How Password Managers Helps Protect Your Data While Browsing the Internet

TechRounder PDF Edition

Live article:
https://www.techrounder.com/security/how-password-managers-helps-protect-your-data-while-browsing-the-internet/

By Vipin PG | Published July 27, 2022 | Updated March 8, 2026 | Format: Analysis | 5 min read

In brief

A password manager is a computer program useful for storing, generating, and managing passwords for local applications and online services. A password manager is convenient for the users as it holds all the passwords securely.

A password manager is a computer program useful for storing, generating, and managing passwords for local applications and online services. A password manager is convenient for the users as it holds all the passwords securely. If a password is forgotten, the password manager helps retrieve it as the data is stored in the program.

The password manager also helps create strong and unique passwords for all the essential accounts. Password managers protect the users from the risk of phishing attacks as hackers can deduce easy passwords without any hassle. It also stores passwords of every account, so a user doesn't have the load to remember everything.

In many cases, password managers eliminate the possibility of typing the passwords hence helping the users from typing it in a crowded place where the chances of people looking into the password are maximum. This article discusses the basics of password managers and the types of managers you can choose from.

Password Manager

Password managers are a form of cross-platform support. These programs also support using biometric data instead of a master password for additional security. There are many ways by which password managers help users to protect their data while browsing the internet. There are three types of password managers that help to save data while browsing.

Online Password Manager Services

Web-based or online password manager services help users to store their passwords on multiple devices. In this type of password manager, there is only one location, and all devices must sync to that location. The passwords in this type of program are stored on a cloud that is the provider's server.

An advantage of using this type of password manager is that most managers are free of cost; hence no extra money needs to be paid. Additionally, hackers can try phishing attacks, but that might be useless as online password manager services store the data in the provider's server, making it difficult for the hackers to access the data.

Offline Password Managers

Offline password managers or locally installed password managers store the data in the device. The device can be a smartphone or a computer. The passwords are stored separately from the password manager in an encrypted file. Password managers often increase the possibility of securing the data by storing each password separately.

One must have a strong master password for accessing the offline password manager. One of the significant advantages of using offline password managers is that these programs make it harder for hackers to access the system. As all the passwords are stored offline, one can only access them easily by seizing the device.

Token-Based Password Managers

There are a variety of password managers available today, each with its own set of features. For example, some offer token-based authentication as an added layer of security. But is this necessary?

Token-based password managers or stateless password managers are the programs where a local piece of hardware is used to access or unlock specific accounts. This hardware can be a flash USB device. This type of password manager does not require synchronization between the devices one uses, as there is no data on those devices.

In this way, hackers cannot find the passwords, preventing attacks and securing data on devices while using the internet. Token-based password managers are open-source, and most are free of cost.

Token-based authentication adds an extra step to the login process, requiring the user to enter a code from a physical device or app in addition to their password. This makes it more difficult for hackers to access accounts, even with passwords. For extremely security-conscious people, token-based authentication may be worth the inconvenience. But for most users, it’s probably not necessary. A strong password is still the best defense against online attacks.

The usefulness of Password Managers

There is no doubt that password managers can be helpful. They can help you keep track of all your passwords in one place, and they can also help you generate strong passwords. However, there are some potential drawbacks to using a password manager. First, if you forget your master password, you will not be able to access any of your passwords.

It can be a significant inconvenience, and it may even result in you losing access to important accounts. Web-based password manager services also help backing up your data, so data is not only secured but is always kept retrieved. Additionally, if your password manager is compromised, all your passwords could be at risk. Therefore, it is important to choose a password manager that is secure and that you trust.

Choosing The Right Password Manager

There are many factors to consider when choosing the right password manager. The most important factor is security. Ensure that your password manager uses strong encryption methods to protect your passwords.

Another critical factor is the ease of use. Choose a password manager that is easy to use and understand. Finally, consider the price. Some password managers are free, while others charge a monthly or annual fee. Choose the password manager that fits your budget and needs.

Several password managers are out there, and picking the right one can be tricky. Here are a few tips to help you choose the right password manager for your needs.

- Make sure the password manager is compatible with your devices.
- Choose a password manager that offers features that meet your needs.
- Compare the security features of different password managers.
- Consider the price of the password manager.
- Read reviews of password managers before choosing one.

Conclusion

In these ways, one can secure their data at any given time. Password managers are not only helpful in securing passwords but are also beneficial in the safekeeping of essential documents, medical records, and photos in an encrypted vault.

In addition, Internet security is maintained using password managers. As you can see, a password manager can be a handy tool, particularly if you have a lot of different passwords to remember. Using a password manager can help keep your passwords safe and secure and make remembering them easier when needed.

References

1. rd.com - list / what-hackers-can-do-with-email-address - https://www.rd.com/list/what-hackers-can-do-with-email-address/

2. safetydetectives.com - best-password-managers / chrome - https://www.safetydetectives.com/best-password-managers/chrome/

3. creativebloq.com - advice / back-up-data - https://www.creativebloq.com/advice/back-up-data