iPhone Protection from

10 Tips to Protect Your iPhone From Hackers

We tend to think of our iPhone getting hacked as a far-off scenario, but large tech companies like Apple pay big money to white hat (good 'witch') hackers to find the bugs and loopholes they can't see. Just recently, Apple decided to make iOS 10.3.2 available to even older iPhone users because of a flaw found that had gone unknown for a couple of years.

iOS 10 has more security features directly on your iPhone than ever before. Can someone hack your iPhone? Sure; it's even possible for someone to hack an iPhone remotely.

But you can do a lot to secure your iPhone and protect it from possible hackers. Here's how you can protect your iPhone from hackers, both local and remote.

1. Update Your iOS Regularly

(But Give Major New Releases Some Time)

A lot of iPhone users may be skeptical of this advice and for good reason. Updating your iOS devices to the latest software is the absolute best way to make sure your devices are as protected from hackers as possible. That's because with each update Apple improves security features and fixes any previously overlooked weak points.

The first couple weeks of an iOS release are often full of problems. Waiting a week or two is enough time for any major flaws to become apparent; once an update for the update has been released, it's past time to update your device.

To update your device:

- Open the Settings app.
- Select General.
- Tap Software Update

2. Enable Two-Factor Authentication

When Two-Factor Authentication is enabled, you have to use a trusted device to login to a new device.

For example, say you got a new iPad. When you go to sign in with your Apple ID for the first time, your other trusted devices like your iPhone will receive a notification asking for approval. If allowed, your iPhone will display a verification code. Once you enter the verification code on your iPad, the device is approved.

This feature works so well because anytime someone tries to log in to your Apple ID account, you'll get a notification and have the ability to approve or deny the attempt. This feature requires iOS 9 or later.

To turn Two-Factor Authentication:

- Open the Settings app on your iPhone.
- Tap your name at the top.
- Select Password & Security.
- Tap Two-Factor Authentication.

3. Turn On Find My iPhone

When Find My iPhone is turned on, you can see the location of your devices from any of your devices or from any computer via iCloud.com. While it's not recommended you track down an iPhone that's fallen into the hands of a hacker, Find My iPhone will allow you to find your device if you lose it. However, that's not why it's recommended for protecting your device from hackers.

The great thing about Find My iPhone is that if your device is stolen, you can remotely erase your device so that none of your personal information can be stolen.

To turn Find My iPhone on:

- Open the Settings app.
- Tap iCloud or tap your name at the top and then select iCloud (depending on your iOS).
- Scroll down and tap Find My iPhone.
- Toggle Find My iPhone on.

4. Switch to a Six-Digit Passcode

While it may seem like an inconvenience to add two extra digits to your passcode, it's worth the added security. The possible combinations for four digits versus six digits is a huge difference.

If you have a hard time remembering six digits, spell out a six letter word for your passcode instead. To do this:

- Open Settings.
- Tap Touch ID & Passcode.
- Select Change Passcode.
- When choosing a new passcode, select Passcode options and choose 6-Digit Numeric Code.

5. Set Your Phone to Self-Destruct

You can turn on a Setting that will wipe your device clean after ten consecutive failed passcode attempts. Only turn this setting on if you're super concerned about some of the information you have on your phone.

People with children should be careful too, since ten failed attempts erases everything. But it is a fantastic security measure.

To turn on Erase Data:

- Open Settings.
- Select Touch ID & Passcode.
- Scroll down and toggle on Erase Data.

6. Be Smart Online, in Messages, and When Opening Emails

A big way many hackers will get to your iPhone information remotely is through malware links and scammy emails. Only open things (links, messages, emails) from sources you trust. This means that if you're browsing on the web, only open a link if you know where it's going and know that the site it's on is legitimate.

If you receive any messages from unknown numbers, look at the message preview to see if it's someone you know. If the message is strange, asking for something, a random link, or other suspicious text, simply delete it without opening the message. Same goes for email: if you don't know who has sent the message or if it's a newsletter you haven't signed up for, delete it.

Be wary of hackers and scammers posing as companies like Paypal and Apple. Look at the URL and see that it was a subtle variation of Paypal and not Paypal itself.

7. Change Your Apple ID Password Regularly

Your Apple ID is incredibly important to your iPhone's overall security. Changing your Apple ID password regularly is the best way to ensure no one accesses it without your permission.

Create a new Apple ID password every six months.

If you have two-factor authentication enabled, you can change your Apple ID password right on your device.

To do so:

- Open Settings.
- Tap your name at the top.
- Select Password & Security.
- Tap Change Password.

8. Use Secure Wi-Fi & Avoid Logins in Public

Public Wi-Fi is one of the easiest ways to get hacked since the network is inherently less secure.

For paying bills, logging into accounts, and other private activity, it's highly recommended you use a closed Wi-Fi network, like the one you have set up at home.

A lot of people need to use public Wi-Fi as they do the majority of their work in cafes. If that's you, consider downloading a Virtual Private Network (VPN), which will create a private security net around your internet activity.

9. Only Use Trusted Charging Stations

In the last few years, you may have noticed the charging stations popping up in airports, cafes, and other public places.

While these stations are designed to be convenient for our modern lives, they aren't guaranteed to be legitimate. The easiest way around this is to keep a small battery pack with you to charge your devices when they're low. That way, everything is charged at home but you also have extra power on-the-go.

If you're in a tight spot and need to use a public charging space, just make sure it's legitimate and not just some random charger that showed up there.

10. Disable Siri on Lock Screen

Hesitate to include disabling Siri on Lock screen. It's a long-shot that someone would hack in with Siri. There have been instances of someone being able to access private information by using Siri and finding a loophole in the iPhone's security.

Every time one of these loopholes is discovered, Apple fixes it in the next update. But if you're concerned with someone bypassing your iPhone's Lock screen, it's a good final measure to implement.

If you're more concerned about remote hacking, this is tip won't matter as much to you. But if you're worried about someone picking up your phone and finding their way in, turning off Siri on Lock screen is the way to make sure they'll need your passcode to get in. To disable Siri on Lock screen:

- Open the Settings app.
- Select Siri.
- Toggle off Access When Locked.