CODEX

Should we save our passwords in a browser?

Naved Anjum Follow
Sep 9 · 3 min read

Don’t allow your browser to save your passwords. None of them. Not one. If you do, those passwords are vulnerable. All someone has to do is have access to your computer (remote or physical) and, unless you use Safari or the Master Password feature in Firefox, those passwords are available for anyone to see.

If you absolutely must have your browser store your passwords, and you’re not using macOS, make sure to use Firefox and enable the Master Password feature. Use Chrome at the peril of your passwords.

In place of having your web browser store your passwords, make use of a password manager. By doing so, the likelihood of someone viewing your passwords is considerably lower. It's not perfect, but it's far better than handing over the security of your passwords to a web browser.

There are various types of password managers to choose from, with cloud-based options being among the most popular. The added benefit of them using the cloud is having access to your passwords from anywhere. Most of the popular brands (1Password, Dashlane, LastPass, etc.) offer apps for your smartphone, so if you use multiple devices (which most of us do), then cloud-based services will sync all your passwords across all devices. Some even have desktop options and browser plug-ins, so they have all of the bases covered.

When it comes to subscriptions, the basic set of options is offered for free. If you find those lacking, you can always pay for one of the more premium tiers, which usually include more settings and added security features.

As convenient as all of this sounds, it comes with one caveat. You're putting all your eggs in one basket, as it were; and some online password managers have faced their share of problems in the past. A few months ago, for example, researchers found security flaws in a number of popular password managers, some Android versions of their apps were found to be susceptible to phishing attacks, while others allowed endless attempts at entering the master PIN.

It is important to keep in mind that since your data is stored on a server, in case of a breach or a successful hack, cybercriminals can download the information in bulk and your account may end up in that data trove. Should this happen, you are dependent on the operators of your chosen service having properly implemented strong encryption *and* on the strength of your master password, keep in mind that it guards the gate to most of your digital life.

Although most of us have similar needs when it comes to managing our digital lives, there may be minute differences in our preferences. So, you need to be aware of which option suits your requirements the best. There are at least a few questions you should answer for yourself when choosing a password manager:

- How does the service you've chosen store your data?
- If something happens to your device, is the data recoverable?
- Are there any additional security options you can activate to boost protection?

Be sure to choose your password manager carefully and avoid the common mistakes when you're creating your master password.

Cybersecurity Password Management Infosec Awareness Digital Privacy