The best password managers of 2020 and how to use them

A password manager is essentially an encrypted digital vault that stores the login information you use to access apps on mobile devices, websites and other services. Besides keeping your identity

In the best of times, keeping track of your passwords was an overwhelming task for many. And now, with everyone struggling to adapt to a post-coronavirus world, the last thing you need to worry about is which Post-It note has which password on it. That's why it's time to take the plunge on a password manager, if you haven't already. These software services allow you to generate and store secure passwords and manage your login credentials across all your devices, automatically filling in forms in web browsers and syncing your data across Windows PCs and Macs, Android phones, iPads ($400 at HSN), iPhones ($699 at Apple) and more.

A password manager is essentially an encrypted digital vault that stores the login information you use to access apps on mobile devices, websites and other services. Besides keeping your identity, credentials and sensitive data safe, a password manager can generate strong, unique passwords to ensure you aren't reusing them across your devices and services. With all the recent news of security breaches and identity theft, using unique passwords can go a long way to ensuring that if one site gets hacked, your stolen password can't be used on other sites.

Plus, with a manager, you don't have to remember the various pieces of login information, such as credit-card information or shipping addresses. With just one master password -- or in some cases a PIN or even your fingerprint -- you can autofill a form or password field. Some also feature online storage and an encrypted vault for storing documents.

All our best password manager picks come in free plan versions, which typically let you securely store passwords for one device (although our pick for best free manager can be used for syncing across multiple devices). Our best password manager picks also feature subscription options that let you sync your log-in information across all your devices, get access to secure online storage, and share credentials with trusted family and friends. They also all handle hardware authentication through YubiKey. And if transparency is important to you, several of our picks are open-source projects. We also look at what a password manager is and the basics of how to use one.

Note that these services are independently chosen by our editors. The current version of the list is largely unchanged from its previous iteration because we haven't seen any new services that are worthy of taking down our favorites -- yet. If and when that changes, we'll update this story accordingly.

Other free and paid options worth considering

Both LastPass and 1Password are solid, affordable password keepers, and in a straw poll of CNET staffers, they were about neck and neck in use -- though the latter may include some taking advantage of the 1Password for Journalism initiative that offers free service to us hacks. But if you find neither of our two recommended password managers works quite how you want, a handful of other apps are worth considering. These all have free versions available.

Bitwarden

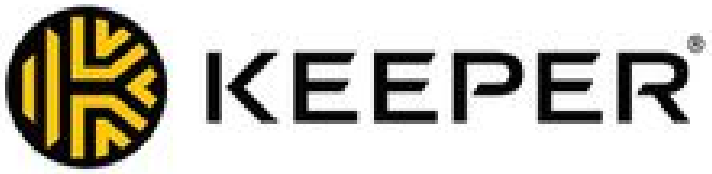
1. Offers free version
2. Base price beyond free: $10 per year
3. Works with: Windows, MacOS, Linux, Android, iPhone and iPad. Browser extensions for Chrome, Firefox, Safari, Edge, Opera, Vivaldi, Brave and Tor Browser.

Bitwarden is a lean, open source encryption software password manager that can generate, store and automatically fill your passwords across your devices and popular browsers -- including Brave and Tor -- for free. It lacks some of the bells and whistles of our picks, but if all you're looking for is a service to manage your login information, it's hard to pass up Bitwarden. And you can share all your login info with another person. For $10 a year, you can add 1GB of encrypted file storage. And for $12 a year, five family members or friends can share login information.

Dashlane

1. Offers limited free version (50 passwords on one device)
2. Base price beyond free: $59.88 per year
3. Works with: Windows, MacOS, Android, iPhone and iPad. Browser extensions for Chrome, Firefox, Safari, Internet Explorer, Edge and Opera.

Dashlane provides a simple and secure way to manage your passwords and keep other login information stored. Just for managing passwords, we like it as much as our picks, but the free Dashlane app limits you to one device and 50 passwords. The $60 Premium subscription is similar to plans from 1Password and LastPass. The $120 Premium Plus annual subscription adds credit and ID-theft monitoring.



Keeper

1. Offers limited free version (unlimited passwords on one device)
2. Base price beyond free: $29.99
3. Works with: Windows, MacOS, Linux, Android, iPhone and iPad. Browser extensions for Chrome, Firefox, Safari, Internet Explorer, Edge and Opera.

Keeper is another secure password service that helps you manage login info on Windows, MacOS, Android and iOS devices. A free version gives you unlimited passwords on one device. The step-up version costs $30 a year and lets you sync passwords across multiple devices. For around $60 a year, you can get 10GB of secure file storage.

KeePassXC

1. It's free
2. Donations accepted
3. Works with: Windows, MacOS, Linux, Chrome OS, Android, iPhone and iPad, BlackBerry, Windows Phone and Palm OS. Access via the web plus popular browser extensions. (Except for the official Windows version, KeePass for other platforms are unofficial ports.)

KeePass, another open-source software, started on Windows and has been ported using the same code base to other platforms, including MacOS, Android and iOS. On the plus side, it's totally free and endorsed by the Electronic Frontier Foundation. On the other side, it's really for advanced users only: Its user interface takes a bit of fiddling to get all the independently built versions of KeePass to work together.

What about NordPass and Norton Password Manager?

There's been a shift in the market for VPN and antivirus software in recent months. Many of the companies behind these software packages are expanding them to become wider software suites. For instance: NordVPN now offers NordPass, a dedicated password manager, and Norton now offers a Norton Password Manager as part of its antivirus and identity theft packages. We haven't specifically reviewed these, if only because they don't yet appear to have a feature set or pricing option that beats any of our preferred options above. If and when that changes, we'll check them out in more detail.

Password manager basics

Still need more info on what password managers are, and why they're better than the alternatives? Read on.

How does a password manager work?

To get started, a password manager will record the username and password you use when you first sign in to a website or service. Then the next time you visit the website, it will autofill forms with your stored user login information. For those websites and services that don't handle automatic filling, a manager lets you copy the password to paste into the password field.

If you're stuck picking a good password, the manager can generate a strong password for you and watch that you aren't reusing it any across services. And if you use more than one device, you want a manager that is available across all your devices and browsers, so you can access your passwords and login information -- including credit-card and shipping information -- from anywhere through the manager app or its browser extension. Some provide secure storage so you can store other items too, such as documents or an electronic copy of your passport or will.

Take note: Many password managers keep the master password you use to unlock the manager locally and not on a remote server. Or if it's on a server, it's encrypted and not readable by the company.

This ensures your account stays secure in case of a data breach. It also means that if you forget your master password, there may not be a way to recover your account through the company. Because of that, a few password managers offer DIY kits to help you recover your account on your own. Worse case scenario, you start over with a new account and manually reset your passwords at each specific destination site and account and start again.

What makes for a secure password?

A good password should be a long string of capital and lowercase letters, numbers, punctuation and other nonalphanumeric characters -- something that's difficult for others to guess, but a snap for a password manager to keep track of. And despite what you may have heard, once you select a good password or passphrase, you don't really need to change it periodically.

Can I use a web browser to manage my passwords and login information?

You can certainly use Chrome, Safari or Firefox to manage your passwords, addresses and other login data. You can even set up a master password to unlock your credentials within a browser. And while using an online browser's password tool is certainly better than not using a password keeper at all, you can't easily access your passwords and other login info outside of the browser or share login info with others you trust.

What about iCloud Keychain?

Through iCloud Keychain, you can access your Safari website usernames and passwords, credit card information and Wi-Fi network information from your Mac and iOS devices. It's great if you live in Apple's world. But if you venture outside and have a Windows or Android device or use the Chrome or Firefox browser, iCloud Keychain comes up short.

You finished reading the article "**The best password managers of 2020 and how to use them**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com