iPhone Privacy - Best Practices & Security Tips

By Trey Peacock, Winning Cases Based On Science & Data For Over 25 Years
Originally published on LinkedIn.com

Left behind in an Uber. Lost in the chaos of an airport. Abandoned in a hotel room, or pilfered from a coat pocket. The potential scenarios for losing access to your phone are endless. I dare say many of you have experienced one or two of them already, now that we're fast approaching the 16th generation of iPhone. But despite how common these occurrences are, losing your phone — or having it stolen — doesn't get less annoying over time. In fact, as thieves become less scrupulous and more determined, they have learned that the real value isn't in the phone itself. It's the precious data that lies behind your lock screen. Earlier this summer, the *Wall Street Journal* did a **story** on some of the more aggressive efforts thieves are using to steal your passcode, swipe your phone, and then lock you out of all your data, including photos, passwords, and other private information.

To that end, I've gathered some of the most effective, and easily implemented tips that can help you safeguard your data, money, and privacy from snoopers and thieves. Properly protected, your iPhone can easily become a digital fortress the moment it leaves your possession. Then, you can rest easy knowing that even in the face of theft, your accounts and files remain secure.

Tip #1 - Guard Your Apple ID Password & iPhone Passcode

If you think of your iPhone as a castle, then your Apple ID and password are like the coin of the realm — the currency that opens all doors and passages. You need your Apple ID password to change most of the crucial settings required for turning a phone over to another user. They also act as the last line of defense to preserve the phone's allegiance to you and your data when your device is completely lost. Your Apple ID password is tied to the email account you use to log into your iPhone in Settings. Make sure that the password is unique, complex, lengthy, and not used for any other account.

Set a stronger passcode.
It's likely that your passcode is a 4- or 6-digit passkey that your friends and family have seen you type in a thousand times, heard you shout across a crowded room or car, or that you generally have not cared too much about keeping secret. That should change immediately. As the WSJ notes, thieves can easily observe your entry of that passcode from afar and enter it once they steal your iPhone. Once a thief changes that passcode, he can easily access and change other settings on your phone that effectively bar you from your own data. I highly recommend shifting to a longer, 10-character alphanumeric passcode that's entered via the keyboard rather than the traditional number pad. This makes it both harder to crack by force and more difficult to detect by snooping. To do this, go to your Face ID & Passcode Options in Settings, enter your passcode, then select "Change Passcode" and enter it again. Then tap "Passcode Options" and select Custom Alphanumeric Code. If you want further protection, purchase a glass privacy screen filter that makes it highly difficult for nearby onlookers to see what is on your screen. Here is a link to the **one I use**.

Add a Screen Time passcode.
In addition to keeping your kids' screen time and app store purchases in check, the Parental Controls features in your iPhone make a handy tool for adding another layer of security to foil thieves as they try to unlock and unregister your device. By adding a Screen Time passcode, thieves will need to crack not one, but two passwords before claiming your phone as their own. To enable Screen Time passcode, go to Settings and find the Screen Time heading. Scroll down and tap "Use Screen Time Passcode" to set a passcode (should be a unique one). Then, tap the Content & Privacy restrictions banner and set it to ON. Make sure to check the box for "Don't Allow" changes to your passcode, account, and cellular data.

Tip #2 - Guard Your Passwords

This one is pretty self-explanatory and one I have addressed several times in these articles. Just like you wouldn't leave the front door of your house unlocked, don't leave your accounts unprotected. It's like inviting a hacker in to steal your data. Sort of.

Use a third party password manager.
Get any sensitive passwords — especially those for banks and payment systems — out of Apple's proprietary iCloud password manager. Any information stored there can be accessed through your Apple ID, so if that gets breached, the floodgates are open. To prevent that, try to create redundancies and extra barriers by using a separate service, like Dashlane or 1Password. With both of those services, you'll set a unique, long, alphanumeric master password, and can choose to enable Touch ID or Face ID access as well.

Use an authenticator.
Most of these services also offer the use of an "authenticator" that takes the place of pesky codes sent through text (which can be intercepted by hackers and thieves) and instead generates a unique, random, one-time code on your phone or tablet that allows you to log in to whatever account you've paired up with. This authentication functionality is handily included in Dashlane and 1Password. As such, accessing the authentication will require access to a password separate

and unique from your Apple ID password that a thief cannot access. If you want to go an extra step (I have), you can pick up a physical authenticator or passkey like the Yubikey. This is a USB or NFC enabled device that requires proximity to the device attempting to enter an account in order for access to be granted. Pretty futuristic right? Go ahead, Ethan Hunt, treat yourself to a Rabbit's Foot.

Tip #3 - Guard Your Files & Photos

Though the convenience of Apple's iCloud ecosystem is hard to resist, we'll repeat once again: the name of the game is redundancy. If that account is breached, all your data will be available to thieves or snoopers. That's bad enough — but it's even worse if they lock you out of your own data. Then, not only will they have all of your data, you will have none. To prevent that dire scenario, make sure to keep your files in a location other than iCloud like OneDrive or Google Drive. At a minimum, if you are going to use iCloud Drive which is tied to your Apple ID and password, please back up your files and crucial data on one of these services. That way, even if your data is breached, you won't completely lose access to it. You should also back up your photos. Everyone keeps a ton of cherished memories going back years in their Photos app—I certainly do. Imagine how crushed you would be if a thief locked you out a lifetime of memories.

Tip #4 - Guard Your Money

Ahh money. It makes the world go round. It makes something from nothing. It makes our pockets heavy in good times and light in the bad. Or, at least, it did, before money, like everything else in our lives, became subsumed into the digital ecosystem and governed by apps, firewalls, usernames, and passwords. Cash has become almost useless. As a result, it's extremely important to take conscious steps to preserve the integrity and security of your personal finances. No one hides a wad of cash under the mattress anymore. Your financial future is in your hands. Literally.

First things first — remove any sensitive information from iCloud enabled apps including Photos. If a thief gains access to your iCloud account, the last thing you want to do is lead them directly to your digital bank vault. Search through your Photos app, your Notes app, and your iCloud password manager and remove anything with a direct mention of your Social Security number, ID number, passport info, bank account information, usernames, passwords, anything. If you must keep copies of this info handy, store it locally on one device that doesn't leave your home, or print out a hardcopy only when absolutely necessary, like when going to the DMV.

Tip #5 - Guard Your Device

Finally, our simplest yet most important tip yet. Keep track of your dang phone! Reader, believe me when I say I've misplaced or lost a few iPhones over the years. But if you can keep a handle on your physical device, so many potential problems disappear. However, mistakes happen. So — in the event your phone is misplaced, lost, or stolen, please, for the love of Tim Cook, follow these steps to prevent any (further) loss of information, files, or funds.

As soon as you notice your phone is missing, use another device to log into your iCloud account and remotely lock your device so that no one who picks it up off the street can access it. If it's just lost, you can log into iCloud on another device and remotely add a message to the lock screen with instructions on whom to call to arrange a return, and even offer a reward. But if you're sure that the device has been stolen, go ahead and remotely wipe the device. This ensures that thieves cannot access any of the data on your phone, even if it does make it a bit easier for them to flip the bricked phone to a buyer. At least you can rest easy knowing they won't get to raid your *New York Times* Cooking recipe box.

If you've taken any one of these tips (but hopefully all of them) and put them into practice, congratulate yourself. You've just taken a concrete, provably effective step towards protecting your digital identity.

About the Author

Trey Peacock, a partner at Susman Godfrey, has been winning cases based on science and data for over 25 years. He has also chaired the firm's IT committee for over two decades. Learn more about Trey here.