The Five Best Password Managers

A while ago, all it took to be a great password manager was to keep your passwords in an encrypted vault. Now the best password managers give you the option to sync or keep them local only, change web passwords with a click, log in to sites for you, and more.

This story originally ran in January, 2015, and was updated with additional reporting from Patrick Austin in August 2017.

Back in 2015, we asked you to tell us which password managers you thought were the best, and pulled the five most popular options recommended by our readers. Since then, some have remained the same, some have updated their look, and some have undergone some pretty substantial changes, fundamentally altering the way they work and the features that appealed to users, for better or worse.

LastPass

LastPass is clearly the juggernaut here, and for good reason. The service was one of the first well-rounded password managers available, and one of the first that really made it

easy to store all of your passwords either online and synced with other computers and devices, or locally on one device. In short, LastPass remembers your passwords so you don't have to, and makes it easy to audit your passwords, use stronger passwords in general, and even automatically change a password for you if a service has been hacked or compromised. LastPass supports two-factor authentication for your password vault using Google Authenticator, USB devices (using a method we've outlined before), or a YubiKey. The service recently received a visual refresh to streamline the UI and make it easier to use, and sports a number of additional features like credit monitoring, secure password and document storage (and sharing), notifications when a site you have an account with has been hacked, tools to autofill forms and streamline online shopping, and more. LastPass supports Windows, macOS, Linux, Android, iOS, and Windows Phone, and has plugins for Chrome, Firefox, Safari, Opera, and Microsoft Edge.

While the company advises against it, you can download older versions of LastPass compatible with your device. LastPass is free to use on all your devices, including your smartphones, without imposing restrictions. For $24 a year, you can sign up for LastPass Premium. Premium features include priority customer support, 1GB of encrypted file storage (for sensitive info like scanned documents), Windows fingerprint reader support, and two-factor authentication either with a Yubikey or a thumb drive with Sesame.

Dashlane

Dashlane launched in beta back in 2012, debuted a UI refresh in 2016, and has since risen to prominence largely because of its attention to its interface (which is sharp and easy to use), simple security, easy auto-login, form auto-fill, and logging of purchases and orders from online shops. It's picked up a number of updates since then, including support for two-factor authentication, the ability to share passwords with emergency contacts in case you can't access your accounts, and the ability to change multiple passwords on dozens of websites with a few clicks. Dashlane will also notify you if you have an account on a site that's hacked, and with its built-in password changer, you can have Dashlane reset the password to a new, unique, strong one without leaving the interface. If you want to change all your passwords at once, you can do that too. The purchase tracking and digital wallet features make it easy to make online purchases even at retailers you don't have accounts with, and search all of your online orders in one place, while secure note and document sharing gives you a place to store passwords that can't be automatically filled in. Dashlane also gives you the option to store your passwords locally only in an encrypted vault (where only you have the master key), or to sync them to your devices and access them on the web. Dashlane supports Windows, macOS, Android, and iOS, and has plugins for Chrome, Firefox, Safari, and Internet Explorer. It's free to download and use, but if you want your passwords synced across devices, you'll need Dashlane Premium, at $40/yr.

KeePass

If free (as in speech and as in beer) and open source are your go-to requirements for a security product, KeePass is perfect for you. Your passwords in KeePass are stored inside an encrypted database that you control, on your own system, and are never synced or uploaded anywhere unless you want to take them from machine to machine. KeePass is also a portable app, meaning it's super easy to take with you and use on multiple computers, even if that machine is locked down and all you have is a thumb drive. It has its own password generator, to help you change passwords and make sure every one of them is unique and strong. Password databases in KeePass can also be configured with multiple keys so you can share access among privileged users, and exported in plain text for quick importing elsewhere (or backups). You can even create physical password keys in the form of thumb drives or CDs (even floppy disks if you want to go retro). Plus, KeePass has tons of third-party plugins and tools to extend its functionality and bring it to more devices, browsers, and platforms. Most notably, KeePass' auto-type functionality works in all windows and all browsers, which means that KeePass can log in to sites that other password managers can't, and can log in to applications, system dialogs, and other password prompts that you'd otherwise have to copy/paste a password into.

1Password

1Password is well-loved and well-regarded for offering a powerful and secure password manager and digital wallet in a really sharp-looking package that shines on every platform it runs on. It's flexible, easy to use, works seamlessly in just about every web browser, and packs in the same features that you've come to expect from a premium password manager and secure document storage tool. 1Password looks great, comes with a strong password generator to help you pick good passwords every time you change one, secure notes for other passwords or notes that you want to keep private, a digital wallet for bank accounts and payment info, and a password "recipe" builder that lets you customize your passwords to your demands instead of just accepting whatever algorithm the password generator spits out at you. Recently 1Password moved from a one-time purchase to a subscription based business model ($2.99 per month for an individual account, $4.99 per month for a family account supporting five people), and is now storing your encrypted password vault in its own cloud storage service. While it may be inconvenient for users who would prefer to locally store their files, according to engineers at 1Password's company AgileBits, it's more secure than syncing data with third-party storage options like iCloud and Dropbox. Older 1Password users can still use their cloud-synced vaults. If you're desperate for local vault storage, the company hasn't disabled it completely, and you can send them an email to discuss different vault storage options with a 1Password

member. You can also set up an emergency kit as a safety net and share passwords with authorized users. You can even keep multiple vaults for different types of passwords. 1Password supports Windows, macOS, Android, and iOS, with plugins for Chrome, Firefox, Opera, and Safari.
