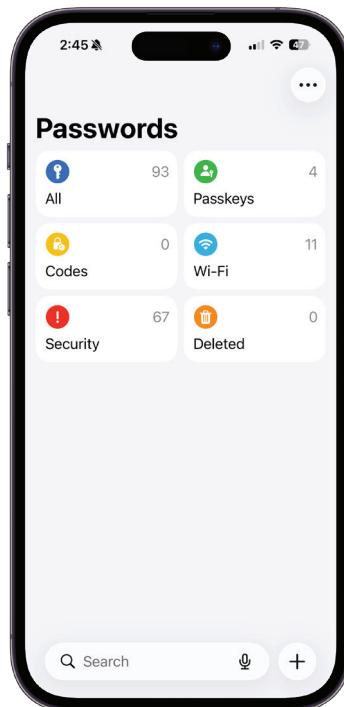




Cheat Sheet

Apple Passwords Never Forget a Password Again



APPLE PASSWORDS

NEVER FORGET A PASSWORD AGAIN

BY CULLEN THOMAS

Apple Passwords is the built-in password management app on your iPhone, iPad, and Mac that helps you lock down all your online accounts and protect yourself from scammers.

With Apple Passwords, you can:

1. **Save passwords** in a secure vault in the Passwords app, and they'll be safely synced with your other Apple devices.
2. **Log into websites without memorizing or typing anything** by automatically filling in your saved usernames and passwords from the Passwords app. It's built right in.
3. **Share passwords securely and safely.** If you update a password, it is automatically updated for everyone you've shared with.
4. **Take advantage of advanced modern security such as passkeys** that go beyond simple passwords .

TOUR THE PASSWORDS APP



All

Tap all to see a list of all records stored in your Passwords app. Each record can store a username, password, code-generation key, and some notes, along with a list of websites where those credentials work.



Passkeys

The Passkeys section lists all the records of your accounts that have passkeys saved. A passkey is a secure way to log in by authenticating directly with the Passwords app, instead of fetching a password. This is more secure and more convenient, since you don't have anything to memorize. Not every website supports Passkeys.



Codes

This section of the Passwords app lists all records where you have set up a verification code to help secure your account. Logging in to the websites listed in this section will require first the password, then a time-based one time code generated by your Passwords app and autofilled just like a password. The codes change every thirty seconds and can only be used once, so even a scammer who knows your password will not know the one-time code and will not be able to access these accounts. We recommend adding your accounts to this section by setting up verification codes for every website and service that supports the feature.



Wi-Fi

This section contains all the Wi-Fi passwords you've stored on your iPhone. Go here if you need to share a Wi-Fi password with someone.

**Security**

The Passwords app constantly checks to see if your passwords have been compromised, or if they are weak and easily guessed. This section alerts you when it finds something that needs your attention. The alerts in this section may be urgent, for example if your bank account password was discovered in a data dump on the dark web. If you have any alerts in this section, resolve them as soon as possible.

**Deleted**

Under the Deleted section you'll find your recently deleted records. Records remain here for 30 days.

Shared Groups

This section lists each password sharing group you have created. Each group can share a different set of passwords with a different set of Apple devices.

SIMPLE PASSWORD APP TROUBLESHOOTING

If your password didn't appear in a webform:

Navigate away from your web browser to the Passwords app. Use the search bar to locate the record you need. Tap on the password. Tap Copy. Switch back to the web browser. Tap on the password form field to bring up the context menu. Tap Paste.

If the Passwords app is offering the wrong password:

Switch from your web browser to the Passwords app. Use the search bar and enter the website where you're trying to log in. Check to see if there are multiple records in the Passwords app for the same website. If there are duplicates, check the date each was last modified to see which is the most recent. If that doesn't work, then you probably have duplicate records (see below). If you don't see a duplicate, then your record in the Passwords app is different from the record the account holds, and thus both records need to be updated. Here's what to do: in the record, tap the Edit button, then next to the password, tap Change Password and generate a new unique

password, making sure to save it first in the Passwords app, then on the website.

If you have duplicate records in the Passwords app:

You can try each record one at a time until you figure out which one is correct, making sure to delete each incorrect record. But if there are several, then it's often easiest to simply delete all of the duplicate records and go to the website and click "I forgot my password" to initiate a password reset. When you reset your password on the website, make sure to use the one generated by the Passwords app, and to save it there.

If the Passwords app is frozen or won't react:

Enter the App Switcher by swiping up slowly from the bottom of your screen, then force close the Passwords app by dragging up on that app. Wait a few seconds, then open the Passwords app again.

PASSWORDS APP PRO TIP!

Many small troublesome mishaps can be avoided if you first create your records in the Passwords app (instead of a web browser) and make sure it saves there with no duplicate entries, and only then update the record held by the website or service using the password reset process.

GLOSSARY OF TERMS

Credential: A credential is something that proves you have permission to access a privileged resource such as an account. Most web accounts use a combination of a username (usually an email address) and a password as their credential to identify their users.

Password: A password is a string of characters and/or numbers known only to you, usually combined with a username as part of a credential. A good way to generate memorable, secure

passwords is the three random words method. Longer is better than weirder—don't use one word with numbers and obscure characters. That is hard for you to memorize and easy for computers to guess. Instead, use a set of random words that is easy to memorize but long.

Passcode: A passcode is a string of numbers known only to you—a numeric password. iPhones and iPads use a passcode instead of a password by default. On those devices, the passcode is used to generate a unique encryption for all the device's content, so even Apple cannot decrypt an iPhone without knowing the passcode.

Passkey: This is the popular name for a system to replace passwords, so you can use your phone or password manager as the key to unlock your account, without any password to memorize. The system's full name is FIDO2 WebAuthN, and it is a strong and safe system.

Passphrase: A string of words only you know. The passphrase, which must be 15 characters long at least, is a more secure version of a password, and can be used in any form that asks for a unique password. It is more secure because it is much longer than a regular password, and longer phrases are much harder to guess.

Hardware Key: A physical key for your online accounts. Normally, these look like USB keys, but they don't store files. Instead, they serve to cryptographically confirm your identity using the same FIDO2 WebAuthn protocol used by passkeys. This is the strongest form of multi-factor authentication because it can't be accidentally given away in a phishing scam or look-alike website.

Password Vault: The place you keep all your credentials.

Recovery Codes: Codes that can be used once and only once to regain access to an account in the event that the usual password is lost. These codes are generated when you create the account, and are meant to be printed out and stored someplace safe.

MFA: Multifactor Authentication (MFA) is the practice of requiring more than one credential to confirm an identity. For most websites, a username and password form the basic credential. Since passwords can be guessed or stolen, additional identifying factors can be added to secure an account, most commonly a phone number. Wherever possible, use MFA with all of your accounts.

TOTP: Short for Time-Based One Time Password. A code you are either sent or generate yourself to supplement your primary credential as part of an MFA process. Note that, despite being called a One Time Password, a TOTP is always a randomly generated code, not a word.

OTP: Short for One Time Passwords, this is an ambiguous term that can refer to either recovery codes (see above) or TOTP codes (see above). We try to avoid this term but it is in popular use to mean either of these different things.

2FA: Two Factor Authentication is just a synonym for MFA.



Cullen Thomas is a Senior Instructor at iPhone Life with more than ten years' teaching experience. Cullen applies a passion for gadgetry to teach live classes, and specialize in privacy and security. Cullen has dual degrees in Media & Communications and Literature, and a Masters degree from the David Lynch Graduate School of Cinematic Arts.