5 things you should know about password managers

More like this

•

RELATED TOPICS

New data breaches are coming to light almost weekly and they reveal a simple but troubling fact: many people still choose weak passwords and reuse them across multiple sites. The reality is, remembering dozens of complex passwords is almost impossible and carrying them around on a scrap of paper that you have to keep updating is a huge hassle. That's why there are password managers.

Here's why they're important, and how to get the most out of them.

1. Password variety is important

Password leaks are a case of "when" and not "if," so you should limit the damage attackers can do by choosing a different password for each online account. Remembering all those passwords is hard without making them predictable, and that's where password managers can play a big role. They're available for most browsers and operating systems, including mobile ones, and provide a hassle-free login experience.

2. Password complexity matters

Most password managers can generate complex passwords for you, and that's important. Websites generally store cryptographic representations of passwords called "hashes," but depending on the algorithm used, those hashes can be cracked. The more complex a password, the less chance an attacker will be able to recover it from the hash, so it's good practice to use passwords with 12 or more characters, combining upper and lower case letters, numbers, and special symbols.

Usually, you'll still need to remember a master password that logs you into your password manager. You may also want to know your password for a few critical accounts, like email, in case the password manager is unavailable for some reason. In that case, sequences of words combined with digits and uppercase letters can be just as difficult to crack. An example would be DogsCatsRabbitsMyTop3Animals. These are typically referred to as passphrases, because they're longer.

3. Offline vs. online

Password managers employ a variety of security models. Some are offline, like KeePass, Password Safe or Enpass, which means they don't synchronize across different devices: you have to move the encrypted database between the various instances of the program each time you add or change a password, or use a cloud sharing service like Dropbox to keep the database in sync. Others, such as LastPass, Dashlane and 1Password, automatically synchronize your passwords across different devices, and some even provide web-based access to your password "vault."

If you choose one of the service-based implementations, pay attention to the architecture and make sure it decrypts the database locally inside the application or browser, without ever sharing the master password with the service provider.

4. Don't rely on a master password alone

Protecting all your passwords with a single master key isn't the best idea because it can create a single point of failure. But many password managers offer two-factor authentication, where accessing the password vault also requires a one-time code sent via SMS or generated by an app such as Google's Authenticator. Make sure the password manager you choose has this feature, and turn it on.

Even when you're using a password manager, it's a good idea to enable two-factor authentication (sometimes called two-step verification) for all your online accounts that offer it. An extra layer of protection never hurts.

5. Make use of other security features

Some password managers offer the option to log you out after a period of inactivity. That's useful, because it's not a good idea to keep the password vault open for extended periods of time, especially on a shared computer. Logging you out automatically can limit the damage if your computer gets temporarily infected with malware. It's also best not to flag devices as "trusted," which disables two-factor authentication for that device.