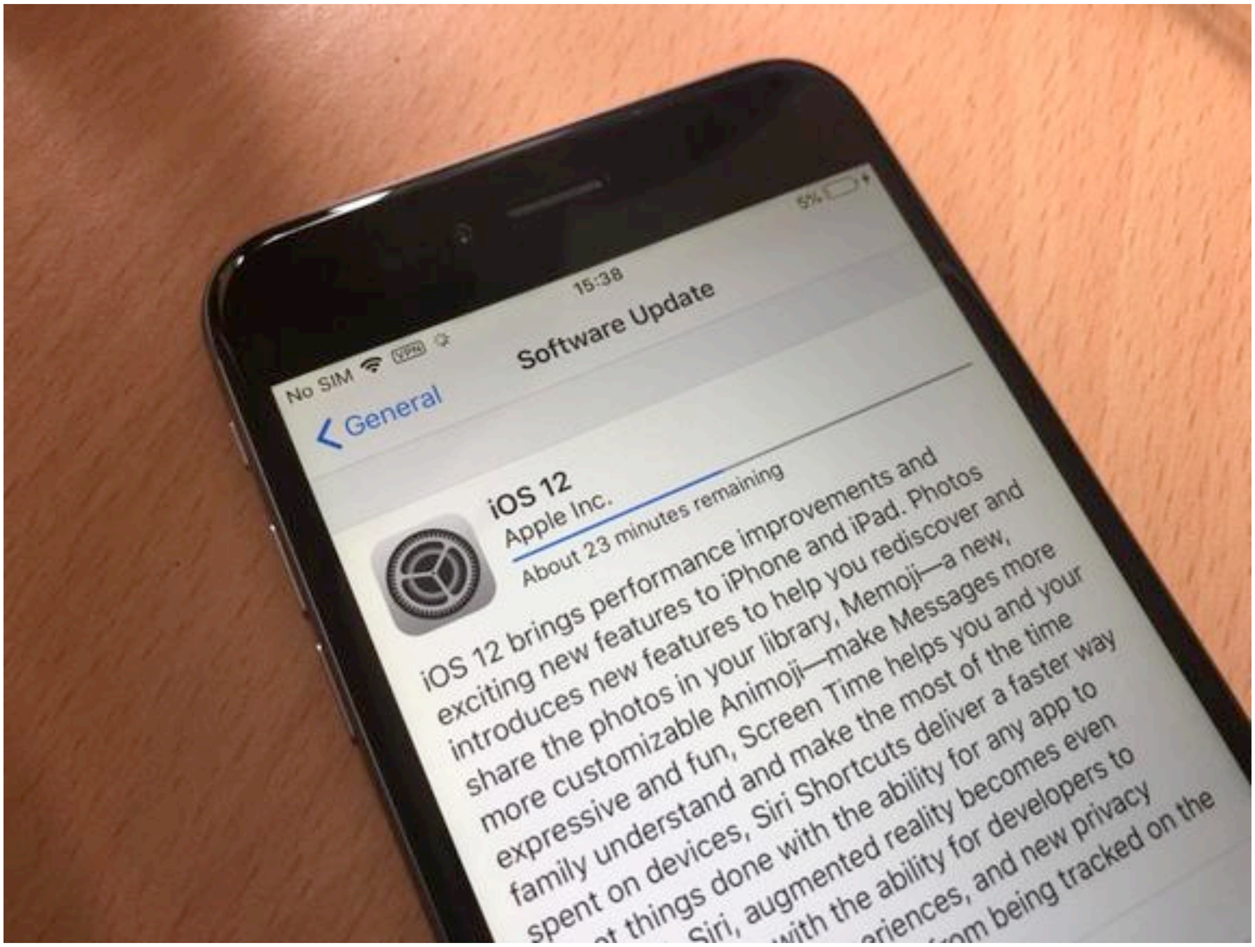
iOS 12: Change these privacy and security settings now

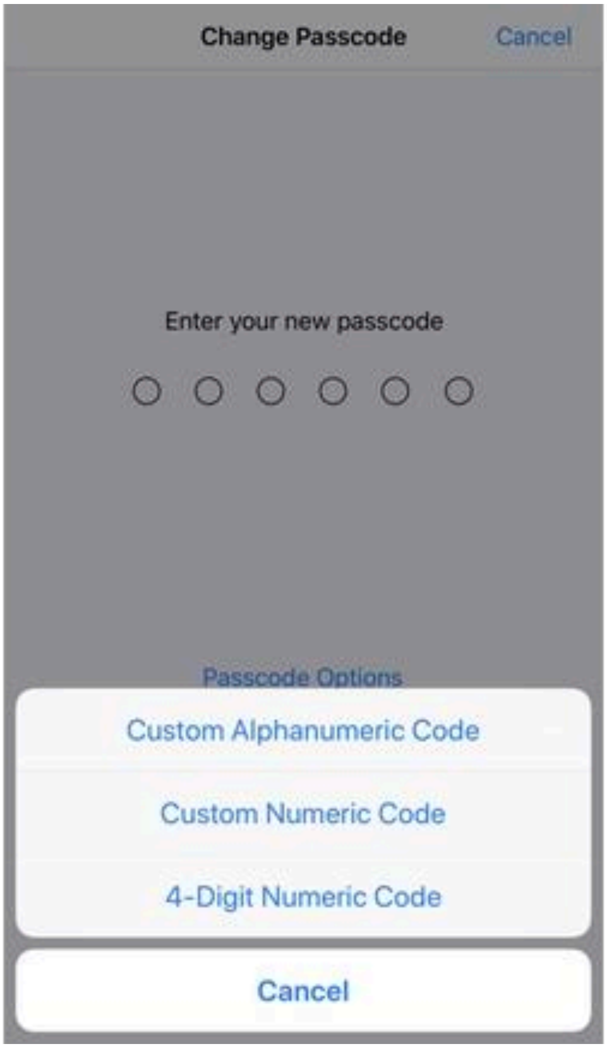
Published: October 4, 2018 -- 19:05 GMT (12:05 PDT)
Caption by: Adrian Kingsley-Hughes - ZDNet



iOS 12 brings performance improvements and exciting new features to iPhone and iPad. Photos introduces new features to help you rediscover and share the photos in your library, Memoji—a new, more customizable Animoji—make Messages more expressive and fun, Screen Time helps you and your family understand and make the most of the time spent on devices, Siri Shortcuts deliver a faster way
ot things done with the ability for any app to
Siri, augmented reality becomes even
with the ability for developers to
eriences, and new privacy
rom being tracked on the

Introduction

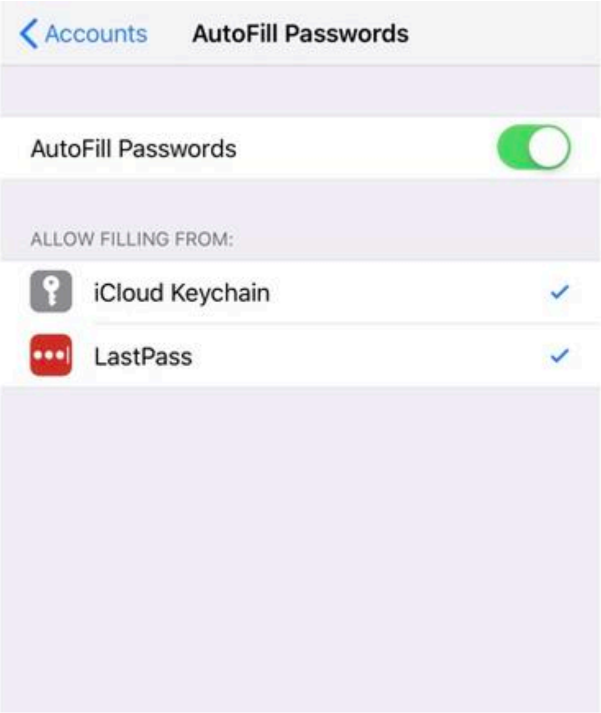
Installed iOS 12 or bought a new iPhone or iPad with the new operating system installed on it? Here are settings and tweaks you should do to harden the security and lock down your device.



Set a strong passcode

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

Go to **Settings** > **Touch ID & Passcode** (or **Face ID & Passcode** on iPhones with Face ID), 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).



AutoFill Passwords

AutoFill Passwords ●

ALLOW FILLING FROM:

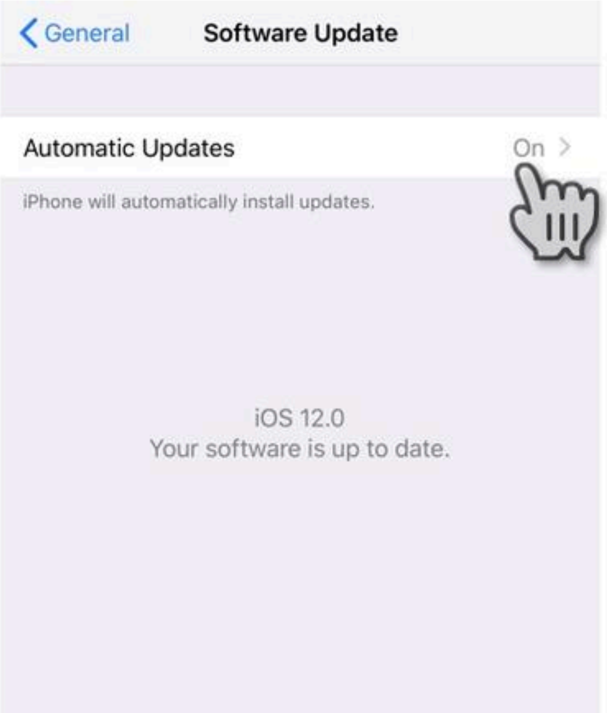
iCloud Keychain ✓

LastPass ✓

Password AutoFill and third-party password managers

iOS 12 now comes with both a password autofill feature using the iCloud Keychain and has 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**.



Automatic Updates On

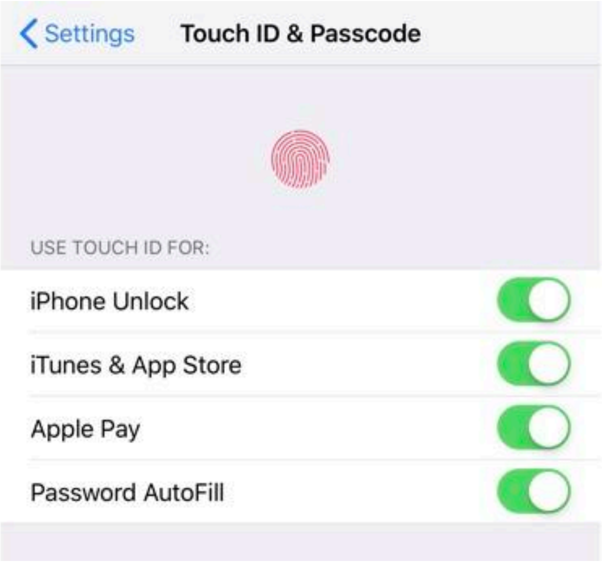
iPhone will automatically install updates.

iOS 12.0
Your software is up to date.

Turn on automatic iOS updates

New in iOS 12 is the ability to install iOS updates automatically, which makes sure that your iPhone or iPad's operating system is always up-to-date.

To set this head over to **Settings** > **General** > **Software Update** and turn on **Automatic Updates**.



Touch ID & Passcode

USE TOUCH ID FOR:

iPhone Unlock ●

iTunes & App Store ●

Apple Pay ●

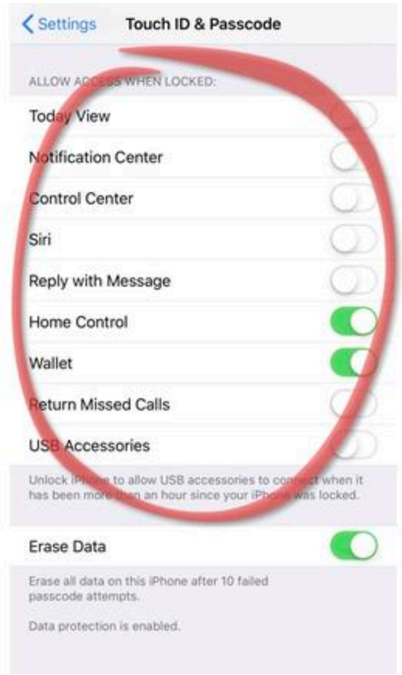
Password AutoFill ●

Control what Touch ID/Face ID is used to authenticate

Do you want the convenience of Touch ID or Face ID, or do you rather the additional protection that having to enter your passcode offers? iOS 12 allows you to switch Touch ID/Face ID on and off for:

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

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



< Settings **Touch ID & Passcode**

ALLOW ACCESS WHEN LOCKED:

Today View	○
Notification Center	○
Control Center	○
Siri	○
Reply with Message	○
Home Control	●
Wallet	●
Return Missed Calls	○
USB Accessories	○

Unlock iPhone to allow USB accessories to connect when it has been more than an hour since your iPhone was locked.

Erase Data	●

Erase all data on this iPhone after 10 failed passcode attempts.

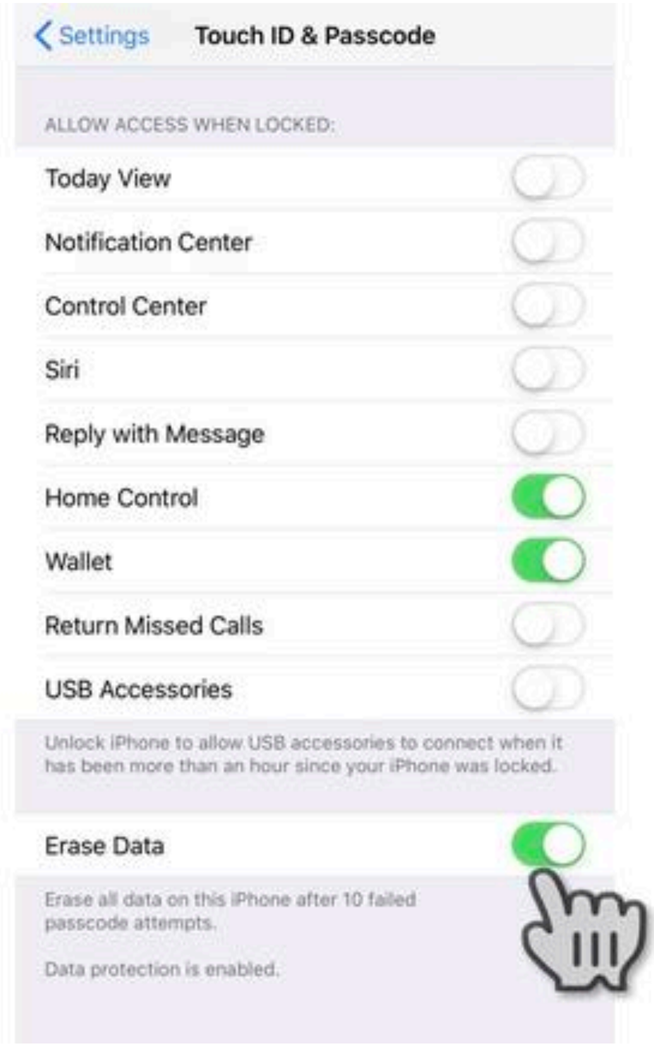
Data protection is enabled.

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** > **Touch ID & Passcode** (or **Face ID & Passcode** on iPhones with Face ID), enter your existing passcode to control this.



Touch ID & Passcode

ALLOW ACCESS WHEN LOCKED:

Today View ○

Notification Center ○

Control Center ○

Siri ○

Reply with Message ○

Home Control ●

Wallet ●

Return Missed Calls ○

USB Accessories ○

Unlock iPhone to allow USB accessories to connect when it has been more than an hour since your iPhone was locked.

Erase Data ●

Erase all data on this iPhone after 10 failed passcode attempts.

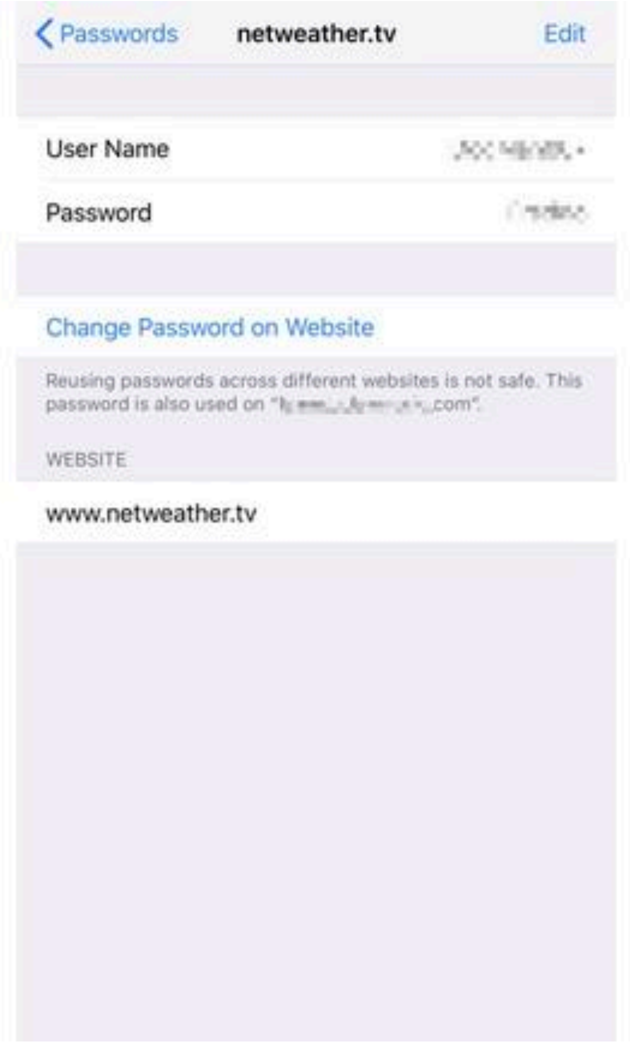
Data protection is enabled.

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** > **Touch ID & Passcode** (or **Face ID & Passcode** on iPhones with Face ID), 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.



User Name [redacted]

Password [redacted]

Reusing passwords across different websites is not safe. This password is also used on "[redacted].com".

WEBSITE

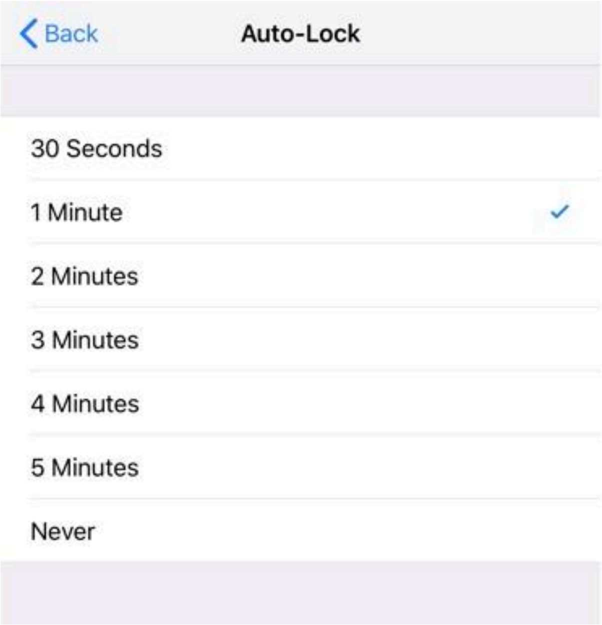
www.netweather.tv

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 touch ID/Face 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**.



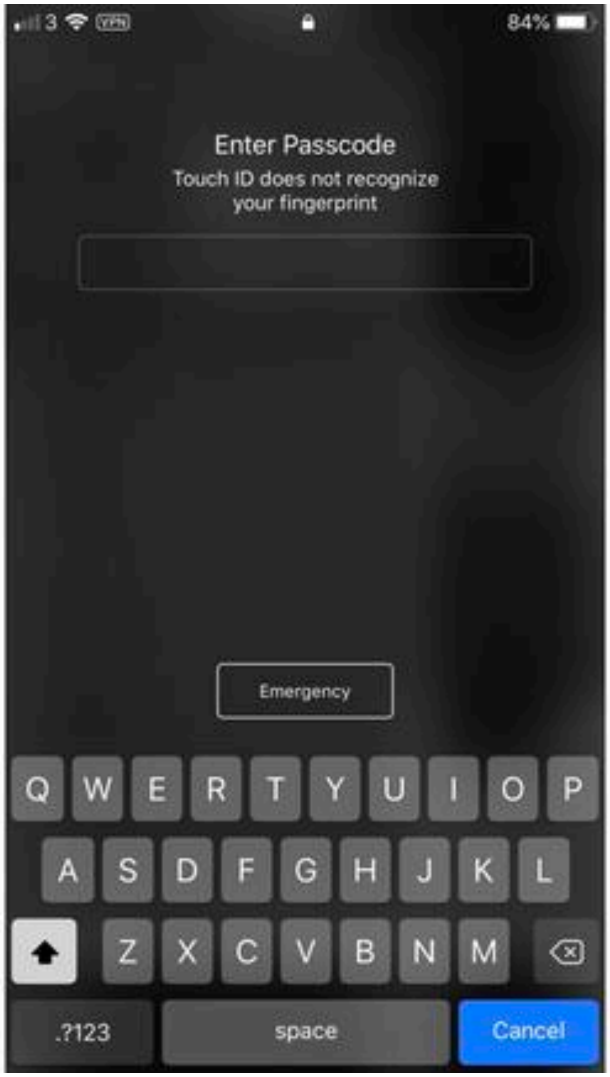
Auto-Lock

- 30 Seconds
- 1 Minute ✓
- 2 Minutes
- 3 Minutes
- 4 Minutes
- 5 Minutes
- Never

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**.



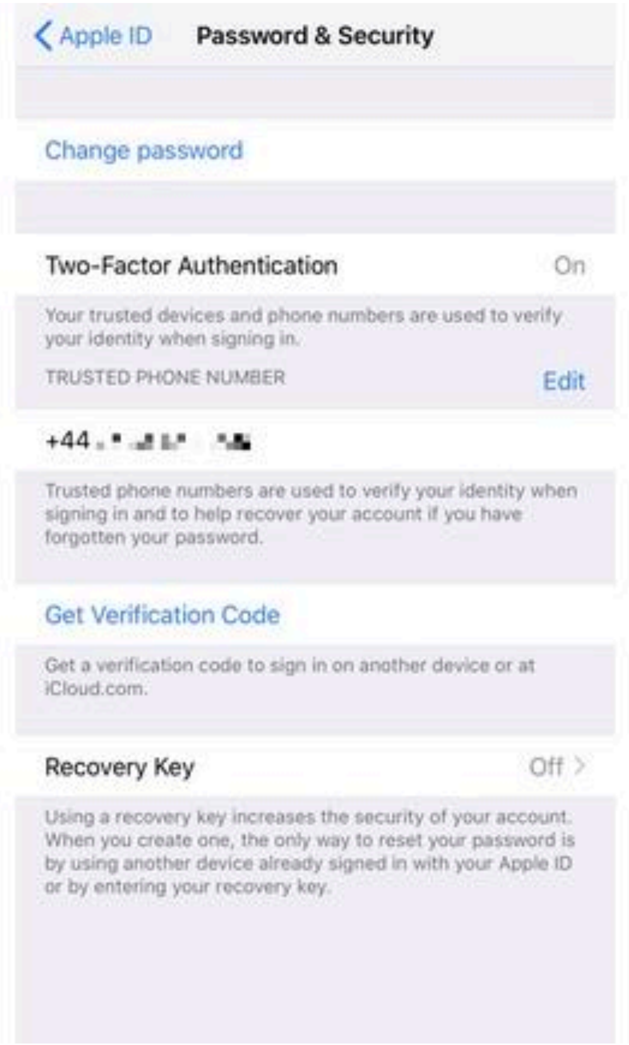
Enter Passcode

Touch ID does not recognize your fingerprint

Disable biometrics to force passcode entry

iOS 12 -- as was the case with iOS 11 -- 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).



< Apple ID Password & Security

Change password

Two-Factor Authentication On

Your trusted devices and phone numbers are used to verify your identity when signing in.

TRUSTED PHONE NUMBER Edit

+44 [redacted]

Trusted phone numbers are used to verify your identity when signing in and to help recover your account if you have forgotten your password.

Get Verification Code

Get a verification code to sign in on another device or at iCloud.com.

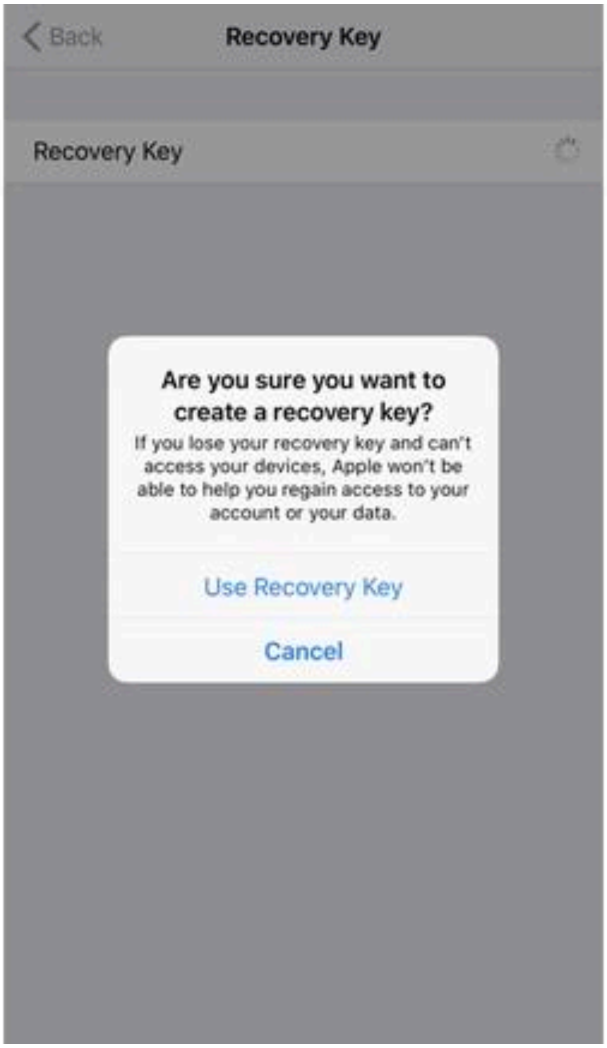
Recovery Key Off >

Using a recovery key increases the security of your account. When you create one, the only way to reset your password is by using another device already signed in with your Apple ID or by entering your recovery key.

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**.



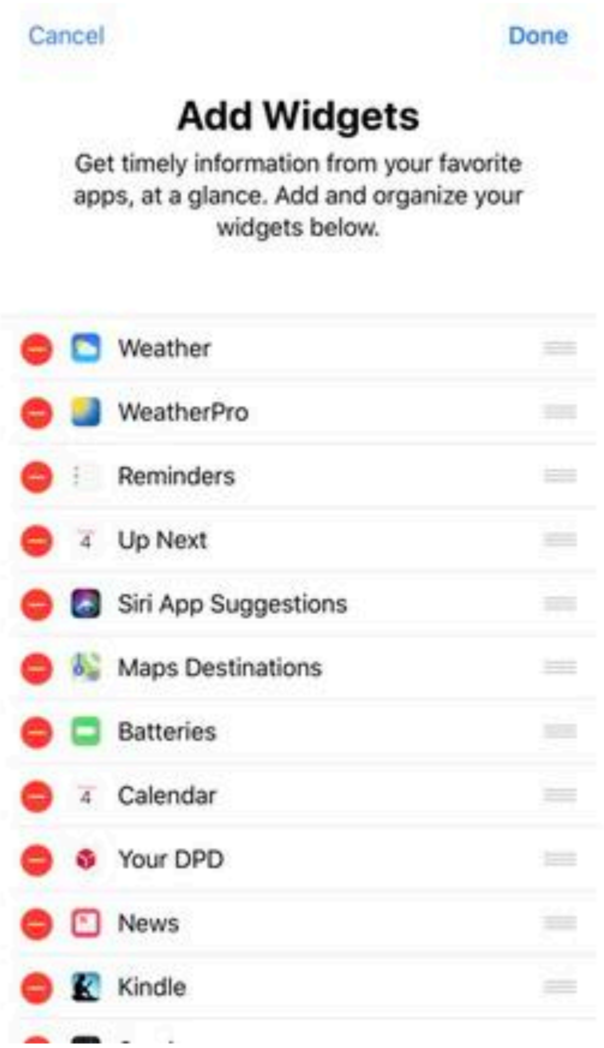
Are you sure you want to create a recovery key?

If you lose your recovery key and can't access your devices, Apple won't be able to help you regain access to your account or your data.

Set a recovery key

While setting up two-factor authentication (go to **Settings** > tap your name at the top of the screen, then go to **Password & Security**, and choose **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.



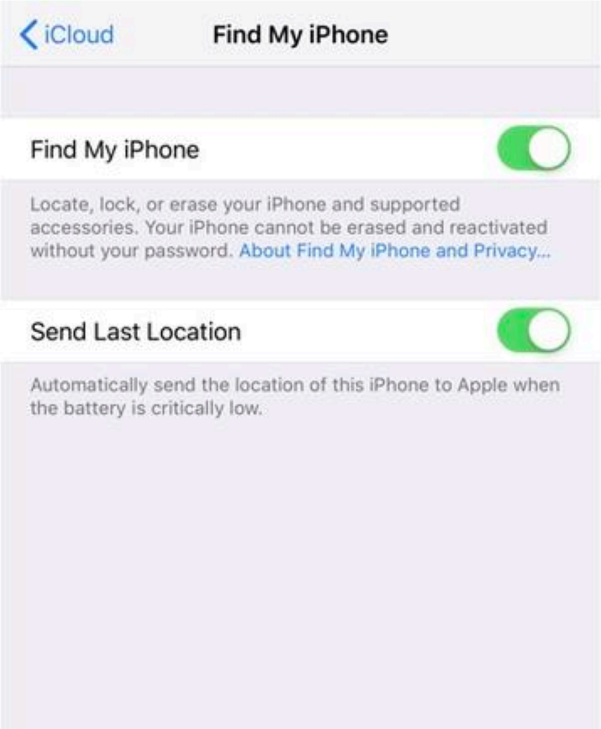
Add Widgets

Get timely information from your favorite apps, at a glance. Add and organize your widgets below.

Disable unnecessary widgets

Widgets can leak data even when your iPhone is locked. You can either disable the Today View from being accessible when your device is locked (see earlier tip: Control access to what's accessible when the iPhone or iPad is locked), or you can edit the widgets as follows:

Swipe to the right on the Home screen into the Today View panel, and then scroll to the bottom of the screen and hit **Edit**. Now, you can remove any panel that you do not need.



Find My iPhone ●

Locate, lock, or erase your iPhone and supported accessories. Your iPhone cannot be erased and reactivated without your password. About Find My iPhone and Privacy...

Send Last Location ●

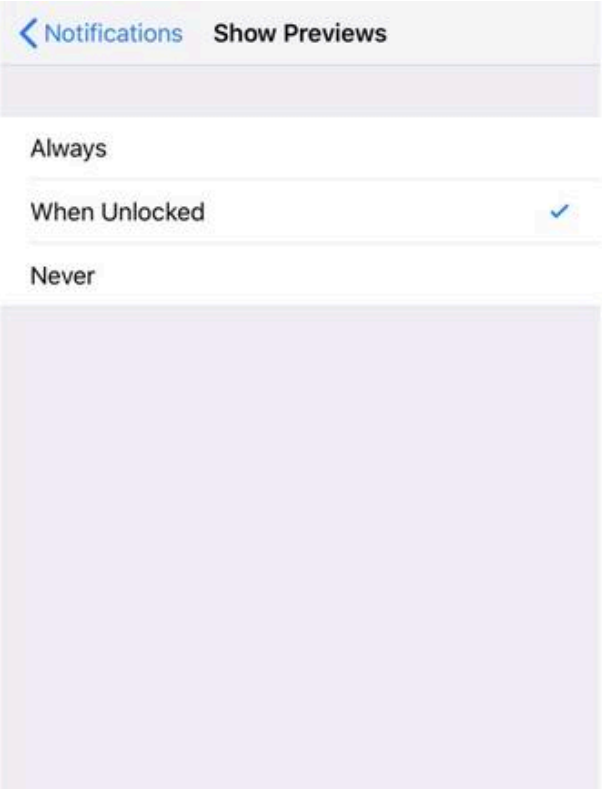
Automatically send the location of this iPhone to Apple when the battery is critically low.

Activate "Find My iPhone"

This is a handy feature to have on if you worry about your device being stolen, or if you are careless with things.

To activate it go to **Settings** > then tap your name at the top of the screen, and go to **iCloud** > **Find My iPhone**.

From here, you can also check the **Send Last Location** feature, which sends the location of your device to Apple when the battery is low, allowing you to find it even when the battery is flat.



‹ Notifications

Show Previews

Always

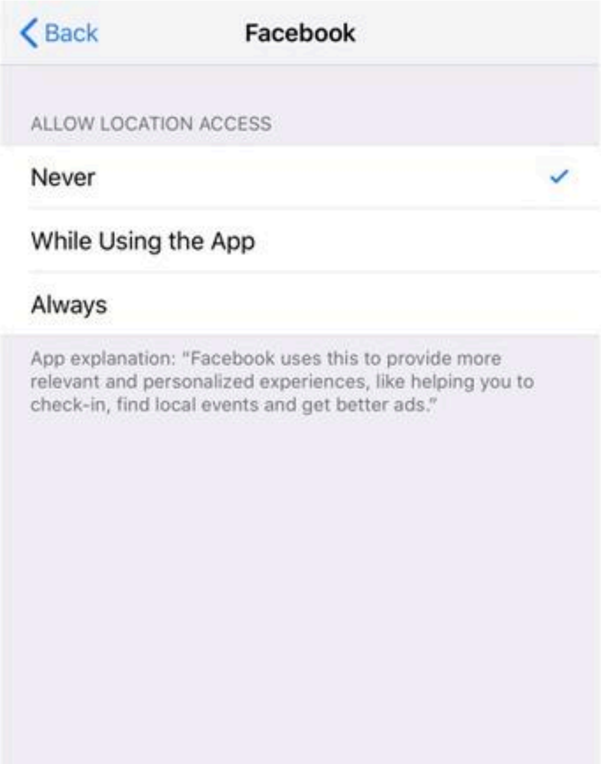
When Unlocked ✓

Never

Control notification data leakage

Notifications displayed on the lock screen can leak sensitive information.

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



Back

Facebook

ALLOW LOCATION ACCESS

Never ✓

While Using the App

Always

App explanation: "Facebook uses this to provide more relevant and personalized experiences, like helping you to check-in, find local events and get better ads."

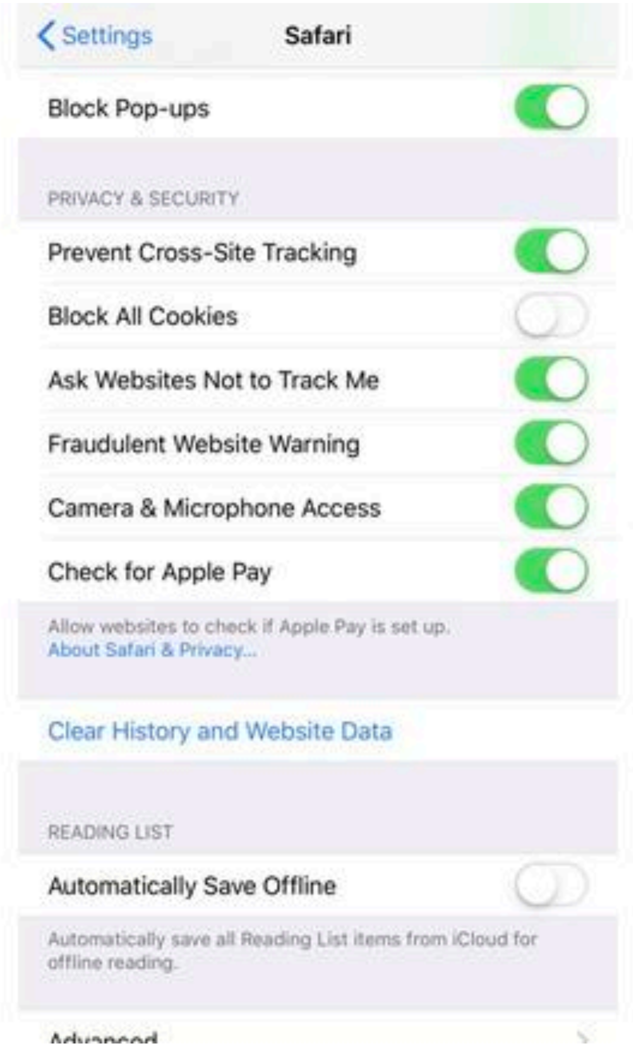
Take control over Location Sharing

You can control how and when apps have access to your location data. Go to **Settings** > **Privacy** > **Location Services**, and from there you can go through your apps.

You can choose between:

- - Never
- - While Using the App
- - Always

Each app should also given you a brief explanation of how if uses location data.



Safari

Block Pop-ups ●

PRIVACY & SECURITY

Prevent Cross-Site Tracking ●

Block All Cookies ○

Ask Websites Not to Track Me ●

Fraudulent Website Warning ●

Camera & Microphone Access ●

Check for Apple Pay ●

Allow websites to check if Apple Pay is set up.
About Safari & Privacy...

Clear History and Website Data

READING LIST

Automatically Save Offline ○

Automatically save all Reading List items from iCloud for offline reading.

Advanced >

Secure the Safari browser

If Safari is your browser of choice on iOS, Apple gives you a number of security customizations.

Head over to **Settings** > **Safari**, and from there, you will get access to numerous options, from blocking pop-ups to preventing cross-site tracking.

original article:
https://www.zdnet.com/pictures/ios-12-change-these-privacy-and-security-settings-now/