By Jen Sharp Jensharp.com

Open Sesame! *How a Password Manager is Easier and More Secure*

We've all been there… you're in a hurry trying to finish a transaction and the app asks you for your password. You forgot it! And now you have to use the forgot-password feature and reset it. You have to choose something you'll remember because this is annoying! So, you use what you normally use, your dog's name. No, it needs a number. Okay, your dog's name and the number "1"… no it needs a special character. Your dog's name, the number one, and an exclamation mark. GOT IT! You're in!

For both security and personalization, many sites require logins, and keeping track of all those usernames and passwords can be stressful. You barely remember that Monday is trash day – why add yet one more password to the mix? After all, why would a cyber criminal want to know your login to PetSmart? Because many people use the same or similar passwords for multiple sites, across both work and home accounts. This creates vulnerability in many areas, even beyond where an original breach may have occurred.

Although security breaches were down in 2022, the threat is still present and costly. Reports estimate anywhere from 44 to 49 million Americans were affected by breaches in 2022, causing identity theft, unwanted financial transactions, and spread to other contacts. The mistake of a single employee unwittingly allowing a breach or leak can take down an entire company. So, your individual password matters.

What's the solution then?

Enter the Password Manager. Password managers allow you to store, generate, and manage all your passwords across many accounts and devices in one vault, accessible by a single password. This allows an individual to only have to recall one complex password rather than any of the other passwords for all of the accounts they collect.

A single password? Isn't that risky?

Isn't it easier for cybercriminals to access your passwords because all of your password-eggs are in one proverbial basket? Not at all! With the level of protection provided by a password manager, it would take password-cracking hackers over a lifetime to crack the cipher of a complex password generated by the password manager — even with the help of their hacking software.

Nothing is 100 percent secure, and password managers never claimed to be. However, they can be more secure and easier to manage than creating and managing your own passwords across several accounts. Cybersecurity specialists agree that password managers are the most secure way to manage and protect your passwords if you use them properly.

How does it work?

Instead of using simple passwords for all these accounts, you can use a unique password for every account. The password manager autofills your passwords according to website or your direction after you login to the password manager account. Also, the password manager can generate a new password with a high level of complexity and

Where do I get one?

Password manager software is commonly found, and a simple search on the web can yield many leads. You should investigate these, research online reviews, ask others in person for recommendations, and take advantage of free trials where available. Though not an exhaustive list, here are some examples of popular password managers:

- 1Password
- LastPass
- NordPass
- RoboForm
- Keeper
- Dashlane
- StickyPassword
- Norton
- KeePass
- Enpass
- Apple Keychain

What features should I look for?

Getting the best password manager means you find features that fit your particular needs. For example, if you use your smart phone for work, you will want a solution that offers protection across multiple devices. If you travel often, you might opt for a built-in VPN. Here are some ideas for features you can look for:

- Data breach scanner
- Dark web scanner
- Built-in VPN
- Secure password generator
- Create based on selected criteria
- Password weakness detection
- Supporting multiple devices
- User-friendliness
- Mobile compatibility
- Browser integration
- Affordable Cost
- Free trial before you buy
- Two-factor authentication
- Bio-metric login options

length that is difficult for you to remember, which also makes it difficult to crack. For example, according to Hive Systems[1], an 8-character password with numbers, upper and lower case letters, and special characters takes a hacker only 39 minutes to crack using software that costs only $1,500. But one with 12 characters takes 3,000 years. Even more significant, an 18-character password with only lowercase letters (no uppercase, no numbers, no symbols) would take two million years to crack.

The complexity and length of passwords are not the only advantage to using password managers. For example, password managers use encryption to protect your password and can do so across multiple accounts. Two-factor or multi-factor authentication can add another layer of protection, as this feature requires a separate device such as your smart phone to verify any login activity. Another layer could include biometrics, such as fingerprints or face scans, that verify it is really you accessing the password requested. Password managers also add commonly built-in protection from viruses, malware, spyware, spam, and hacking.

The BIG picture

While nothing is 100 percent secure, using a password manager is far more secure than typing in "Fido1!" for every new login you have to create! Without a password manager, the results from exposed passwords are far more common and far more severe. The availability and low-cost of password manager solutions makes choosing to use them a no-brainer.

Since 1997, Jen Sharp (JenSharp.com) has served business and government across Kansas and the US and even internationally, specializing in Web development, design & programming including e-Learning, ecommerce, content management systems, and other small business solutions.

[1] Source: https://www.techrepublic.com/article/how-an-8-character-password-could-be-cracked-in-less-than-an-hour/#:~:text=As%20described%20in%20a%20recent,the%20latest%20graphics%20processing%20technology