How Safe Are Password Managers?

howtogeek.com/445274/how-safe-are-password-managers

Chris
Hoffman

Irina Adamovich/Shutterstock.com

A password manager stores all your passwords and automatically fills them in your web browser and mobile apps. But is trusting an app with your passwords and storing them all in one place a smart idea?

Yes, yes, it is. We recommend everyone use a password manager, which is far superior to other ways of keeping track of your passwords. Here's why they're a safe choice.

Password Managers Are Safer Than the Alternative

A password manager stores your passwords in a secure vault, which you can unlock with a single master password—and, optionally, an extra two-factor authentication method to help keep everything extra secure.

Password managers let you use strong, unique passwords everywhere. This typically isn't possible for most people—can you really remember unique, strong passwords for every website you use? Password managers can generate and remember passwords like E.wei3-uaF7TaW.vuJ_w.

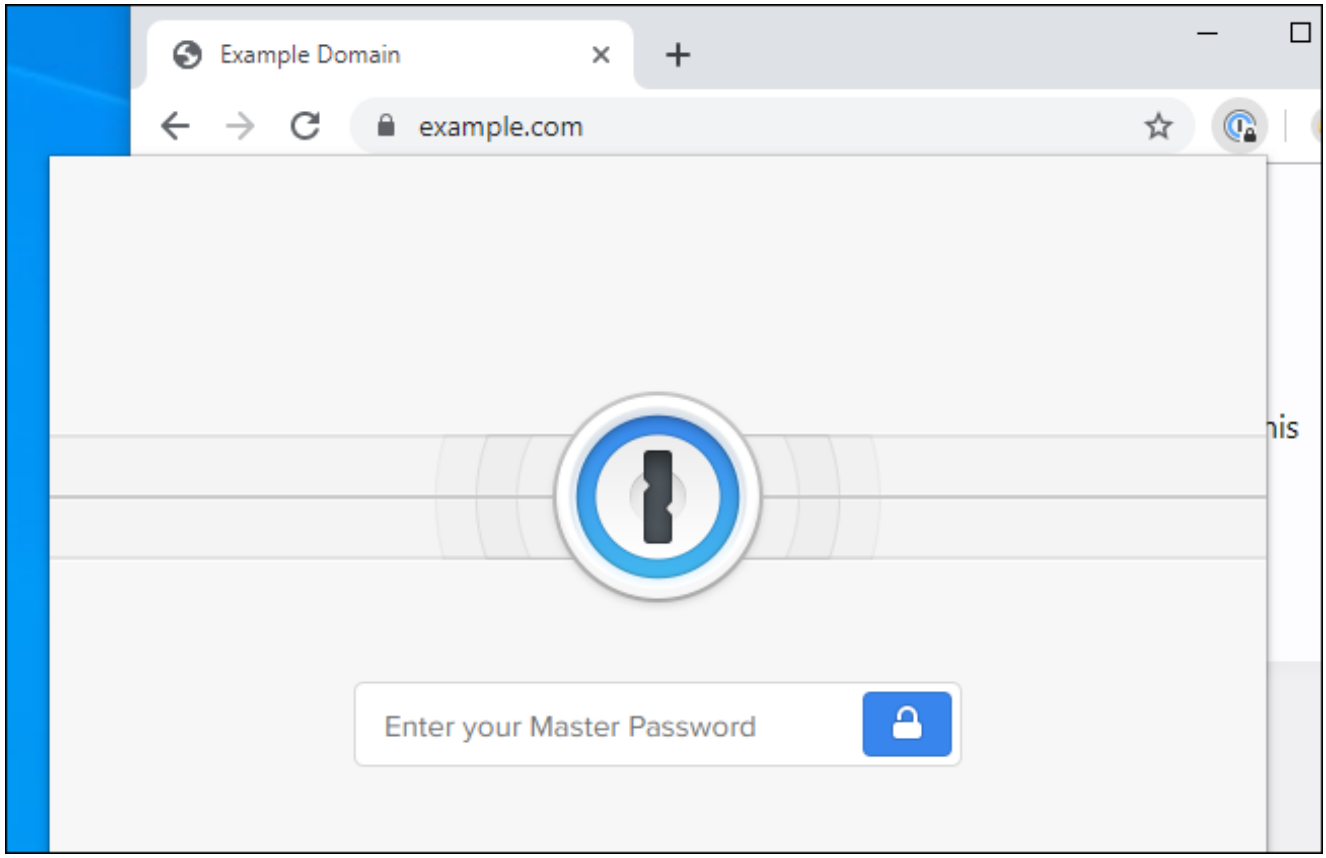
If you don't use a password manager to store your passwords, you probably can't remember all the unique, strong passwords you would need to use. Most people end up reusing passwords on multiple websites—that's the most dangerous thing, as a password database leak at once website means your accounts on another site are wide open. Someone just has to try signing in with the same email address and password combination from the breach.

You could try creating "unique" passwords yourself based on a pattern. For example, maybe your base password is _p@ssw0rd_. You could modify it based on the domain—for example, when signing into facebook, you could take the "f" and the "a" and make it fp@ssw0rda. Repeat this for each account you use, and you have unique passwords you can remember yourself, right? Well, not really—your passwords are now predictable. And what happens when a website doesn't allow special characters or limits you to a specific number of digits and your method doesn't work?

With a password manager, you just have to create one strong password and remember it .

While you do have to place some trust in whatever password manager you choose, using a password manager is more secure than the alternatives. The password managers we recommend have never had their passwords compromised, but many people have gotten in trouble through reusing passwords. Exploiting those reused passwords is often how attackers "hack" accounts these days.

How Password Managers Secure Your Passwords

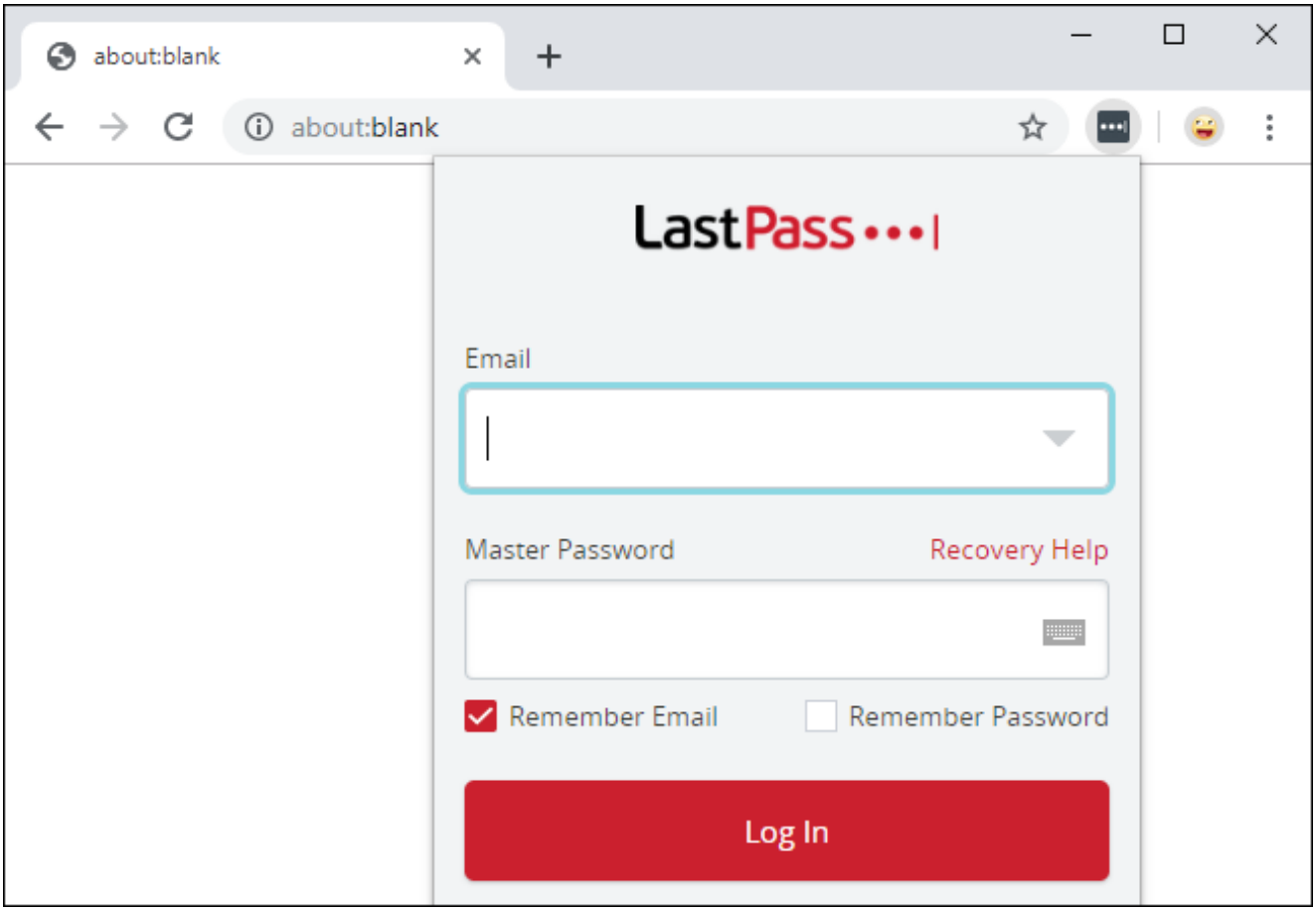


We—and many other sites—recommend 1Password and LastPass as our top picks. Both protect your password vault with strong encryption (AES-256, specifically), even while it's stored in the cloud. While the passwords are on your PC, phone, or tablet, they're protected with a "master password" you know that makes them unreadable by anyone without that password. On modern devices, you can also unlock your vault with biometric authentication—like Face ID or Touch ID on iPhones.

Both services say the master password never leaves your device, and they couldn't access your passwords if they want—they have "zero knowledge" of your passwords. They've undergone third-party audits and code reviews. Neither has ever suffered a serious breach, and both are up-front and transparent about how they protect your data. See the 1Password and LastPass websites for more details.

Prefer doing it yourself? Open-source password managers like Bitwarden and KeePass also exist. You can use these open-source applications to store your password on your own devices or servers. For example, you could set up your own sync server for Bitwarden or manually sync a KeePass database between your devices. It will likely be more complex and more work—and the apps aren't as user-friendly—but if you prefer open-source software, options are available.

Can You Trust Password Manager Companies?



Ultimately, you are placing some trust in the password-manager companies here. Sure, the companies promise to keep your passwords safe, but they could update their software to capture your passwords, or a massive security hole could open your passwords to attack. The companies are audited for security, but what if they turned bad?

Sure, that's a risk. You trust your password manager like any other application you use. The same is true for any application on your PC or most browser extensions: They could spy on you and phone home, reporting your passwords, credit card numbers, and communications to someone else.

But that hasn't happened yet. These are reputable companies in the business of security. It's probably more dangerous to install random browser extensions—many of which get full access to everything that happens in your browser and could phone home with those details—than store your passwords in a password manager.

We Use Password Managers and Recommend Them

We follow our own advice and use password managers like 1Password and LastPass here at How-To Geek, too. The password managers built into browsers like Chrome and Apple's Safari are getting better, but they just aren't as powerful or fully featured yet.

On top of the safety, password managers offer many convenience benefits. You can easily share your passwords with a friend, family member, or coworker. You can automatically fill those passwords on mobile without typing them in—even on an iPhone or iPad. Password managers like 1Password and LastPass provide alerts if any of the passwords you're using have been breached in an attack and recommend passwords you should change. It's a big improvement over trying to keep track of all your passwords without any help.

RELATED: ***Why You Should Use a Password Manager, and How to Get Started***