



7 Simple Smartphone Privacy Tips:

An Exclusive White Paper for Deluxe® Customers by John Sileo



Most business people think of their smartphone as a highly critical and necessary tool in running an efficient and competitive operation. In other words, their jobs depend on it.



Many thieves, on the other hand, think of your smartphone as an effective key to unlock your personal wealth and hijack your company's sensitive data. And why wouldn't they? These days, the average smartphone contains nearly as much sensitive information as a fully functioning laptop computer. In addition to carrying contact information, business people tend to store user names and passwords, bank log-ins, account details, sensitive emails, customer records and competitive data on devices that are as easy to misplace as our keys. Combine this raw computing power with mobility, sprinkle in the distractions and demands of a small business, and you have a recipe for potential disaster.

Just as we equip our computers with the latest in security technology and train users to avoid fraud, we must also protect our smartphones against identity thieves, hackers and competitive espionage. The following *7 Simple Smartphone Privacy Tips* will get you started.

› 7 Simple Smartphone Privacy Tips

1. Lock it up & don't lose it.

Mobile phones are small and get used constantly, which makes them extremely easy to steal. In our push to be tech savvy, we often

Cendant Technologies, a data-protection company, discovered that travelers have lost 11,000 mobile devices at the busiest airports in 2011 alone.

forget the simplest solution for protecting the data on the device – lock it up and don't lose it. Keeping your phone physically on your person 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 moment. Many phones are stolen from restaurant tables, coat

pockets, shopping carts, airport security bins, taxis and car cup holders, while they are momentarily unattended or left behind.

In addition, be careful to whom you loan your cell phone. Here's the latest scam: Someone asks to borrow your phone to make a quick, urgent call. You think they are tapping out a phone number, but they are actually installing a malicious application (app) that allows them complete remote access to the contents of the phone, even after they've handed it back to you. The entire process takes about 45 seconds.

In case you do lose your smartphone, make sure that you have a recent backup or sync of the phone's contents so that you don't lose that as well.

2. Turn on password protection and the auto-lock feature.

All smartphones have password protection features that can be turned on to help keep unwanted users out. If you configure the settings properly, the phone will auto lock itself after a few moments of inactivity. Getting back in requires a simple 4-digit passcode. This single step is as vital as password protecting your laptop computer, a practice that can save you from losing thousands of dollars due to unwanted intruders. If nothing else, passwords slow down the thief long enough to give you time to remotely "wipe" your memory (see Step 3). Don't make the password easy to guess (7777 or 1234), as thieves already know the most common combinations. Stay away from birth dates, addresses, phone extensions and other obvious codes.

Make sure that you set the auto-lock feature (the amount of inactive time before the passcode kicks in) to no more than 2 or 3 minutes. It can be inconvenient to type in a passcode every time you use the phone, but it doesn't compare to the inconveniences a stolen phone creates.

3. Enable remote tracking & wiping capabilities.

A good IT department won't allow mobile phones out of their site prior to taking most of the steps listed in this document. Even if you don't have a dedicated IT department, you should take the

same amount of care. If you don't, it could mean losing your job if company data is breached on your mobile phone (or losing your identity when personal information is taken).

Remote tracking allows you to physically track the location of the phone as long as the GPS (Global Positioning System) function is turned on and the phone is not powered down. If your phone disappears, you simply log on to the tracking software from your

One lost smartphone can cost a business thousands of dollars and untold downtime. Recovering is quite possibly the least efficient way to spend your limited time and money.

computer and locate the phone. GPS is the same technology that allows you to use mapping software on your smartphone, so it is common and almost always on by default. Remote tracking has actually been used to catch criminals in action.

Remote wiping takes protection one step further. If your phone goes missing, you can remotely

clear all of your data – including email, contacts, photos, videos, texts, and documents – off of the phone, immediately eliminating the risk posed by loss or theft. If your password is strong, you should have at least an hour to log in to your remote software and wipe the contents of the phone. Many smartphones come with remote tracking and wiping built in to their operating systems. If not, you can generally purchase a mobile app that provides this type of extended security.

4. Utilize Password-Protection Software.

Admit it, you use the same easy-to-remember password for multiple websites. It's not a crime (well, at least not yet). And, now that you have started to use your phone as a computer (email, surfing, calendar, contact manager, mobile banking), you occasionally need those passwords on your mobile phone. But, the passwords you store on your smartphone are only as effective as your ability to use them wisely. If you store passwords in an unencrypted file (e.g., address book, spreadsheet or note-taking program), you are begging data thieves to break into all of your accounts, not just one. By the same token, if you use the same password for multiple sites, you are putting all of your valuable financial accounts at risk. Once a thief

has one of your passwords, they enter it into a software program that tests it against every financial website.

A potential solution, one that doesn't require you to remember hundreds of different alpha-numeric passwords that look like this – tR\$y%7!x;@qa8& – is to download a reputable password-protection app for your mobile phone. Password-protection software gives you the tools to securely manage and protect sensitive passwords, financial data, credit card numbers, online identities, software licenses, etc., behind a single, secure password that you memorize. As long as you protect that one password, you are far more secure than if you continue to use insecure password practices. Password protection software will help you lengthen, strengthen, vary, change and encrypt these crucial keys to your net worth.

5. Minimize unnecessary application spying.

Several months ago, Google was forced to withdraw more than 50 apps from the Android Marketplace because they were posing as banking apps but funneling users' private data to criminals. So how do you know that the 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.

In fact, some of the most popular and legitimate apps are spying on you as well. They don't intend to steal from you, but they are

Indiscriminately downloading apps onto your smartphone is a guaranteed way to allow thieves and competitors access to everything on the handset.

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. Companies purchase this data in order to market to you in a more targeted way.

There is no perfect solution to prevent malicious apps from infecting your smartphone. However, here are a series of suggestions to minimize your chances of installing an application that shares or steals your information.

- Never open email, text, video, photo, social networking or other unknown documents or attachments from untrusted sources.
- Never click on shortened links unless you are highly confident they are from a trusted source.
- Apps, even legitimate ones, often capture and transmit a variety of your personal information. If you are using smartphone apps, face it, your information is being transmitted. If you want to understand the extent to which your information is being shared, read the privacy policy for that application.
- Get your apps from a trusted source; don't just install the latest fad. Stick with app stores that are monitored and written up in journals, and only download apps that have been out for more than six months.
- Paid apps tend to transmit less personal data than free apps. After all, the free apps have to make money somehow!
- If an app gives you the option to opt out of information sharing, take it.
- When downloading applications, do your research first. Has the app been reviewed by a reputable source (*Macworld*, *PC Magazine*, *PC World*, *WSJ*, *NYT*)? This doesn't guarantee security, but it does lower your chances of downloading malicious software.
- If an app requests permission to access your personal data (text messages, cell number, current location, etc.), make absolutely certain you want to share that information before agreeing.
- If you no longer use an app, or are suspicious about it, remove it from your phone.

6. Hold off on mobile banking & investing.

Sometimes there is no possible way to prevent identity theft. The reality of living in the information economy is that your identity will occasionally be compromised. But, don't worry, if you catch fraud quickly, you shouldn't lose much.

Because of all of the risks of data leakage posed by smartphones and the relative youth of security in the mobile phone space, I don't yet recommend using online banking and investing apps or browser-based banking. For now, the security on mobile phones is in its infancy and the attackers are many steps ahead. All it takes is for one rogue app to funnel your brokerage login credentials to an outside source and your net worth could be eliminated. The risk, for now, is too high. Contain your online banking and brokering to a home-based or business-based computer system with all of the proper security precautions (strong passwords, anti-virus and anti-spyware software, firewall protection, updated operating system patches, etc.).

7. Customize your geo-tag & GPS settings.

Geo-tagging allows others to track your location without your knowledge. With the increased use of Internet-enabled smartphones, geo-tagging has exploded in popularity. For example, when social media users take a picture or video and upload it to a social media page, they are probably transmitting location data that can be easily read by others.

Your real-time location makes it easy to determine your home address, work address, places you visit often and your daily schedule. Checking in to social location websites like FourSquare or Facebook makes it simple for friends, relatives, bosses, spouses, parents, enemies, law enforcement, stalkers, and thieves to know exactly where you are.

Most smartphones allow you to control GPS features application by application. So, for example, you can keep location services turned on for your mapping program, but restrict access for other programs. Spending a few minutes examining these settings will increase your privacy and safety.

A smartphone can be a highly effective and efficient tool, for personal and corporate users. But like any powerful piece of equipment, you must take the time to protect it. The more you think of your smartphone as a computer and the less you think of it as a phone, the more secure you will be. Take steps now to protect this asset.



John Sileo lost almost a half-million dollars, his business and his reputation to identity theft. Since then, he's become [America's leading keynote speaker on identity theft](#), social media exposure and weapons of manipulation. His clients include the Department of Defense, Pfizer and Homeland Security. To learn more, visit [ThinkLikeASpy.com](#) or contact him directly on 800.258.8076.

› **Fight Fraud and Reduce Risk with Security Products and Services from Deluxe.**

Deluxe Security Solutions provide a number of highly innovative products to protect your business transactions and assets. From our new [High Security Checks](#) with 22 advanced security features, to our [Security Pens](#) with special ink that helps prevent against check washing and document fraud, we have the [High Security tools](#) you need to feel secure.

Visit deluxe.com/highsecurity or call **800.328.0304** for more information.