We break down the pros and cons for seven of the best password managers on the market.

If you're like many online users, you might use the same password across personal and work websites to help you avoid forgetting one. If that password is compromised, however, you have to go to each site using that password to update your login credentials. The best password managers put a stop to that so you can stay safe across the internet.

7 Best Password Managers for 2021 How Do Password Managers Work?

Password managers serve as an encrypted digital vault for your online information and important documents. You create a master password upon signing up for a password manager service, and that password then gives you access to your entire data vault of login credentials.

As our lives become more digital-focused, password managers pose several benefits. You can keep your login credentials for every website you use, as well as credit card information, driver's license, passport, Social Security card and tax documents within the data vault of your password manager. Not all password managers, however, are equal. We'll help you select the best service for your needs.

How Did We Test Password Managers?

We rated password managers based on the offered privacy and security. Your online data is sensitive, so our top priority is that information remains secure and private with state-of-the-art encryption.

After that, we reviewed and tested the features provided by each password manager. We also tested the functionality of the apps, browser extensions and web vaults for each company. We considered the overall customer experience and the general reputation of each password manager company.

Finally, we evaluated the cost of each company's password manager plans against the features included to determine the overall value of the service.

Best Paid Password Manager: Dashlane

Pros

Cons

 Easy-to-use interfaces

 Expensive compared to competitors

 Company has never been breached

 The free version has limited features.

 U.S.-patented security architecture

 Only the major devices and browsers are supported

Dashlane offers apps and browsers that are a breeze to use, accessible customer service and airtight security. We recommend Dashlane's Premium plan, which costs $6.49/month or $59.99/year. This plan includes unlimited devices, dark web monitoring, an automatic password changer, encrypted file storage and best of all, access to a virtual private network (VPN). Dashlane partners with Hotspot Shield to provide VPN access — something many password managers can't provide.

Dashlane patented its security architecture to protect your data, which is one reason the company has never been breached. Its "zero-knowledge" security model means your master password, data and encryption key are never sent to Dashlane's Amazon Web Services (AWS) cloud servers. Like most other password managers on our list, your master password will always be stored via encryption on your local device.

Dashlane Specs

Business started: 2009

Advanced Encryption Standard (AES)-256 encryption: Yes

Multifactor authentication: Yes

Access to stored data after cancellation: Yes

Annual third-party reports/audits: No

Unlimited passwords: Yes (but not for free)

Dark web alerts: Yes

Storage: 1 GB encrypted data

Supported devices and browsers: Windows, Mac, iOS, Android, Chrome, Firefox, Safari, Edge, Linux

What we don't like: Dashlane only supports mainline browsers and operating systems, so if you're using a niche browser, this password manager may not be the best password manager choice. The Windows and Mac desktop apps are also reportedly getting nixed this year, which may be a dealbreaker for some. Dashlane is also one of the more expensive password managers on the market, which means it may not fit into everyone's budget.

For a more in-depth look at Dashlane, read our full Dashlane review.

Best Password Manager Value: Bitwarden

Pros

Cons

 Free plan is great

 Pay more to unlock all features

 Premium plan is inexpensive

 Not intuitive for users

 Diverse browser support

 Customer support isn’t strong

For $10 a year, Bitwarden Premium provides unlimited passwords and devices, a strong password generator and the option to use cloud hosting or self-host your data. You’ll also get emergency access, one gigabyte of encrypted file storage and filesharing, Bitwarden Authenticator, vault health reports for your passwords, advanced two-factor authentication and customer support through Bitwarden forums.

Bitwarden is an open-source program, so anyone can see and help make sure its code is secure. Due to this, Bitwarden’s security is well above average, and its software flexibility as an open-source program is virtually unparalleled.

Bitwarden Specs

Business started: 2016

Advanced Encryption Standard (AES)-256 encryption: Yes

Multifactor authentication: Yes

Access to stored data after cancellation: No

Annual third-party reports/audits: Yes

Unlimited passwords: Yes

Dark web alerts: No

Storage: 1 GB encrypted data

Supported devices and browsers: Windows, Mac, Linux, iOS, Android, Brave, Chrome, Firefox, Safari, Edge, Opera, Tor Browser, Vivaldi

What we don’t like: These prices and customization, however, include a few downsides. Bitwarden doesn’t have the same number of features as other pricier password managers, and its customer service isn’t as strong. If you run into a problem using Bitwarden, you’ll have to turn to Bitwarden’s forums to figure out how to fix the problem or try to consult the developers. For many customers, Bitwarden’s customer support won’t be enough for their needs.

The cost-to-features value Bitwarden delivers, however, is unparalleled among password managers. At such a low yearly price for Premium, we recommend Bitwarden over any other password manager if you’re on a tight budget. Read more in our full Bitwarden review.

Best Free Password Manager: Norton Password Manager

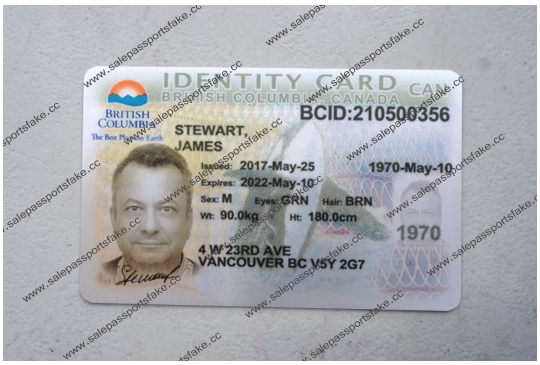
Pros

Cons

 Unlimited password storage and connected devices

 Lacking some important features

 Password autochanger



 Password sharing is not supported

 Biometric authentication

 Poor native apps

If you want to use a free password manager, Norton Password Manager is our top recommendation. Intended to be used as an add-on for Norton 360 plans, you can download Norton Password Manager free of charge.

Norton delivers on security with its password manager, and you can easily identify duplicated and compromised passwords you need to update within the safety dashboard. The password auto-change feature is a perk, but it doesn’t work for every website.

We appreciate that Norton provides 10 gigabytes (GB) of encrypted data storage, which is more storage than most password managers offer and should be enough space for any user.

Norton Password Manager Specs

Business started: 1982

Advanced Encryption Standard (AES)-256 encryption: Yes

Multifactor authentication: Yes

Access to stored data after cancellation: N/A

Annual third-party reports/audits: Yes

Unlimited passwords: Yes

Dark web alerts: Yes

Storage: 10 GB encrypted data

Supported devices and browsers: Android, iOS, Chrome, Firefox, Safari, Edge, Internet Explorer

What we don't like: With Norton, however, you won't have access to a few key features other password managers include, such as the ability to securely share passwords with other people. The web vault worked well when we tested it as a Chrome extension, but we found the iOS app to be lacking when compared to services like Dashlane or LastPass. Customer service can be a little clunky, too — it's difficult to find information on the Norton Password Manager website and we had to fill out an online form on the main NortonLifeLock site in order to chat with a representative.

Best Password Manager for Individuals: Kaspersky

Pros

Cons

 Low price at $14.99/year

 No dark web monitoring

 Intuitive apps

 Limited free plan

 Solid reputation

 No password sharing

For those who don't need to share a password with anyone and want to keep the price of their password manager low, Kaspersky's one-year plan is our top recommendation. At $14.99 per year for new customers, the Premium version offers state-of-the-art encryption for all your devices.

One of Kaspersky's best items of note is the unlimited storage for encrypted documents. You can securely store your sensitive files — driver's license, passport, credit card information, medical records, photos and more — without a data limit. We haven't seen this with any other password managers.

Kaspersky Specs

Business started: 1997

Advanced Encryption Standard (AES)-256 encryption: Yes

Multifactor authentication: Yes

Access to stored data after cancellation: Yes

Annual third-party reports/audits: Yes

Unlimited passwords: Yes

Dark web alerts: No

Storage: Unlimited gigabyte (GB) encrypted data

Supported devices and browsers: Windows, macOS, iOS, Android, Chrome, Firefox, Opera, Safari, Edge

Kaspersky's Premium version is the only plan we recommend. The free plan only stores 15 passwords and documents in total. We also wish Kaspersky provided some sort of dark web monitoring but you may need to tack on an additional ***https://passportgeneratoronline.com***

product such as antivirus protection. Kaspersky also offers a stand-alone VPN.

Best Password Manager for Families: LastPass

Pros

Cons

 Solid browser and device support

 Checkered security history

 Easy to use for the whole family

 Occasional bugs

LastPass is a great option for family sharing because you get access to six accounts for $48 per year. We like LastPass' family manager dashboard and how easy it is to group and share items. Families also receive priority customer support, so you'll be able to access help should you need it at any point.

The http://www.bbc.co.uk/search?q=US Passport Maker online web vaults for Chrome, Safari, Firefox and more, along with the Windows, Mac, iOS and Android apps, are easy to navigate. From password sharing to emergency access to dark web monitoring to advanced multifactor authentication, there's not much more you need from a password manager for your family.

LastPass Specs

Business started: 2008

Advanced Encryption Standard (AES)-256 encryption: Yes

Multifactor authentication: Yes

Access to stored data after cancellation: Yes

Annual third-party reports/audits: Yes

Unlimited passwords: Yes

Dark web alerts: Yes

Storage: 1 GB encrypted data

Supported devices and browsers: Windows, Mac, Linux, iOS, Android, Chrome, Firefox, Opera, Safari, Edge, Microsoft Edge Legacy

What we don't like: LastPass, however, is clouded with a negative security history due to a breach in 2017. LastPass says it has tightened its security since then, and no encrypted data was compromised. There have also been reports of bugs with the apps, and we encountered one bug using the web vault that froze Safari and forced us to restart our browser.

Learn more in our full LastPass review.

Best Password Manager for Businesses: Keeper

Pros

Cons

 Simple interfaces for users

 Add-ons make it pricey

 Strong reputation on Trustpilot

 No monthly plan payment option

Keeper offers business owners a powerful and flexible business plan packed with features. You can manage your team with ease, build security reports and share folders and passwords throughout the company. You can also implement and enforce security policies across the company for heightened privacy.

One of Keeper's best features is the amount of two-factor authentication support it offers. On Keeper's Business plan, you can authenticate through text message, Time-Based One Time Passwords (TOTP), FIDO U2F (Universal 2-Factor) and even a smartwatch. Keeper's Enterprise plan includes advanced two-factor authentication for even greater data security.

Keeper Specs

Business started: 2009

Advanced Encryption Standard (AES)-256 encryption: Yes

Multifactor authentication: Yes

Access to stored data after cancellation: No

Annual third-party reports/audits: Yes

Unlimited passwords: Yes

Dark web alerts: Yes

Storage: 10 – 100 GB encrypted data

Supported devices and browsers: Windows, Mac, Linux, iOS, Android, Chrome, Firefox, Safari, Edge, Opera, Internet Explorer

What we don't like: You will need to pay more for additional secure file sharing up to 10 terabytes (TB). Keeper also offers other features like dark web monitoring, KeeperChat and advanced reporting and alerts for extra money per user every year. For more info on business pricing, check out our full Keeper review.

Best Password Manager for Customer Care: 1Password

Pros

Cons

 Simple to use, especially on Apple products

 No free version

 Friendly customer support

 Lacking features like emergency access

More than any other password manager today, 1Password has figured out how to serve its customers with excellence. That customer care has paid off because 1Password has a loyal fanbase.

As a user, you get first-class security with 1Password, and managing your password vaults via the dashboard is easy. A few features 1Password offers include:

Unlimited passwords and devices with all plans

1Password Watchtower, which monitors the web for leaks

Travel Mode (which lets you hide specific password vaults while traveling)

Two-factor authentication

1Password Specs

Business started: 2006

Advanced Encryption Standard (AES)-256 encryption: Yes

Multifactor authentication: Yes

Access to stored data after cancellation: Yes

Annual third-party reports/audits: No

Unlimited passwords: Yes

Dark web alerts: Yes

Storage: 1 GB encrypted data

Supported devices and browsers: Windows, Mac, Linux, iOS, Android, Brave, Chrome, Firefox, Safari, Edge

There is no free plan, but we think 1Password's customer service is worth the investment. Just one look review of 1Password's community forums clarifies that the dedicated support team stands above the rest. Read our full 1Password review for an in-depth look at plans and features.

Password Manager FAQs

What is a password manager?

A password manager helps you remember your passwords for your online accounts while also keeping them safe. Password managers store your passwords in a cloud-based, or locally hosted, encrypted "vault" online. Your vault is locked behind your master password, which is also encrypted.

Password managers can autofill your username and password information on websites, so you don't have to remember or type them. Most password managers can also autofill your credit card information, shipping address and more.

What features do the best password managers include?

If your password manager provides access to an unlimited number of devices, you can sync your data. That way, no matter which device you use, you can access information in your password manager.

In addition to convenience, password managers often utilize password generators to randomize your passwords so they can be longer, stronger and virtually impossible to guess or hack. Each password should be unique to each account. Having unique passwords for each of your accounts protects you from having a compromised password for multiple websites.

Why do I need a password manager?

Repeating the same password for multiple websites or using weak, easy-to-guess passwords puts your online security at risk, especially in case of a data breach. Hacking is widespread and seemingly easier than ever, which means your safety is on the line every time you use the internet.

Can't I just store passwords in my browser?

If you use a browser like Chrome or Safari that offers to store and autofill your passwords for you, you may wonder why a password manager program is necessary.

Saving your passwords to your browser's keychain isn't nearly as safe as using an encrypted password manager. If a hacker gains access to your physical device, all your passwords can be compromised at one time. Password managers encrypt your passwords and store them out of sight, so a hacker can't see them even if your physical

device is compromised.

Additionally, many password managers offer extra features that do a lot to improve your online security. And password managers do a better job of automatically syncing your items across all devices.

How do I create secure passwords?

We recommend using a password generator for each of your unique login credentials. That way, if any of your passwords are stolen, the rest of your passwords stay safe, and you only have to change one password.

If you want to create a strong password independently, the general rule is the longer, the better. You'll want to include lowercase and uppercase letters, as well as numerical characters and special characters to keep hackers out. Password managers work well because they can instantly remember and autofill long strings of passwords so you don't have to.