# Password Managers: The Pros and Cons

Lance Whitney, TOP STORY

*You can rely on password managers to automatically take care of your website passwords, but there are a few hurdles you'll have to overcome.*

Password managers provide an effective means of cooking up and controlling your website passwords so *you* don't have to deal with the hard part of creating them, using them on the Web and -- this is key -- *remembering* them. Such tools offer several benefits, including the ability to generate complex passwords, store and remember your passwords, and automatically apply them at their respective websites.

But you still need to be aware of potential snags when using a password manager. For example, you have to create and remember a complex master password that can protect all your other passwords, otherwise there's the possibility of someone gaining access to your passwords. Your passwords are typically stored on a server maintained by the vendor, and we know that servers can be hacked. Plus, password managers are only good on the devices on which they're installed. Use a friend's PC or a computer at the library, and you're stuck because you don't have access to the passwords for your sites. How can you benefit from the pros of password managers while still dealing with the cons?

First, let's briefly highlight a few password managers and the benefits they offer.

## Dashlane

Available for Windows, Mac OS X, iOS, and Android, Dashlane sets itself up as an extension to your web browser. The software works with all the major browsers with the exception of Microsoft Edge, which doesn't handle too many extensions as this point. To use Dashlane, you create a master password to store all your website passwords. When you log into a website, Dashlane prompts you to save your username and password to its collection. The next time you visit that site, the software automatically populates the right fields with your login credentials. **The basic version of Dashlane is free; the Premium version that allows an unlimited number of devices is $39.99 a year**

.

## 1Password

Another password tool that works with Windows, Mac OS X, iOS, and Android, 1Password integrates with your web browsers to generate and store your website passwords. The software creates, stores, and applies a complex password for each site. You're prompted to think up a secure master password to protect all your website passwords. You can try **1Password for free for up to 30 days. After that, you'll have to shell out $2.99 a month for the individual version or $4.99 a month for the family version.**

## LastPass

Designed for Windows, the Mac, iPhone, iPad, and Android devices, LastPass works as a browser extension. You create a master password to store your website passwords. Sign into one of your password-protected sites, and LastPass prompts you to save the site and your login credentials into its "vault." The next time you log into a site, LastPass automatically populates the username and password fields with the correct credentials. **The basic version of LastPass is free. A premium edition for $1 a month offers extra features, such as family sharing and fingerprint identification.**

## RoboForm

Available for Windows, the Mac OS X, iOS, and Android, RoboForm also sets itself up as an extension in your browser, specifically appearing as a toolbar. When you need a new password for a website, you can tell RoboForm to generate a complex password using alphanumeric characters as well as symbols. That password is then saved. The next time you browse to that website, RoboForm recognizes the URL and automatically populates the right fields with your username and password. **The free version limits you to ten logins; the paid version offers unlimited logins and costs $19.95 a year**.

So in a nutshell, here are the pros of password managers:

- They create complex passwords that are strong and secure, saving you the time and energy of trying to devise such passwords yourself.
- They can create a different password for each website, so you don’t run the risk of using the same password over and over again.
- They store those passwords so you don’t have to worry about remembering them yourself.
- They automatically apply those passwords at their respective websites, saving you the hassle of having to manually enter your login credentials.
- And they work across all the major browsers and operating systems, including those on mobile devices. LastPass and RoboForm even support Microsoft Edge in Windows 10.

Sounds great. Yep, it is, but what about the cons? What are the failings or flaws of password managers, and how can you get past them?

First, you need to think of a complex password to safeguard all your other passwords. That’s certainly more doable than trying to juggle dozens or hundreds of complex passwords for all your websites. But still it is a password that’s critical and one that you have to create and remember.

To generate your master password, the usual rules apply. Make it difficult to hack but easy for you to recall. You can adopt a long string of uppercase and lowercase alphanumeric characters as well as symbols, such as B73hq-19FF!vFg13. But another and perhaps better option is to use a phrase or sentence, such as “*You're* traveling through another *dimension*, a *dimension* not only of sight and sound but of mind.” Experts recommend using sentences as passwords, and the master password can be a lengthy sentence since you don’t have to type it that often.

Second, your website passwords are stored on a server maintained by the vendor of the password manager. That server is naturally protected by a firewall, while the passwords themselves are encrypted. But that doesn’t mean you’re 100% in the clear. LastPass was **hit by a hack in 2011** and **again in 2015**, both of which compromised certain user data, though the website passwords were untouched. However, if a hacker was able to guess your master password, that potentially leaves your website passwords at risk. So what’s the answer? Create a strong master password. The stronger it is, the more unlikely a hacker could ever figure it out. In 2011, the CEO of LastPass even said that anyone with a strong master password had no reason to be worried.

Third and finally, your website passwords are stored on your own desktop PC and/or laptop. That means you have no access to them if you’re using a computer at a different location and don’t have your laptop with you. Well, that’s a limitation you can correct. RoboForm offers a program called RoboForm2Go, which stores your website passwords on a USB drive that you can plug into another computer. However, RoboForm2Go is no longer being updated as browsers increasingly are restricting the attachment of these types of extensions. So what’s the alternative? You can run your password manager on your smartphone. If you’re using a computer at a library or coffee house or similar spot and you need to log into a password-protected website, simply consult the password manager on your mobile device for the login credentials.

## In conclusion

Password managers may not be the perfect solution, but they’re far better than the alternative of using simple passwords or using the same password at every website. Until the industry is able to offer a truly superior and secure website login method, password managers are your best bet.