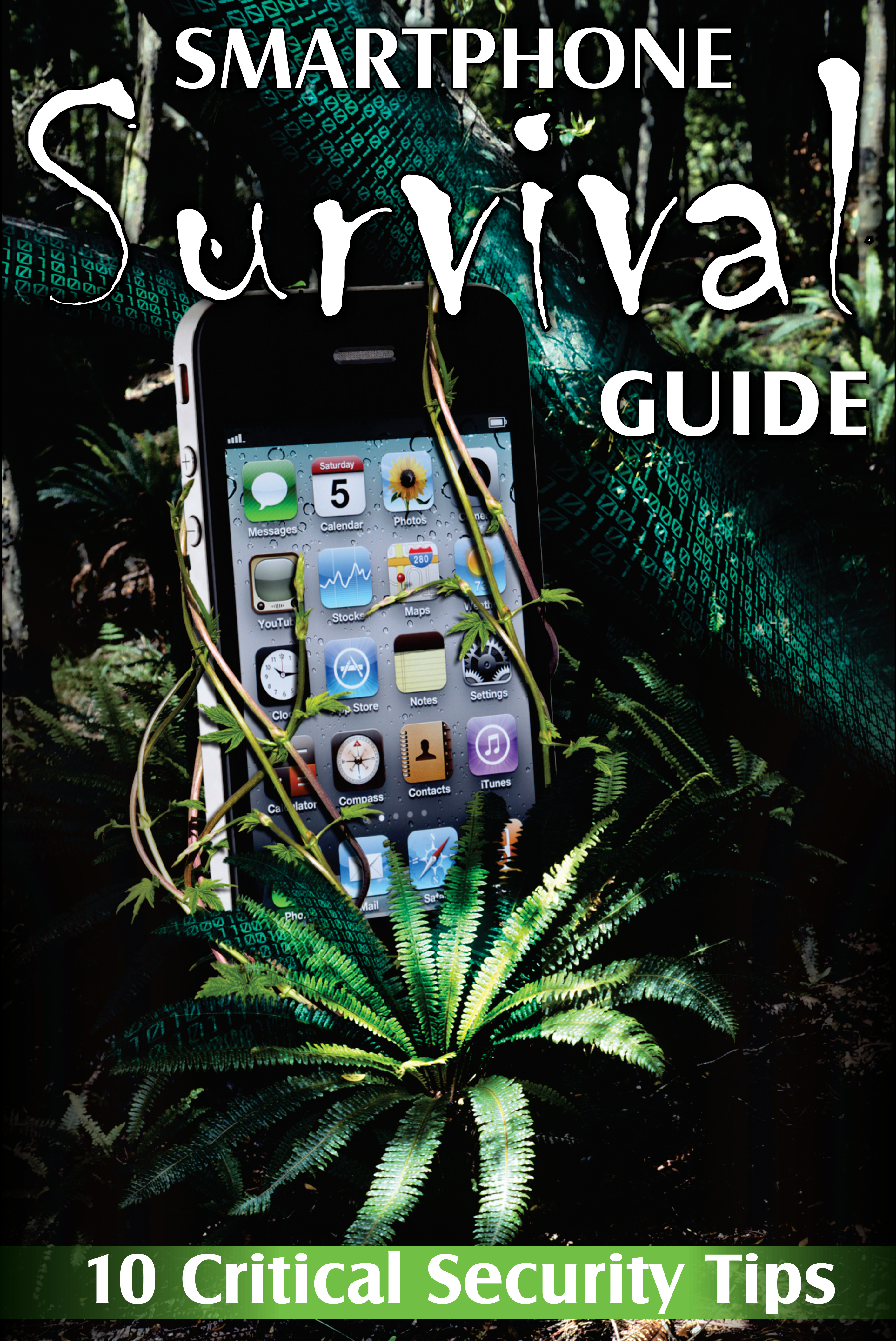
SMARTPHONE Survival GUIDE



10 Critical Security Tips

Published simultaneously in Canada.

Requests to the Publisher for permission should be addressed to the Permissions Department, The Sileo Group, 381 S. Broadway, Denver, CO 80209, (303) 777-3221, fax (866) 422-4922.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

To obtain a copy of this workbook in other formats, please visit www.Sileo.com. For bulk purchases, please contact The Sileo Group directly on (303) 777-3221.

Smartphone Survival Guide

10 Critical Security Tips

Table of Contents

For a digital version of this document, go to https://sileo.com/wp-content/uploads/Smartphone-Survival-Guide.pdf

Important Note

I primarily discuss Apple and Android mobile devices in this guide because they make up a lion's share of mobile phones. That said, for all of the smartphones and Operating Systems (also referred to as OS) discussed in this workbook, be sure that you consult your operator's manual and online instructions for your particular mobile device and service provider, as there are numerous models and constant updates to settings and options. Here are a few websites to get you started:

Android
https://support.google.com/android/?hl=en#topic=7313011
Or See Mobile Phone Manufacturer's Website

Apple
http://support.apple.com/manuals/

BlackBerry
http://docs.blackberry.com/en/smartphone_users/

Windows
http://www.microsoft.com/windowsphone/en-us/howto/wp7/default.aspx

Your Smartphone is as Powerful (and Dangerous) as a Computer

Your smartphone is a full-fledged computer; more powerful than a laptop from just a year ago. Consequently, data theft has gone increasingly mobile. In addition to carrying contact information on our phones, we now carry client files, banking logins, account information, sensitive emails, medical data and other private information, both personal and professional. Combining this miniature super-computer with mobility makes it highly attractive to criminals. You spend time and money protecting your computers, and your smartphone is no different. Here's how to get started:

1. Make physical possession an obsession.

Ok, this should be obvious: Mobile phones are small and therefore extremely easy to lose (or have stolen). But as often as I say it, in our push to be technologically savvy, we often forget that the first form of protecting smartphones (or laptops, for that matter) is by limiting physical access to the device. Keeping your phone physically on you or locked up when not in use is the most basic form of protection. Don't set your phone down in a restaurant or bar even for a second. Many phones are stolen from café tables, coat pockets, shopping carts, airport security bins, taxis and cars while they are momentarily unattended or somehow left behind. The thieves want access to your contacts, your online logins and they want to be able to call your bank as if they were you.

In addition, be careful to whom you loan your cellphone. I wish it weren't true, but eavesdropping software can be loaded in the few minutes that you allow someone else (usually a stranger who asks for help) to control your phone. This unfortunately includes competitors and suspicious spouses who want to install Tapping software on the handset. For example, it takes about 60 seconds to load mSpy on a smartphone, allowing an outsider to turn on your microphone (completely undetected) and listen to nearby conversations. I recently worked with a corporation whose competitor had installed mobile-spying software on the mobile phones of their top sales people while at an industry conference using a relatively simple Social Engineering scheme (that I won't share here).

If you loan out your phone to someone you trust, change the passcode afterwards just to be safe. The latest scam is for someone in a café or the airport to ask you to use the phone to make a quick local call. You think they are tapping away a number when they are actually installing a malicious App. The second most common way is for someone to send a malicious link through an email address you recognize (the thief has taken over their email account), effectively getting you to do their dirty work for them.

Bonus Tip: In case you do lose your smartphone (statistically, the #1 way that smartphones fall into the wrong hands), make sure that you have a recent backup or sync of the contents of your phone so that you don't lose that as well. Also, take a look at Steps 2 & 3 to preventatively protect the data in case your phone does go missing.

As you make it increasingly difficult to steal data off of your smartphone, thieves will tend to move on to easier targets (unless there is something highly valuable on your phone and they know it). Managing to never lose or misplace your phone, of course, is nearly impossible, which is why there are nine additional ways to protect your Smartphone.

2. Strengthen Your Device Passcode & Encryption.

All smartphones have password protection features that can be turned on to help keep unwanted users out (or at least slow them down a bit). Unfortunately, many people still don't have passcodes turned on, often because they want to access the phone while driving (which is unsafe and generally illegal). If nothing else, passcodes slow down data thieves and imposters long enough to give you time to remotely ‘‘wipe’’ your device (see Step 3). In addition, data encryption is generally only enabled when you have a passcode on your phone. The stronger the passcode, the stronger your encryption. Encryption is a critical part of smartphone security. Watch here for a short video on Securing Your Smartphone.

If you are reading this guide, you likely already have your passcode turned on. If not, turn on your passcode now (Apple, Android). Turn on the Auto-lock option so that the device locks up after a short period of time and consider turning on the feature that wipes your phone clean if the wrong password is entered repeatedly. Just be careful that your kids don't play a joke on you by wiping the contents of your phone by entering the incorrect password too many times (this is common with teenager's phones at school).

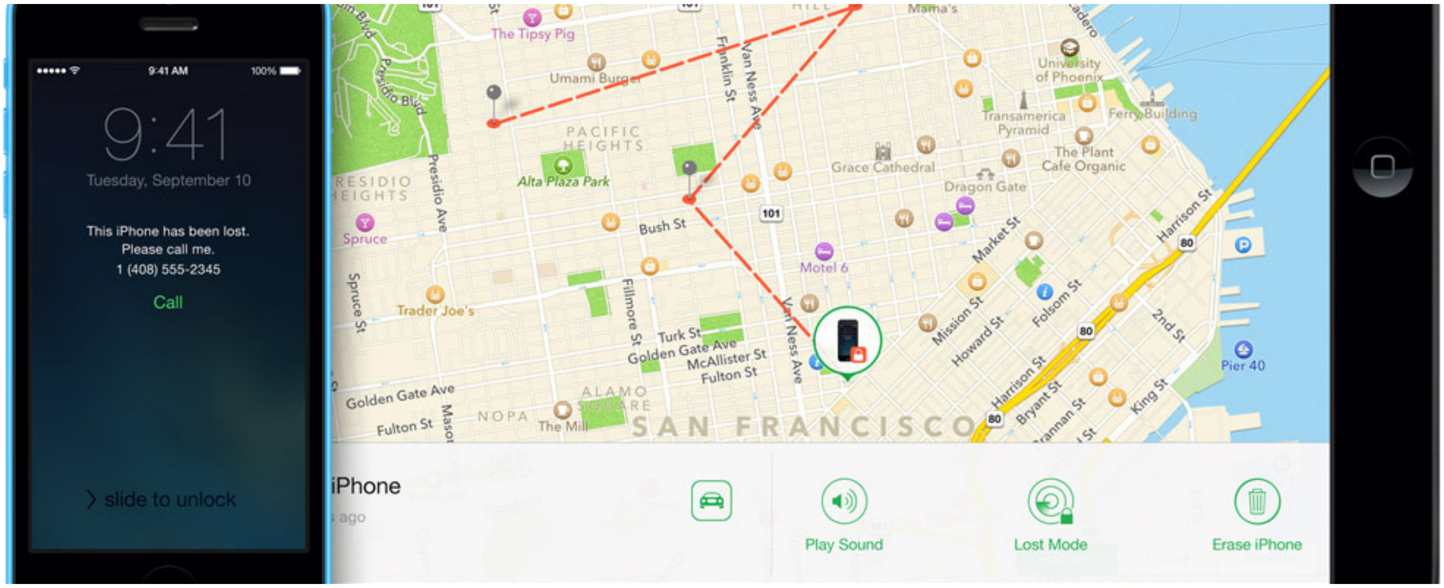
I strongly recommend that you **make your phone harder to hack** by strengthening your password in two ways:

1. **Enable a biometric password** (like a thumbprint or facial scan) to make unlocking the device more convenient (and for the most part, more secure). I highly recommend this step on Apple devices, as they are very secure from a biometric standpoint. Android phones, because they are made by different manufacturers, are less tightly controlled and therefore generally less secure. I would complete more independent research before enabling this feature on

your Android phone. While biometric passwords, like any other technology, are not fool-proof from a security standpoint, they do increase the likelihood that you will put a long and strong passcode on the device (because you only rarely have to type it in, you simply activate the biometric in its place). In addition, you should…

2. **Use a 6+ digit alpha-numeric passcode.** Most of us have been conditioned to use 4-6 digit numerical passcodes on our phones. This length of passcode is relatively easy to hack. I suggest that you make an alpha-numeric passcode on your phone that is longer than 6 digits. This stronger passcode is then coupled with your biometric password, making it simple to login biometrically 95% of the time. When you restart your phone or make any system changes, you will have to re-type your full password, but that will be infrequent.

3. **Use a SIM card lock.** A screen lock is helpful but won't stop a criminal from removing your SIM card (which is full of your identity) from your phone and using it on another phone. To prevent this from happening, set up a SIM card lock in the form of a PIN number (Apple, Android) that will need to be entered when a phone is turned on in order to connect to a network.



This iPhone has been lost.
Please call me.
1 (408) 555-2345

3. Enable Remote Tracking and Wiping Capabilities.

A good IT department won't allow mobile phones out of their organization prior to taking most of the steps listed in this document. The minimum requirements, however, are the use of passwords, remote wipe and remote tracking. Even if your company does not take these steps, you should, as it could mean losing your job if company data is breached on your mobile phone (or losing your identity if you use it personally).

Remote tracking means that as long as the power on your mobile phone remains on, you can physically track the location of the phone (thanks to the GPS inside). This feature has actually been used to catch criminals in action. Remote wipe means that if your phone is lost or stolen, you can remotely clear all of your data – including e-mail, contacts, photos, videos, texts, and documents – off of the handset, immediately eliminating the risk posed by loss or theft (as long as your password is long and strong enough to repel password cracking software while you remotely access, track and wipe the mobile phone). To see remote tracking at work, take a look at this short video, How to Bulletproof Against a Stolen Smartphone.

If you are utilizing a company mobile phone, it is probably wise to let your IT department set this feature up for you. To set up remote tracking and wiping capabilities on a personal or small business smartphone, follow the instructions on the Android Find My Device or Apple Find My iPhone websites. Mobile phone Apps like Lookout, McAfee and Bit Defender Mobile Security also provide remote tracking capabilities as well as mobile phone security software. Remote tracking is also handy when you forget where you left your phone last.

Even if you don't enable remote wipe or remote tracking, you still have options. If your phone goes missing, you should contact your wireless provider and have them immediately shut down service. This is a pretty easy way to keep a thief or opportunist from using the phone or running up charges.

4. Install Security Software

Hackers and advertisers target their malware (viruses, worms, Trojans, botnets) and adware at the operating systems with the greatest adoption in the market (Apple iOS, and Google Android). A huge majority of Americans now own a smartphone. This makes it a very attractive target for the types of attacks we have always tried to prevent on our computers. Mobile hackers focus on installing rogue software on your phone that turns control of your device over to them. They might do this by getting you to click an enticing link (which downloads malware) or installing a seemingly useful App that is meant to siphon your information back to their waiting servers.

Mobile attacks have many sources, including malicious texts and email links, infected software from dodgy websites and even compromised code from legitimate App stores. No matter how carefully App stores vet the Apps they offer, some malware is bound to slip through the cracks.

Smartphone security software isn't bulletproof, but it does add another layer of protection to your device. Because software changes so quickly, I would recommend reading reviews of mobile phone security Apps on your App Store of choice as well as at a software review site that you trust. Consumer Reports recommends both McAfee and Avast Mobile Security. Good security software will allow for remote tracking and wiping, will scan your phone for malware/spyware, and even examine downloaded applications. It's somewhat difficult for security software to detect malicious texts or spam, so don't click on that link (in email or text) unless you were expecting it.

One recent example of mobile malware is a password stealing App, distributed on Google Play as a Trojanized version of Instagram. The app is marketed as a set of tools and utilities to help users gain Instagram followers and analyze usage data. The malware leads the user to a phishing website with a simple design that makes it difficult to distinguish between what's real and what's no, easily capturing the user's login credentials. Security software won't catch all of these malicious apps, but it will catch more than having no protection at all.

5. Load Apps & Data with Discretion

It goes without saying that you should only put data on a smartphone that you absolutely need. Files that aren't there can't be stolen. But since most people want full functionality from their smartphone just like their computer, it's important to take additional steps to protect your files.

Wherever possible, utilize mobile Apps that require a password to get into the App itself, especially if the application has access to financial accounts. For example, password managers like 1Password, Dashlane and LastPass require you to enter a separate password from the device password to access their contents. That way, if a thief gets ahold of your phone, they still can't get into your password vault (without forcing you in some way). The same is generally true for well-protected banking, investment and financial Apps. If you can get into the App without an additional password, you are poorly protected.

Many Apps are now tied to the biometric passwords stored on your device. This is a convenient way to lock and unlock access to Apps, but does have its risks, as you are using the same password to get into the phone and into the App. If criminals are able to hack the first version, they will immediately have access to any apps that utilize that same password. While this isn't a huge concern, it is worth considering.

If you are using Cloud Computing Services like Salesforce.com, DropBox, Evernote, Google Drive or other popular App/Cloud services, make sure you turn on password protection at the software level as well as the device level. In the case that you set your smartphone down when it is still logged in, you don't want a thief to also have access to these accounts.

Finally, when you are finished using your phone and are planning on giving or throwing it away (or returning it to the I.T. Department or even stuffing it in a drawer), make sure you completely wipe all of the data off of the phone. This should include removing the SIMM card and erasing any internal memory on the device. Remote wiping is an efficient and effective way to perform this function, but not as comprehensive as actual device-wiping software.

6. Minimize Unnecessary App Spying

How do you know that the application (App) you are downloading and allowing to access your Smartphone (and all of the data on it) is legitimate? In some cases – you don't. And how do you know that someone else hasn't installed a tapping App on your mobile phone without your knowledge? Often, the secretive App installation is done by a disgruntled spouse, a nosy employer, a sophisticated competitor or a thief who convinces you to click on a malicious link and install spying software.

Apple tries to minimize the number of malicious applications in its App Store by using a centralized screening process to certify the security of every App. They do acknowledge, however, that malicious applications have snuck through. Google Play tends to put users in charge of their own security, which means Droid users are generally less protected from malicious apps. All of the application stores will remove false apps when they are aware of them, but it can sometimes be too little too late.

In addition, some of the very most popular and legitimate Apps are interested in your data as well. They don't intend to steal from you, but they are collecting, aggregating and selling your private information for a profit. After examining over 100 popular apps, the Wall Street Journal found that 56 of them transmit the phone's unique device ID to companies without the user's knowledge. Forty-seven of the applications transmitted the phone's actual location, while five sent other personal information such as age and gender. This shows how many times your privacy is potentially compromised without your knowledge. Take these steps to better protect your privacy:

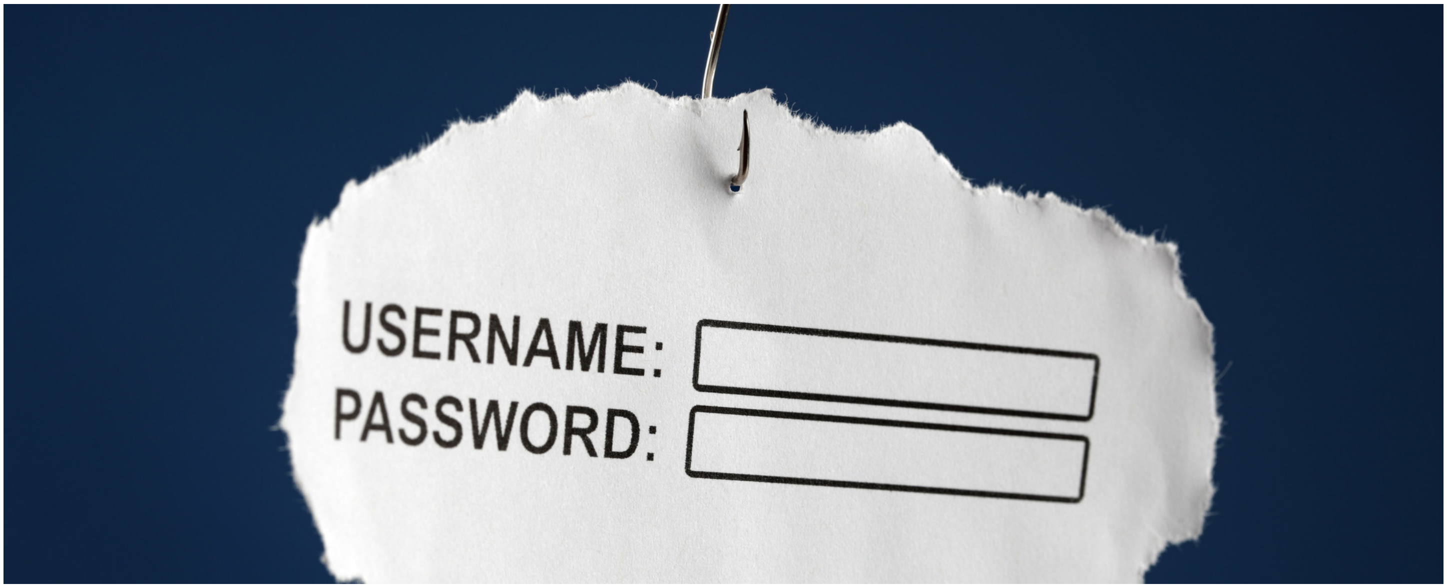
1. Minimize your exposure by **limiting the number of Apps on your phone** to those that have been publicly and positively reviewed, have been around for more than 6 months and are software that you will actually use.

2. **Adjust your Privacy & Location Settings** (Apple, Android) so that only critical Apps have access to your location, and only when you are using the App. If the App is turned off, it should not be tracking your location. Every month, Apple and Google are adding additional privacy and security features to their smartphones. I recommend spending 30 minutes once every 6 months going through every security and privacy setting in your phone to maximize your protection.

3. If an App (like Facebook or Instagram) requests permission to access your personal data (contacts, photos, texts, cell number, current location, etc.) make absolutely certain you want to share that information before your grant permission.

4. Realize that paid Apps tend to transmit less personal data than free Apps. After all, the free Apps have to make money somehow and your information is their inventory.

5. If you no longer use an App, or are suspicious about it, remove it from your phone.



7. Don’t Click on Malicious Links (In Emails or Texts)

Just like computers can be compromised by phishing (learn more about that in this Anti-Phishing Video), so can smartphones via both email and text message. SMiShing (a mashup of SMS text and Phishing) uses cell phone text messages to deliver the “bait” which entices you to 1) Download device-takeover malware or 2) Divulge vital login and password information. The “hook” (the method used to actually “capture” your information) is usually a disguised URL that looks like it’s taking you one place while it actually takes you to another. To minimize your risk:

1. Don’t click on links in emails or text messages unless you were expecting to receive them and know exactly where they point.

2. Whenever possible, instead of clicking the link, surf directly to the legitimate website.

3. Understand that no legitimate bank, business or financial institution will EVER ask you to divulge or confirm your personal information via email or text message.

4. Install 3rd-Party Spam Filters on your email service to eliminate a majority of phishing emails. Unfortunately, this doesn’t work for malicious links sent via text message.

8. Secure Your Mobile Banking, Investing and Shopping

Mobile banking and investing has come a long way since it first showed up on smartphones. I am a fan of online banking, as long as you are taking the appropriate security measures:

1. Only utilize banking and investing Apps from reputable financial institutions that have had their App available for at least 6 months. They need time to work out the bugs. In general, I prefer to use banking Apps over directly surfing on a mobile web browser, as the Apps tend to be more secure than the browser.

2. Don't bank, invest or shop online from a public Wi-Fi connection, as they are commonly "sniffed" by thieves. Instead, utilize your cellular connection (LTE, 5G, etc.) or your own, encrypted Wi-Fi connection. (See Step 10 Below for details).

3. Make sure that your financial Apps have a separate password to get into the App or website. If they don't anyone with access to your unlocked phone can bank or buy as you.

4. Turn on Two Factor Authentication, which makes it far harder to compromise your bank, investment and shopping accounts. Watch this short video for background on Two Factor Authentication.

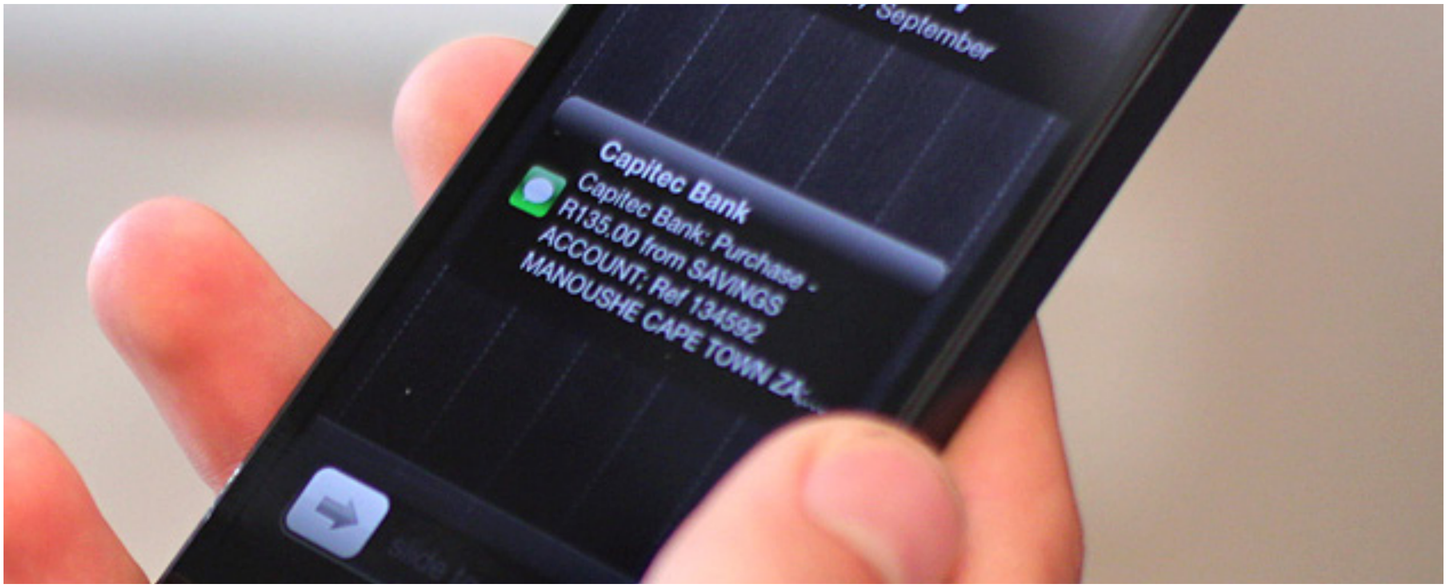
5. Always log out of banking, investment and shopping Apps (and websites) when you are done.

9. Don’t Get Juice-Jacked at the Airport or Cafe

You know those USB charging stations you see at the airport? Don’t go near them! USB technology isn’t just a means of charging mobile devices, it was designed to suck data back and forth between devices and hackers have figured out a way to preload the USB port with malware that drains your data. I know, there’s nothing sacred anymore. It’s particularly frustrating when you get the “Your battery is below 20% and will go to sleep” message right in the middle of something important.

Hey, we don’t get to take naps when we’re at 20%, do we? And then we panic, desperate for just a little juice, and plug our devices into the nearest rectangular object around. Before you know it, voila, your phone contracts a serious infection and starts gossiping about you with the nearest cybercriminal.

This hacking method is called juice jacking and it is similar to ATM skimming. All it takes is for you to plug a USB cord from your smartphone into one of these ports to transfer all of your private information, including passwords and banking information stored on your phone. If you need to charge your device, use the old-fashioned kind of charger with a plug (no data transfer there), or plug it directly into your anti-virus protected laptop which you THEN plug into a wall. Outlets are your friend, USBs your foe.



10. Use Tethering and Mobile Account Alerts to Your Advantage

Smartphones are not just a risk in the data protection game; they can also be used as a tool to lower your risk. Here are two examples of ways that you can put your Smartphone to work in the fight against data theft.

Smartphone Tethering

Another major source of data theft is Wi-Fi hotspot usage. Most Free hotspots do little to protect the data that you transmit over the wireless network. In fact, many home and company wireless networks are not set up to provide a secure connection to the internet and are, therefore, no safer than those you access for free in cafés, airports and hotels. Just say no to using free Wi-Fi hotspots, on your phone and your laptop. The most common form of exploitation associated with hotspots are "man-in-the-middle" attacks where a spy intercepts the transmission between your wireless network card and the cafés wireless router or modem.

Using a legal, free and simple-to-use tool like Firesheep, a thief (or competitor, foreign actor, etc.) can sit next to you in a café and "sniff" your connections. Luckily, your smartphone can provide a proactive way to help you protect your connection to the Internet when surfing wirelessly.

Tethering connects your computer to the Internet using a smartphone and the data connection (3G, 4G, LTE) that is built into the phone. It encrypts the mobile transmission between your cell phone and the cell tower. Therefore, when you use your Smartphone to surf the web, you are accessing a protected connection that probably can't be sniffed. The connection might be slightly slower than a traditional Wi-Fi hotspot, but it is also much safer. The Smartphone can be tethered in three basic ways:

1. With a tethering cable (usually USB to Smartphone connection). This is the safest option because it is a direct connection between your phone and your computer, eliminating any wireless sniffing between those two devices.

2. With a Bluetooth wireless connection. If you don't use an encrypted Bluetooth connection, spies can sniff the data as it crosses from your computer to your phone. In addition, turning on Bluetooth functionality opens up one more door for hackers to gain access into your system.

3. Wi-Fi. If connected through Wi-Fi, the tethering feature is usually called a mobile hotspot, and can often connect to multiple devices. Again, if you utilize Wi-Fi tethering, you need to make sure that the connection between your computer and the mini hotspot is encrypted so that data isn't intercepted before it heads to the Internet.

Most Smartphones are equipped with software to provide tethered Internet access via Bluetooth or a USB cable. Tethering may be provided as part of your monthly data plan, but I wouldn't count on it. I tend to use tethering anytime I'm sending emails, dealing with financial institutions or handling sensitive data. If I'm simply surfing news or sports sites, then I'm more comfortable using the free Wi-Fi connections (as long as my computer is protected with a firewall against hackers gaining access into my laptop via file sharing over wireless). I generally also log in as a different user on the laptop with very restricted access. This will minimize collateral damage if a thief does back their way in to your connection. Finally, I carry a laptop with very little sensitive data on the hard drive to minimize what can be lost or stolen.

For added security, set up a Virtual Private Network (VPN) that protects the data from the moment it leaves your device to it's final destination. A VPN provides secure access to an organization's network and allows you to get online behind a secure layer that protects the data being transmitted back and forth. If you have access to a VPN, I highly recommend that you use this when using Wi-Fi.

When you are not using Bluetooth or Wi-Fi, turn them off. The most likely way that your smartphone can be compromised is by downloading malware concealed in a file or App. Both Wi-Fi and Bluetooth provide a doorway into your mobile phone (especially when they are set up without security in mind). When they are turned on, they actively try to connect to other networks, even when those networks are run by dishonest people. In addition, if tethering is set up incorrectly, it can give the criminal access not only to your Smartphone, but also to your computer. When not in use, turn them off and eliminate chances of foul play.

Mobile Account Alerts

Virtually every major credit card company, bank, mortgage broker and investment firm will allow you to set up account alerts inside of their App. The alerts notify you immediately when a withdrawal, transfer or other transaction is made on your account. Spend $5 on coffee; you get an alert, either in the App itself or by email or text. The alerts allow you to keep frequent tabs on financial transactions, increasing the chances that you will detect fraud quickly. Account alerts are one of the most powerful and least expensive (free) methods for monitoring your valuable financial accounts.

About John

John Sileo's identity was stolen and used to embezzle $300,000 from his clients. The exposure destroyed John's career and consumed two years of his life as he fought to stay out of jail. Combining real-world experience with years of study, John became an award-winning author and leading expert on cyber security, identity theft and data privacy. John is CEO of The Sileo Group, a data security think tank that helps organizations protect the information that drives their profits. His body of work includes engagements with the Pentagon, USA Today, Visa, 60 Minutes, Homeland Security, Rachael Ray, Schwab and organizations of all sizes. John graduated with honors from Harvard University and spends his free time with his remarkable wife and two highly spirited daughters.