iOS 13: Security and privacy settings you need to tweak and check

Concerned about the security of the data you store on your iPhone and iPad? Here are the steps you should take to lock down an iPhone running iOS 13. (Updated for iOS 13.1.2)

By Adrian Kingsley-Hughes for Hardware 2.0 | October 1, 2019 -- 12:35 GMT (05:35 PDT) | Topic: iOS - ZDNet

Have you installed iOS 13, or perhaps bought a new iPhone with the new operating system installed on it? Here are settings you should change and tweaks you should make to harden the security and lock down your device, along with a tour of some of the new security and privacy features built into the platform.

#1: SET A REALLY STRONG PASSCODE

Good iOS security starts with having a really strong passcode. If this is something that's easily guessable then everything else you do is pretty much pointless.

No matter whether you use Face ID or Touch ID to access your iPhone, you still need a passcode, and the longer the passcode you can use -- and remember -- the better.

Go to **Settings** > **Face ID & Passcode** (or **Touch ID & Passcode** on older iPhones), enter your existing passcode, and then tap on Passcode Options to get a set of options. Choose between **Custom Alphanumeric Code** (the most secure) or **Custom Numeric Code** (second best option), or **4-Digit Numeric Code** (I don't recommend this last option).

#2: BLOCK UNKNOWN CALLERS

This is a great way to get rid of nuisance and spam callers. To enable this feature, go to **Settings** > **Phone** > and toggle to **Silence Unknown Callers.**

#3: BLOCK APPS FROM HAVING BLUETOOTH ACCESS

After you install iOS 13 you might find a whole swathe of apps such as Facebook asking you for permission to transmit data over Bluetooth. You can either allow or deny access when the prompts are displayed, or you can head over to **Settings** > **Privacy** > **Bluetooth** and make the changes there.

Note that this doesn't affect audio streaming to headphones and speakers.

#4: PASSWORD AUTOFILL AND THIRD-PARTY PASSWORD MANAGERS

iOS 13 now comes with both a password autofill feature that can use information stored in the iCloud Keychain along with the ability to connect to third-party password apps such as LastPass, Dashlane, and 1Password.

You can find this feature in **Settings** > **Passwords & Accounts** > **AutoFill Passwords**.

#5: MAKE SURE IOS AUTOMATIC UPDATES ARE ENABLED

iOS 13 has the ability to keep itself updated automatically, which is a great way to make sure that your iPhone is fully patched.

This should be set up automatically, but you can check it over at **Settings** > **General** > **Software Update** and making sure **Automatic Updates** is enabled.

#6: WI-FI TRACKING IS BLOCKED

Under iOS 12, it was possible to track iPhone and iPad users by the public Wi-Fi points the device was connecting to silently as the owner went about their business. This ability has now been blocked under iOS 13 so you can wander about without the fear of being tracked.

#7: TAKE CONTROL OVER LOCATION SHARING

Another thing you might have noticed after installing iOS 13 is that you get notifications informing you that apps are using your locations data, and giving you the option of allowing this to continue or blocking it.

Don't worry, you can change your mind by going to **Settings** > **Privacy** > **Location Services**, and changing permissions for your apps.

#8: FIND YOUR DEVICES

iOS 13 has a cool new app called Find My which you can use to locate your friends and family, share your location, or find a missing device.

This app has two cool features, one is **Enable Offline Finding** that helps you find lost devices that aren't connected to Wi-Fi or Bluetooth. The other is **Send Last Location**, which sends the device's location to Apple when the battery is low.

#9: CONTROL WHAT TOUCH ID/FACE ID IS USED TO AUTHENTICATE

Do you want the convenience of Face ID or Touch ID, or do you rather the additional protection that having to enter your passcode offers? iOS 13 allows you to switch Face ID/Touch ID on and off for:

- iPhone Unlock
- iTunes and App Store
- Apple Pay
- Password AutoFill
-

Go to **Settings** > **Face ID & Passcode** (or **Touch ID & Passcode** on older iPhones), and enter your existing passcode to take control of this.

#10: CONTROL ACCESS TO WHAT'S ACCESSIBLE WHEN THE IPHONE OR IPAD IS LOCKED

Control how much -- or how little -- you want to be accessible on a locked device. iOS 12 gives control over the following:

- Today View
- Notification Center
- Control Center
- Siri
- Reply with Message
- Home Control
- Wallet
- Return Missed Call
- USB Accessories

The bottom line is that the more you lock down, the more secure your device and data will be. The USB Accessories feature is especially useful, because it will prevent the Lightning port being used to connect to any accessory if

your iPhone or iPad has been locked for more than an hour.

Go to **Settings** > **Face ID & Passcode** (or **Touch ID & Passcode** on older iPhones), and enter your existing passcode to take control of this.

#11: SET BRUTE-FORCE PROTECTION

iOS has built-in brute-force protection to prevent an unauthorized user from trying to guess your passcodes.

Go to **Settings** > **Face ID & Passcode** (or **Touch ID & Passcode** on older iPhones), enter your existing passcode, and scroll down to **Erase Data**.

After 10 attempts (toward the end there will be a time lockout to slow down the entry process), the encryption key will be deleted and your data wiped.

#12: CHECK FOR PASSWORD REUSE

If you use the iCloud Keychain to store web passwords, you can now use this to check for password reuse (which is bad, so don't do it!).

Go to **Settings** > **Passwords & Accounts** > **Website & App Passwords** and authenticate with either Face ID/ Touch ID or your passcode.

You will see a grey triangle with an exclamation mark next to any entry that is reused. To change the password, tap **Change Password on Website**.

#13: REDUCE THE LOCK SCREEN TIMEOUT

The shorter you set the lock screen timeout setting (there are options ranging from 30 seconds to never), the faster your iPhone or iPad display will require authentication to access it.

You can change the auto-lock time by going to **Settings** > **Display & Brightness** > **Auto-Lock**.

#14: DISABLE BIOMETRICS TO FORCE PASSCODE ENTRY

Here's a simple trick to know that allows you to disable Face ID or Touch ID and force the use of the passcode. To do this press the power button five times (just be sure to cancel the SOS Emergency calling feature if you have this activated).

#15: SET UP TWO-FACTOR AUTHENTICATION

One of the best ways to protect your data is to set up and use two-factor authentication. This means that, even if an attacker has your iCloud username and password, Apple will send an authentication code of a device you've chosen, which should block most attacks.

Go to **Settings** > and tap your name at the top of the screen, then go to **Password & Security**, then choose **Two-Factor Authentication**.

While setting up two-factor authentication you can also set up a **Recovery Key**.

Once set, without this key, or another device signed in with your Apple ID, you will not be able to reset your password.

#16: CONTROL NOTIFICATION DATA LEAKAGE

Notifications displayed on the lock screen can leak sensitive information.

To stop this go to **Settings** > **Notifications** > **Show Previews** and change the setting to **When Unlocked** or **Never**.

#17: MORE CONTROL WITH SAFARI

Under iOS 13, the Safari browser now has the ability to control access to features such as the camera, the microphone, and current location on a per-site basis. Go to **Settings** > **Safari** and look for the toggles under **Settings For Websites**.

original article:
https://www.zdnet.com/article/ios-13-security-and-privacy-settings-you-need-to-tweak-and-check/?ftag=TRE-03-10aaa6b&bhid=23405847687286447375579737817622