

A JARGON-FREE GUIDE

Apple Passwords, Made Simple

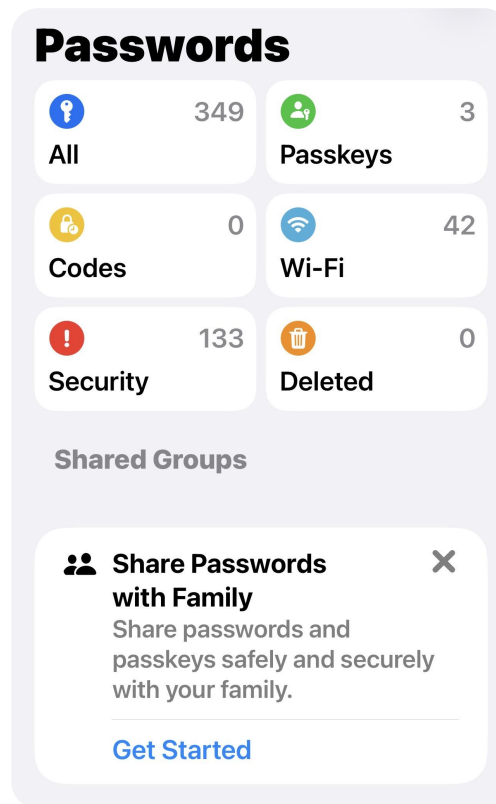
*Everything the Passwords app does, why it matters,
and how to fix it when it misbehaves — explained
for real people.*

A teaching guide · Built for anyone who's ever forgotten a password



**Senior Tech
Tutor Marin**

www.techtutormarin.com



Start Here

If you own an iPhone, iPad, or Mac, you already have a capable password manager sitting on your device — it's just called **Passwords**, and a lot of people never open it. That's a shame, because it quietly solves one of the most stressful parts of modern life: keeping track of dozens of logins without either reusing the same weak password everywhere or scribbling them on sticky notes.

The idea I want you to walk away with is simple. You should only have to remember *one* thing — the code that unlocks your phone. Everything else gets stored, generated, filled in, and even shared for you. This guide walks through what the app can do, tours each part of it, and then hands you a short list of fixes for the moments when something doesn't behave.

What it actually does for you

Four jobs, mainly. It **stores** your logins in an encrypted vault that syncs across all your Apple devices. It **fills them in** automatically when you land on a login screen, so you rarely type a password again. It lets you **share** a login with someone you trust, and if you later change that password, their copy updates on its own. And it supports **passkeys** — a newer, phishing-resistant way to sign in that skips passwords entirely. We'll unpack that last one below, because it's genuinely worth understanding.

A Tour of the App

Open Passwords and you'll see it's organized into a handful of sections — the same tiles you'd tap on your iPhone. Here's what each one is for, and when you'd reach for it.



All

Your complete list. Every entry can hold a username, a password, a code-generator, notes, and the sites or apps where that login works. When you just want to look something up, this is the master list.



Passkeys

Accounts you've upgraded to a passkey instead of a password. A passkey lets your device prove who you are directly — nothing to type, nothing to memorize, and nothing a fake website can trick out of you. It's both safer and easier. The catch is that the site has to support it, and not all do yet.



Codes

Logins where you've set up a rotating verification code. After your password, the site asks for a short code that changes every thirty seconds — and Passwords fills it in for you automatically. Because each code expires almost immediately, someone who steals your password still can't get in. I'd encourage turning this on for every account that offers it; it's one of the biggest security upgrades for the least effort.



Wi-Fi

Every Wi-Fi network password your device has saved. Handy when a guest asks for the code and you'd rather not go hunting through Settings.



Security

The app quietly watches for trouble — passwords that are weak, reused, or that have turned up in a known data breach. When it flags something here, treat it as a to-do list. If a password showed up in a leak, change it soon; if it's reused across sites, give each account its own.



Deleted

A safety net. Anything you delete waits here for thirty days before it's gone for good, so an accidental delete is easy to undo.



Shared Groups

Collections of logins you've chosen to share — a household streaming account, say, or shared bills. Each group has its own members, so you can share one set of passwords with family and a different set with, for instance, a co-worker.

When Things Go Sideways

Most of the time the app just works. But here are the snags people actually run into, with the shortest path out of each.

► The password didn't offer to fill in on a website

Open the Passwords app directly, search for the entry, and tap to copy the password. Go back to the site, tap and hold the password field, and paste. It's a manual workaround, but it gets you in while you sort out why autofill skipped it.

► It filled in the *wrong* password

Usually this means you have two saved entries for the same site, or the app's copy has drifted out of sync with what the site actually expects. Open Passwords, search the site, and see if more than one entry exists. If so, check which was edited most recently. If there's only one and it's still wrong, the site and the app simply disagree — the cleanest fix is to reset the password on the site and let the app generate and save the new one.

► You've got duplicate entries piling up

With just a couple, try each until one works, then delete the rest. With a messy pile, don't fight it — delete them all, use "Forgot password?" on the website to reset, and save the fresh password the app generates. One clean entry beats five stale ones.

► The app froze or won't respond

Swipe up slowly from the bottom of the screen to bring up the app switcher, flick the Passwords app up and off to close it, wait a few seconds, and reopen. A fresh start clears most hiccups.

THE ONE HABIT THAT PREVENTS MOST OF THIS

Create new logins **inside the Passwords app first**, confirm they saved cleanly with no duplicates, and only then update the account on the website. Doing it in that order keeps the app and the site in agreement — which is the root cause of nearly every "wrong password" headache.

The Vocabulary, Decoded

Security terms get thrown around a lot and rarely defined. Here's a plain-language glossary you can point people to.

Credential — Proof you're allowed into an account. For most sites that's a username (often your email) plus a password.

Password — A secret string only you know. The best ones are long rather than weird: a few random, unrelated words are far easier to remember and far harder for a computer to crack than a short word dressed up with symbols.

Passphrase — A password made of several words, ideally fifteen-plus characters. Longer means stronger, and it's kinder to your memory too.

Passcode — The numeric code that unlocks your iPhone or iPad. It also encrypts everything on the device — which is why not even Apple can open a locked iPhone without it.

Passkey — A modern password replacement (its formal name is FIDO2 / WebAuthn). Your device becomes the key, so there's nothing to type and nothing a fake site can phish out of you.

Hardware Key — A physical key, often USB-shaped, that confirms your identity using the same technology as passkeys. The sturdiest form of protection, since it can't be handed to a look-alike website by mistake.

Password Vault — The encrypted place your credentials live. The Passwords app is your vault.

MFA — Multi-Factor Authentication: asking for more than one proof of identity, so a stolen password alone isn't enough to get in. Turn it on everywhere you can.

2FA — Two-Factor Authentication — just MFA with exactly two factors. Same idea, older name.

TOTP — A Time-based One-Time code that refreshes every thirty seconds. Despite the "password" in the name, it's always a random number, never a word.

OTP — One-Time Password — a loose term that can mean either a TOTP code or a recovery code. Vague enough that it's worth clarifying which is meant.

Recovery Codes — Single-use backup codes that get you into an account if you lose your usual login. Save them somewhere safe when an account first hands them to you.

A closing thought: security isn't about doing everything at once. Pick one account today — your email is a great place to start, since it's the key to resetting everything else — give it a strong unique password, turn on a verification code, and let the Passwords app remember it for you. Do that a few accounts at a time, and within a couple of weeks you really will never forget a password again.

ABOUT THE AUTHOR

Rob Shore is both a community volunteer and the founder of Senior Tech Tutor Marin, which serves Marin County by offering older adults one-on-one, jargon-free help with iPhones, iPads, Macs, and all of the apps and programs that support them. He can be reached at shorespeak@gmail.com or 831-221-0018. Learn more at www.TechTutorMarin.com.