10 Easy Steps to Better iPhone and iPad Security

howtogeek.com/447616/10-easy-steps-to-better-iphone-and-ipad-security

Tim Brookes

ymgerman/Shutterstock.com

There's a good chance you spend more time interacting with the online world on your smartphone than any other device. Let's take a look at how you can up your iPhone and iPad security game.

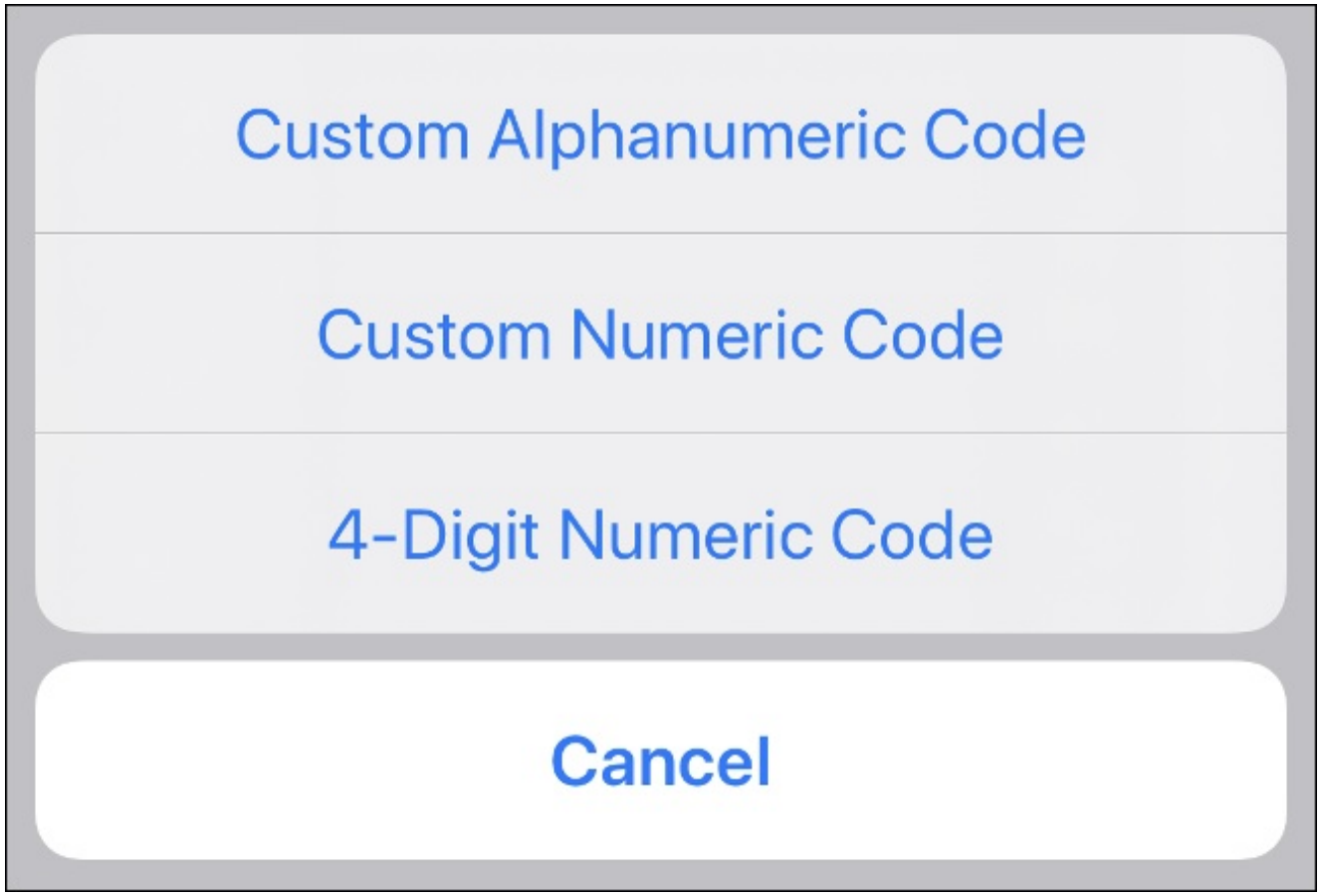
1. Keep Your iPhone (and iPad) Up to Date

It might sound obvious, but keeping your iPhone (or iPad) up to date is one of the most important things you can do from a security standpoint. Security issues are often discovered in iOS, and once they're public knowledge, that means they're ripe for exploitation. Apple regularly patches these holes with incremental updates.

You can turn on Automatic Updates under Settings > General > Software Update so that you never need manually install one of these updates again. Your phone will install any updates for the current version of iOS automatically while you sleep.

You'll still need to manually upgrade your iPhone to the next *major* version of iOS (e.g., iOS 13 to iOS 14) when the time comes. That's by design, and it means you can delay upgrading if you're concerned about the teething troubles that crop up with each new major iOS revision.

2. Use a Secure Passcode and Face ID or Touch ID

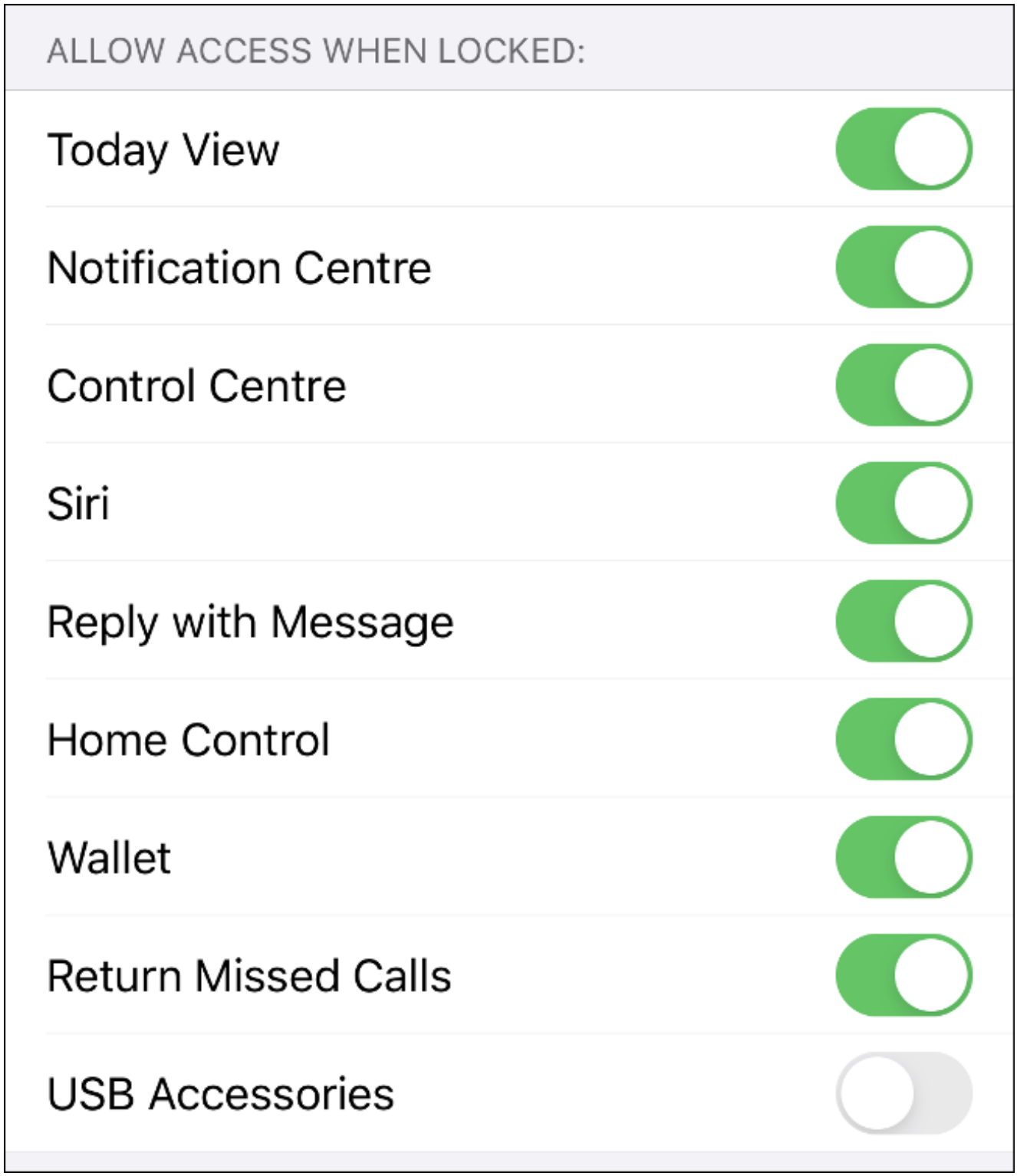


You're probably already using Face ID or Touch ID to unlock your device with your likeness or fingerprint, but how secure is your passcode? The passcode is your device's Achilles heel if someone has your phone or tablet in their hands. It's the only thing stopping a would-be snooper from accessing your entire digital life.

With the arrival of biometrics like Face ID and Touch ID, it's easier than ever to unlock your iPhone. As a result, you should make it more difficult for anyone who isn't you. That means setting a longer, less predictable numerical passcode or even a password that uses more than letters. You'll still have to enter this from time to time, like when your device restarts, but not often enough for it to be a drag.

Head to Settings > Face ID & Passcode (or Settings > Touch ID & Passcode, or just Settings > Passcode depending on your device) and select Change Passcode. When prompted for a new passcode, tap Passcode Options at the bottom of the screen. Here you can decide to use a "Custom Alphanumeric Code," which is what we'd normally call a password.

3. Secure Your Lock Screen



Your lock screen can give away a lot of your secrets. If you receive a text message, it's there for anyone to see. If you ask Siri to read your last message or email, the assistant will oblige. You can even reply to messages and access smart home controls by default.

Since it's so easy to unlock your iPhone or iPad, it's unnecessary to give away so much information while the device is in a locked state. Head to Settings > Face ID & Passcode (or Touch ID & Passcode, depending on your device) and disable any services you don't want

others to access from the lock screen.

If you want to hide incoming notifications until your device is unlocked, you can do so under Settings > Notifications > Show Previews > When Unlocked. This is very convenient on a device with Face ID since all you need to do is look at your phone, and your notification previews will appear. It's a touch less convenient for devices with Touch ID since you have to authenticate physically with your finger.

4. Don't Open Shady Links

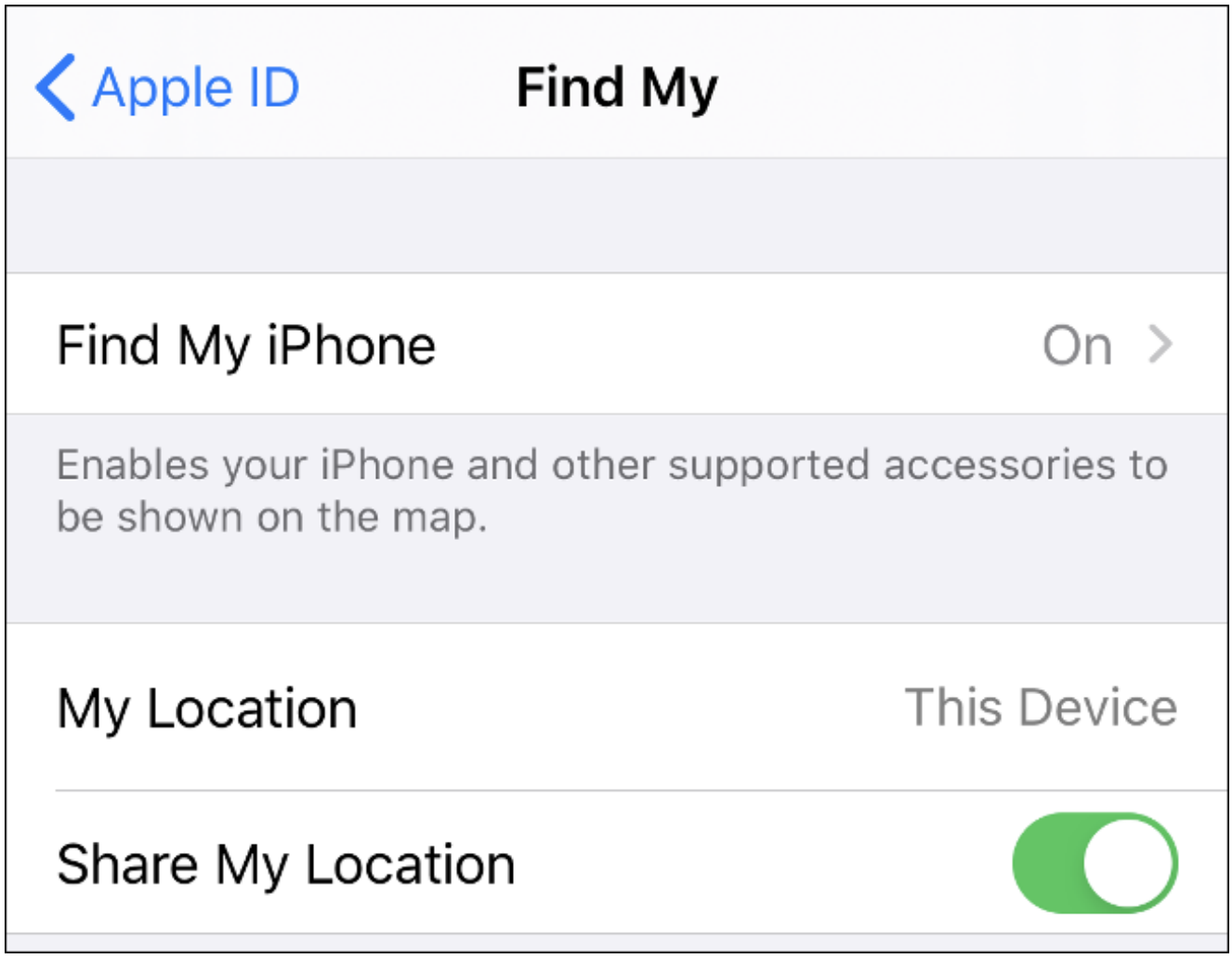
In August 2019, researchers from Google's Project Zero announced they had discovered several compromised websites that had been exploiting vulnerabilities in iOS to install spyware on devices. Apple patched the vulnerabilities, but it is estimated that thousands of users had their devices compromised over several months.

The spyware could reportedly leave Apple's app sandbox and access login credentials and authentication tokens. Contacts, photos, the user's current GPS location, and messages sent via services like iMessage and WhatsApp were all transmitted back to a server once every minute. It's the first exploit of its kind on iOS, but there's nothing to say it will be the last.

Exercise caution when tapping strange links in email or text messages that you do not recognize. URLs shortened with services like Bit.ly are ripe for exploitation. Apple may have plugged these security holes, but vulnerabilities are a fact of life when it comes to software development. It's possible that similar exploits could appear again in the future.

We're not saying you should be afraid to tap on links, but it's best to exercise caution and stay away from shady websites. Bizarre links in emails or text messages from strangers may lead you to phishing websites that try to trick you, too.

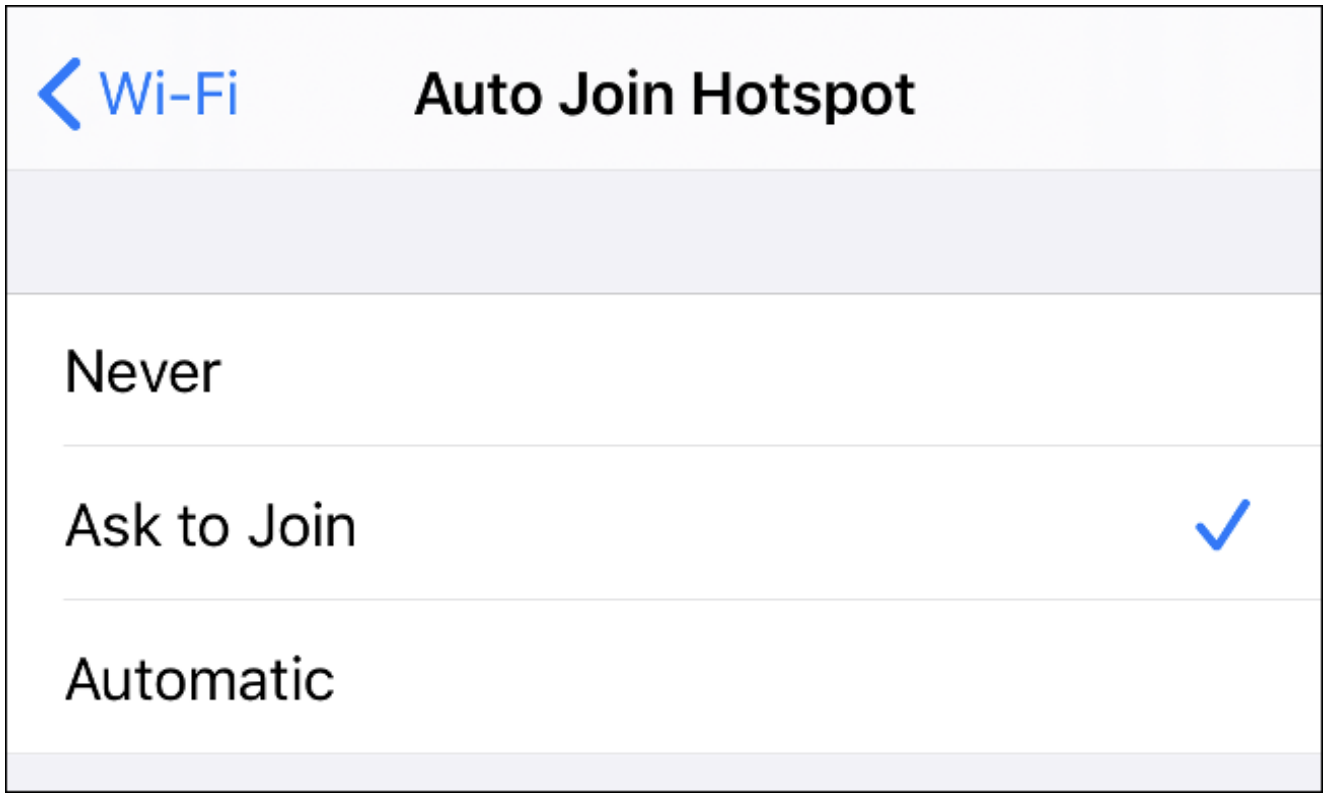
5. Make Sure "Find My" is Enabled



Find My is the new name for a service that allows you to track both your devices and friends. It was previously known as Find My iPhone or Find My iPad, and it will enable you to not only locate your device on a map but also send an audible chime, lock the device, and—in the worst-case scenario—wipe it remotely, removing all your personal data from it.

Most people should have this on by default, but many of us forget to re-enable it after a device repair or software restore. Head to Settings > [Your Name] > Find My and make sure the service is enabled. You can then login to iCloud.com, click on Find My, and see your iPhone listed alongside any other Apple devices linked to your Apple ID.

6. Avoid Using Unsecured Public Wi-Fi



If you aren't taking measures to protect your online traffic, avoid public Wi-Fi networks to avoid falling victim to an attack. Rogue actors can use these services to conduct man-in-the-middle attacks, where they position themselves between you and the wider internet. They then capture web traffic, messages, and any other communication between you and the online world.

The problem is so bad that some public Wi-Fi hotspots are set up by snoopers purely for this reason. They're hoping to snag login credentials, payment details, personal information, and anything else that might have value or benefit them in any way.

Head to Settings > Wi-Fi and set "Auto Join Hotspot" to prompt you when connecting to a new hotspot. If you set this to "Automatic," then your iPhone may join public hotspots automatically.

7. Use a VPN

A Virtual Private Network protects your online habits from prying eyes by encrypting your internet traffic on each end. When the traffic leaves your device, it is encrypted, sent via a VPN to the internet, then decrypted once it reaches its destination. The same happens for the return journey, with the VPN acting as a kind of tunnel to obfuscate your data.

We recommend using a VPN on public Wi-Fi hotspots. With a VPN, it's possible to use public Wi-Fi without worry since your traffic is encrypted and useless to any snoopers.

The easiest way to use a VPN on your iPhone is to download your VPN provider's app and follow the instructions. You can also use a VPN to access geo-restricted content and circumvent online restrictions imposed by governments (though you should only attempt the latter if you know authorities can not detect your VPN).

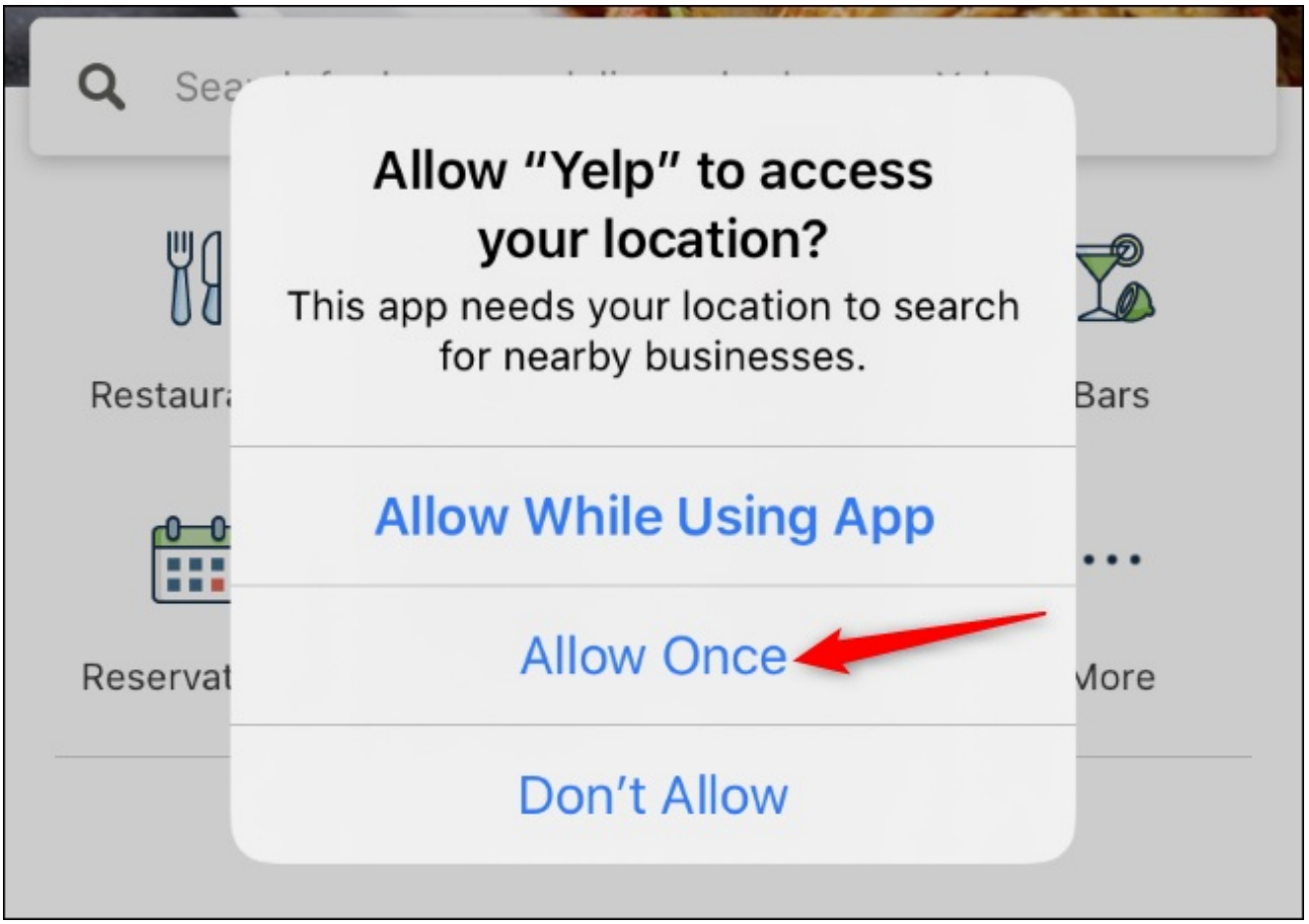
8. Don't Jailbreak Your iPhone

Jailbreaking is the act of installing modified firmware on an iOS device to remove Apple's restrictions. If you jailbreak your device, you can change core iOS behaviors, install software from third party sources, and get unhindered root-level access to the operating system.

This leaves your device in a vulnerable state. Not only can you install fun little tweaks that change the way iOS behaves, but also malware that seeks to harm your device or compromise its security. When you jailbreak, you discard some of the most important aspects of iPhone security, notably the App Store.

But that's not all. Some apps won't work on jailbroken devices, notably apps from financial institutions like banks and online payment processors. If Apple catches you running a modified operating system on your iPhone, you can kiss your warranty goodbye. It's possible to remove the jailbreak by restoring your iPhone using a Mac or PC, but it's not clear whether or not Apple will be able to tell what you've done in the past.

9. Be Careful About Granting Permissions



On an iPhone or iPad, apps have to ask you before accessing your location, contacts, photos, files, camera, Bluetooth radio, and many other resources. You can choose to deny that access if you like. This can break some apps—for example, if you download a third-party

camera app and deny it access to your iPhone's camera, you won't be able to take pictures.

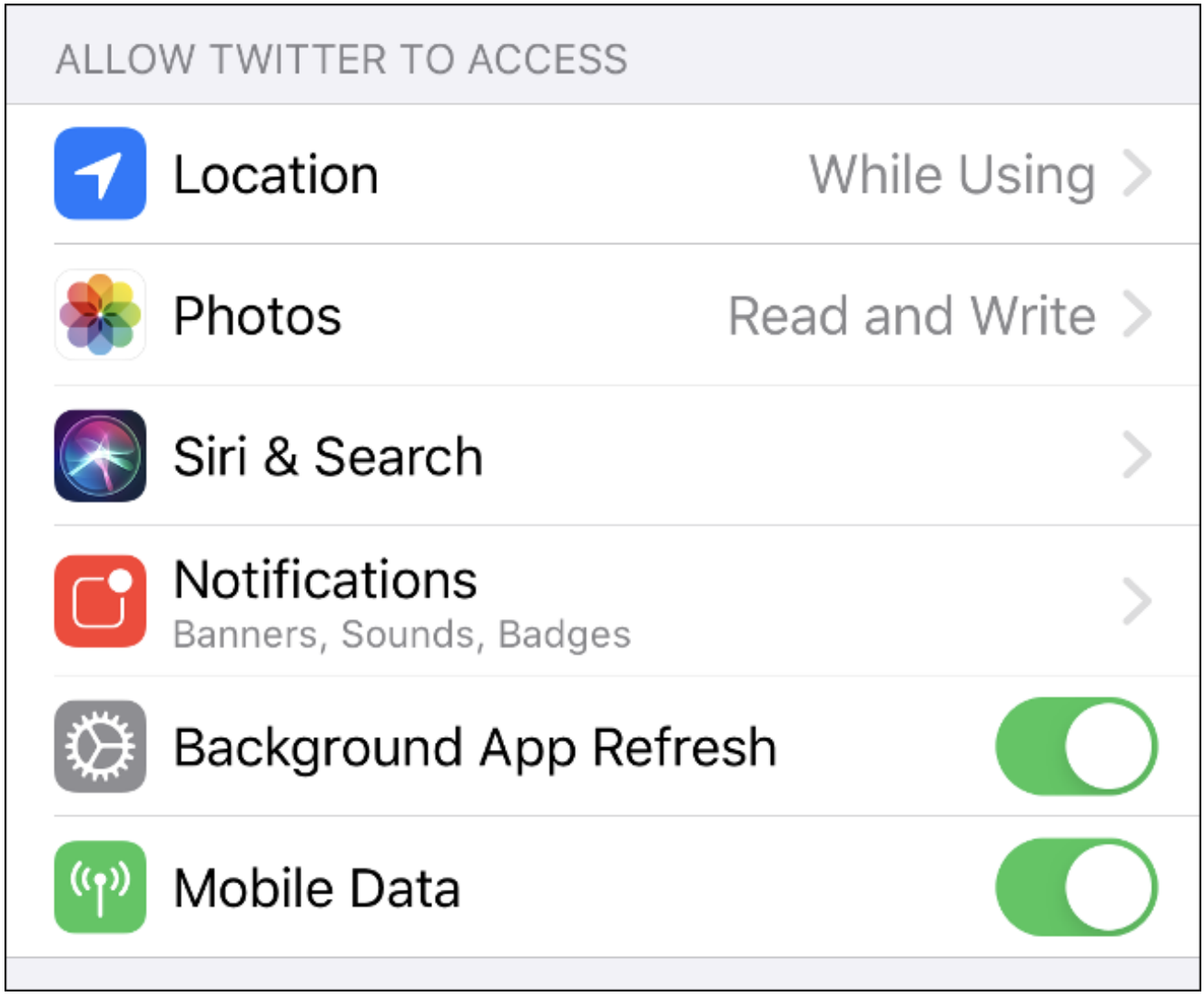
Many apps ask for access to these resources and only need it for specific features. For example, an app may ask for access to your contacts to find friends you can invite to that app. An app may ask for fine-grained location permissions to find stores near you. In both cases, you can avoid giving the app access. For example, you could manually type an address near you to find nearby stores rather than giving your precise location. Or you could give an app access to your physical location only once.

Before giving an app access, consider whether you really want it to have that data. This will help boost the security of your data. For example, an app that uploads your contacts to its servers could later have those servers compromised and leak your contacts. By choosing to be careful about what you share, you're minimizing that risk and boosting your privacy.

10. Regularly Check Your Privacy Settings

Once you've granted that app access, you can be forgiven for forgetting that you have done so.

Head to Settings > Privacy to review your permissions. You can also head to Settings, scroll down until you find the app you'd like to review and see all permissions (and any other associated settings) on one screen.



It's a good idea to run through your privacy and security settings on a semi-regular basis, just to make sure everything is to your liking. If you're wondering where to start, we've created a checklist of iPhone privacy settings.