How to Find Compromised & Reused Passwords on iPhone, iPad, and Mac

Summary

The article describes how to find compromised and reused passwords on iPhone, iPad, and Mac. The Passwords app categorizes issues into compromised passwords, reused passwords, and weak passwords. The article also explains how to fix password issues by changing the password on the website and saving it in the Passwords app.

Apr 30, 2026

The Passwords app, Apple's built-in password manager for Mac, iPhone, and iPad, not only stores your logins and passwords for easy authentication, but it can also alert you to security risks. Passwords app makes it easy to quickly find compromised, reused, or weak passwords, and take action to secure your accounts.

If you're a Passwords app user and you haven't investigated this on your own yet, it's a worthwhile endeavor to do so. It makes it easy to determine if you should be changing a password that has been compromised without your knowledge (and that's usually the case, since data breaches happen all the time and they can be hard to keep track of).

Oh and by the way, the Passwords app password manager and syncing feature used to be called iCloud Keychain, so you might be familiar with these general features but think of it as called something else.

How to Find Compromised & Reused Passwords

You can review password security warnings and compromises directly within the Passwords app on Mac, iPhone, or iPad.

On iPhone or iPad:

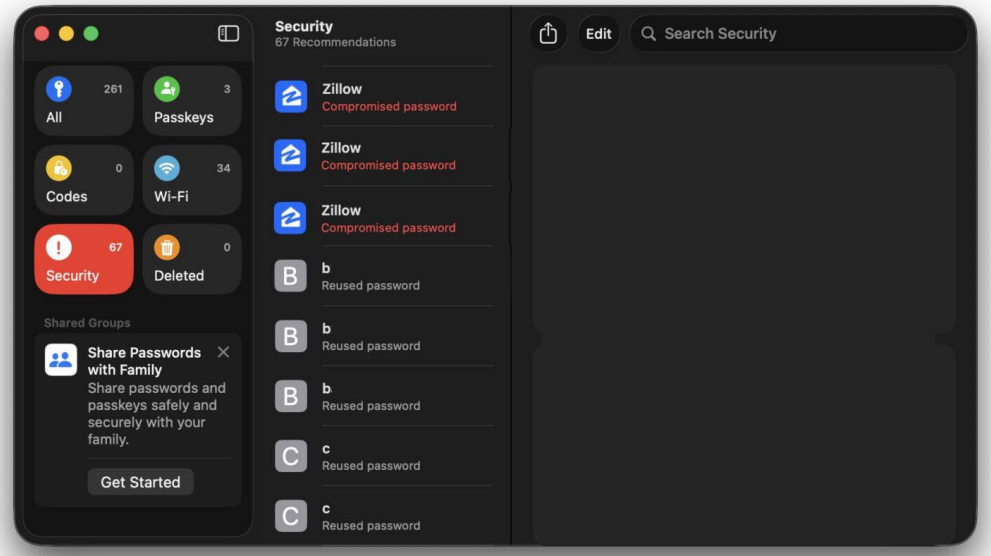
1. Open the Passwords app
2. Authenticate with Face ID, Touch ID, or passcode
3. Tap Security (or Security Recommendations)

Here you will see a list of accounts and logins with potential issues.

On Mac:

1. Hit Command+Spacebar to open Spotlight, type “Passwords” and hit return to launch Passwords app
2. Authenticate within the passwords app as requested, with password or Touch ID
3. Click on Security or Security Recommendations

This view shows the same types of alerts on Mac as it does on iPhone and iPad, showing a list of accounts and logins that have potential security risks.



As you can see in the screenshot here on a Mac with a lot of security warnings in Passwords app, including for many reused passwords for dozens of nonessential websites, and a handful of security warnings for compromised passwords also for nonessential websites. These all needed to be addressed, and exploring the Passwords app Security warnings made it simple for this user to know which passwords to change. It’s not uncommon for people to reuse a password for the hundreds of websites and apps that are out there, but because a reused password results in a single point of failure, it’s not a good security practice. Additionally, even if you have a compromised password on a random website or app service like Zillow as shown in the screenshot here, it’s still a good idea to change that password too. In the example here, the passwords were reused and compromised, and were also weak (things like using “password” as a password are a big no-no), so this provided a good opportunity to boost online account security for this user.

What the Security Warnings Mean in Passwords App

The Passwords app categorizes issues to help you prioritize fixes into several categories:

Compromised Passwords

These passwords have appeared in known data breaches, and these are high priority for security. Since the password has been compromised, it should be changed immediately. This feature uses Apple's integration with breach data sources, similar to services like Have I Been Pwned, to detect compromises from various sources. Many users who store the majority of their passwords in Passwords.app and iCloud will find results in the section, often for things like online retailers, that you may not have even known had a security breach.

Reused Passwords

This means the same password has been used across multiple accounts. Basically this poses a security risk because if one account is compromised, all others are now at risk since they use the same passwords. It's best practices to use a unique password for each individual login and site, which is also why the random strong password generating feature of Passwords.app is so powerful, and useful.

Easily Guessed / Weak Passwords

These passwords are easy to guess, or don't meet modern security standards. Any shorter or simpler basic passwords would qualify under this list, for example if you use the password "password123" for a password, it would probably appear as a weak and easily guessed password. Stronger passwords are longer and more complex with mixed characters. Any weak password should be replaced by a stronger alternative.

Fixing Passwords Issues

If you do see a problem to address, like a compromised password (or several, as is often the case), you can click on "Change Password" for the flagged account, and it will typically take you to the website whenever available, that you can update and change the password with that specific service. You'll then want to save the new password with Passwords app, so that you can use it easily in the future, and so that Passwords app can check it for data breaches too.

You'll need a modern version of iOS, macOS, or ipadOS to be able to use the Passwords app Security risk assessment features, though the feature exists in Safari on older versions of MacOS as well, and in the Passwords section of the System Settings app for a while too, before the dedicated Passwords.app was born. Back then it was called iCloud Keychain.

With Passwords app, you can help to monitor security of your account credentials, and reduce your risk across multiple platforms. And because it's built directly into MacOS, iOS, and iPadOS, there's no need for a third party app or service. This is a simple way to improve your account security and internet presence, and so it's worth opening the Passwords app and taking a look at the Security section not only now, but from time to time.

Of course if you don't use the Passwords app, you won't have access to this feature, or any of the related password saving and autofill features.

Have you checked Passwords app and found compromised or reused passwords using the built-in security tools? What do you think of these features? Share your thoughts in the comments.