10 tips for protecting your iPhone from hackers, thieves, and fraudsters

Brian Allison, June 17, 2020

Everyone with a smartphone is using it more than ever, from the time we wake up to the time we go to sleep - and maybe even when we're supposed to be sleeping but can't. We're using them to stay connected with friends, family, and co-workers, and to conduct all parts of our daily lives, from finance to shopping to healthcare. With all this activity, it's worthwhile to ask if we are secure as we can be with our always-connected lives. If your smartphone is an Apple iPhone, you may feel more confident in your security than an Android user, and there's some justification for that. But it doesn't mean the iOS operating system in the iPhone is immune to cyberthreats.

In April of this year, the news came out that attackers have been exploiting two previously undisclosed vulnerabilities since at least January 2018. Last year, security researchers discovered that more than 20,000 iOS apps were published without App Transport Security (ATS), a set of rules and app extensions Apple built as part of the Swift development platform. ATS is turned on by default, and without it, critical information was being transported without encryption.

Apple is now positioned as a "luxury" brand, and part of that branding is the expectation of privacy and security. But it doesn't mean that the level of security that iPhone users have come to expect from Apple in their phone has been extended to the apps that are downloaded, nor to the servers that run in the background of those apps and store and process the data. If that data is sent from your iPhone without encryption, the luxury brand promise is no longer being delivered.

The relative security of iOS doesn't mean users can ignore basic threats to their data and privacy. While most people don't have to worry about advanced targeted attacks or zero-day exploits, they are still exposed to phishing attacks, device theft, and malware that could put their information at risk. If you're using Safari or another browser to navigate the Web, you're potentially exposed to the numerous web-based threats just like someone using Windows or Android.

These precautions are even more essential at a time when businesses have opened up their networks to allow their employees to work remotely because of COVID-19. Wandera's research shows the use of collaboration software nearly tripled within a two-month period earlier this year, as employees suddenly faced working from home. At INCS, we were extremely busy helping our clients get ready for this new style of working. More enterprise applications have been opened to remote access and mobile devices. The pandemic has forced more frequent use of mobile devices to get work done while navigating home office use and often unplanned childcare and “remote learning.”

Many people who have been isolated at home have started to let their guard down when it comes to practicing strong security. Phishing attacks using the pandemic as a theme have increased more than 600%, which increases the odds that an employee and their employer will be compromised.

All of that makes this a good time to take a closer look at your iPhone security posture. Here are 10 tips that any user can adopt to improve their safety.

1. **Declutter your apps**

   Chances are good you have an app or two that hasn't been used in a while. These apps are not only taking up space, they could be a security risk. Apps no longer maintained by developers don't receive updates and security fixes. They should be updated or deleted if not in use.

2. **Stay up to date**

   That's the most popular piece of advice experts offered, followed by downloading the updates as soon as they're available. Even if an update doesn't mention patches, these regularly come with fixes for security holes discovered since the previous update. If left unpatched, these app and iOS vulnerabilities could put devices and data at risk. Make a habit of checking once a week and updating your apps – it only takes a few minutes. Uninstalled patches are the highest risk for cybersecurity since they represent published vulnerabilities that hackers know how to exploit.

3. **Why Does My Flashlight Need My Location?**

   It doesn't. Third-party apps often request permission to access iPhone features and data they don't truly need -- for example, your location, camera, contacts, and microphone. Experts advise going through your apps to ensure they only have access to the things they need and only use your location when necessary. By going to Settings > Privacy, you can view which apps have access to your contacts, calendar, photos, Bluetooth, microphone, camera, and health data. You can drill down further in Location Services, where you can disable location-sharing and change location access for each app. Don’t share info unless YOU want it shared and you know why.

4. Create an Alphanumeric Passcode

We may be used to unlocking our iPhones with biometric data, but a secure passcode remains important. "Even if you can solve a lot with facial recognition and fingerprints, the code lock is still a central component in the access control of the iPhone," says Ahmed Mohamed, systems engineer and security researcher at Metron Pvt. "If you still use a four-digit code here, you are taking an unnecessary risk because these codes are relatively easy to crack." He and other experts suggest creating an alphanumeric password containing both letters and numbers. To do this, access Settings > Touch ID & Passcode (or Face ID & Passcode). Go to Change Passcode and tap Passcode Options to view the option for Custom Alphanumeric Code. Don't share this passcode with anyone else, and don't add another person's biometric data so they can unlock your device without your permission. People using facial recognition on their phone have found that wearing a mask for the COVID-19 pandemic can keep it from working anyway.

5. More Passwords, Stronger Security

Experts urge iPhone owners to enable multifactor authentication (MFA) where possible and to create strong, unique passwords for each of the applications they use. "Some people also think biometrics -- fingerprints, facial recognition, etc. -- are a replacement for passwords, but they should really think of them more as a replacement for usernames," says Ken Underhill, master instructor at Cybrary. "It's good to remember that a strong, complex password and/or code is still beneficial." He echoes what security pros recommend: creating strong and unique passwords across all accounts, not just for the iPhone itself. Think of MFA as something you know (username and password) and something you have (a text to your cellphone, an authenticator app, or a security fob like a YubiKey).

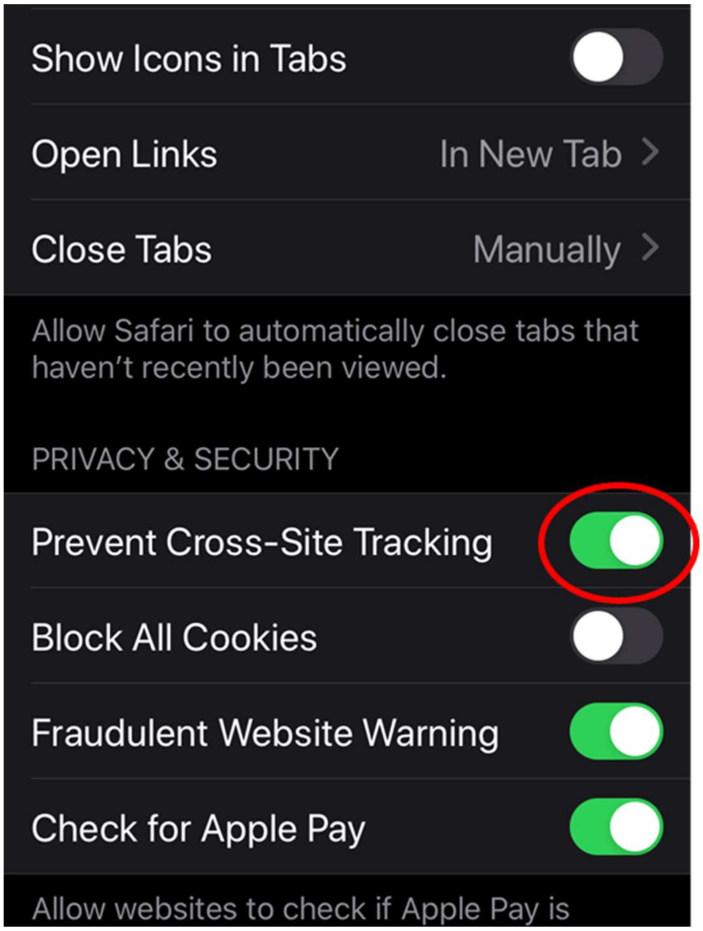
6. Set Login Limitations

If you're worried about your device falling into the wrong hands, you can prevent an attacker from brute-forcing authentication with the "erase data" option. This automatically deletes all data on your phone after 10 consecutive incorrect login attempts. Access Settings > Touch ID & Passcode and scroll to the bottom to toggle Erase Data to the On position. **But be careful, though**, that this could be an extremely risky proposition if you're prone to forgetting your passcode or if you have young children that like to play with your iPhone because once that data's gone, it's really gone if you don't regularly back it up.

7. Take A Closer Look at Safari and Ad Settings

Some websites use cross-site tracking to monitor your online activity so content providers can advertise products and services tailored to your interests. Apple gives the option to turn this off, which can be managed in Settings > Safari. Scroll down until you see "Prevent Cross-Site Tracking" under Privacy & Security and turn it on.

This doesn't mean you'll see fewer ads, but it does mean advertisers won't be able to collect your browsing data to deliver targeted ads. In this section of the Settings app, you can also block pop-ups or enable fake website warnings. See the screenshot below for details:



Show Icons in Tabs ○

Open Links In New Tab >

Close Tabs Manually >

Allow Safari to automatically close tabs that haven't recently been viewed.

PRIVACY & SECURITY

Prevent Cross-Site Tracking ●

Block All Cookies ○

Fraudulent Website Warning ●

Check for Apple Pay ●

Allow websites to check if Apple Pay is

8. **Be Careful Where You Click**

Experts urge any user of any device to avoid clicking any links that appear suspicious or come from unknown sources. Modern phishing attacks don't only target desktops and laptops, they can also arrive via SMS or email, and many use shortened URLs or QR codes to hide the true web address. Unsuspecting users can surrender access to their device by tapping a malicious link in an email or text or by accidentally accessing a fraudulent website. Mobile phishing is the most common mobile threat, Lookout Security's Hazelton says. More than 45% of Lookout's users encountered mobile phishing in the past three months, up from 32.5% in the middle of 2019. "Understand that any link, across any app on your smartphone, can take you to a site that will try to capture your credentials for work or play," he says. While it used to be true that most phishing attempts could be detected from poor grammar, complex or misspelled URLs, and bad visual layout, these are no longer as reliable an indicator as they used to be. Some of these attacks might try to get the user to enter their iCloud credentials, so you should never respond to emails or texts claiming your Apple ID is locked and requires a reset, as these almost certainly are phishing attempts. If you believe there's an issue with your Apple ID, go directly to Apple's official website to resolve it.

9. Remove Tracking Data from Images

We've all received marketing emails packed with images. These pictures often contain hidden tracking code that tells companies whether an email was opened. It's a privacy issue, yes, but it could be a potential security issue if an attacker used the same tools as an attack vector. Concerned users can adjust email settings so these images aren't automatically downloaded, to prevent leaking information about the device, browser, and location. These settings are enabled by default but disabling them puts the user back in control of what gets downloaded and revealed.

It's not enough to be cautious about the emails you receive, but those you send as well. Photos shared via the iOS Photos app include location data by default if your camera has location access enabled. This is handy if you're grouping photos by location or uploading to a shared library, but it's not so handy if it's revealing more information about your photos than you intend. To turn off the location in photos before sharing them, go to the Share process, tap Options, and switch off Location.

10. Public Wi-Fi: Approach with Caution (and a VPN)

Security pros advise against connecting to public Wi-Fi networks, like the one in your favorite coffee shop, that doesn't use a password. This means the information from your phone is not encrypted in the coffee shop and can be intercepted. This is especially true for activities like shopping, online banking, or anything else that would require transmitting personal information.

Criminals also take advantage of these locations and will create a fake public access point, disguised to look like the local shop. When a user connects to one of these networks, the criminal can intercept all the data moving back and forth, including usernames and passwords.

If you must connect to public Wi-Fi, it's recommended you do so with a VPN so your activity is encrypted and not accessible to any criminals who may be lurking on the network.

Following these tips doesn't mean nothing bad can ever happen to you, but they will reduce your risks, and make “the other guy” that doesn't follow them a better target than you. Stay safe out there!

This article is based on “10 iOS Security Tips to Lock Down Your iPhone,” by Kelly Sheridan, published on May 22, 2020. The whole article is available at:

https://www.darkreading.com/endpoint/10-ios-security-tips-to-lock-down-your-iphone/d/d-id/1337841

(registration might be required and it’s a bit of a pain)