NJSBA
PRACTICEHQ
PREPARED BY
Affinity CONSULTING

PASSWORD MANAGERS

By Jeffrey R. Schoenberger

WHAT IS A PASSWORD MANAGER

A password manager is a program that helps one store, create and organize passwords (and logons and websites, etc.).

PURPOSE OF A PASSWORD MANAGER

The purpose of a password manager is three-fold:

1. The program helps you create and store the innumerable login credentials that we all generate. A password manager can propose super-complex, impossible-to-guess, and impossible-to-remember, unique passwords for each site requiring a login. Most password managers also offer to store ancillary data, like software license keys, credit card numbers, store rewards card numbers, and things of that nature.

2. The password manager installs a plugin in your browser and "watches" while you surf the web. If you visit a site for which you've already created or stored credentials in the password manager, it offers to log you in without you having to type, or even copy and paste, your credentials. If you visit a site for which you need to create a username and password, the password manager suggests strong passwords.

3. Most, but not all, password managers let you sync your data over the internet. That way those super-strong, unmemorizable passwords are accessible on your smartphone, tablet, and any additional computers you have. Having those passwords stored with a third party understandably makes some folks nervous. But, unlike most cloud storage vendors, you define the password that unlocks your data. If the password syncing website suffers a breach, the hackers can steal only encrypted data. They still need your "master password" to decrypt your password file. That master password is the one unique, complex password that you do need to memorize.

WHY YOU NEED A PASSWORD MANAGER

1. It's a place to keep logons, websites, account numbers and passwords all in one place. I use 1Password and it will generate and store strong passwords for me (so I don't have to make them up).

2. It will also let me know if my passwords are weak and recommend that I change them. It tells me how many different websites I'm using the same password for (it's not recommended that you use the same password for everything).

3. It also lets me know if there are any reported security breaches for any of the websites it holds passwords for and recommend that you change them.

4. It will hold all my credit card information, secure notes about anything I want and personal information like my driver's license, passport, etc.

5. Finally, it's part of my estate plan. If something happens to me, there's one place that other family members can go to find all pertinent information; everything from credentials to pay the water bill

to PDFs of my actual estate plan documents. In 1Password, this feature is called the Emergency Kit, which is a fancy name for a mix of computer and handwritten information that you complete and store somewhere secure, like a safety deposit box, that family members can access if needed. It will have confidential access information, so it's not something to keep out in the open.

SECURITY NOTE

LastPass suffered a breach in August 2022. The usernames and passwords in the stolen data were encrypted, so a good master password should protect them. Still, given the details in the *Ars Technica* article, replace LastPass with Bitwarden when comparison shopping.

If online password storage unnerves you, the open-source KeePass stores password data only locally on your machine, not in anyone's cloud, but that makes you responsible for backing up and securing your data.

GOOD OPTIONS

Top rated password managers include the following (and I strongly recommend the versions you have to pay for - almost all offer a free version that is missing features):

1PASSWORD - https://www.1password.com/

BITWARDEN - https://bitwarden.com/

DASHLANE - https://www.dashlane.com/

KEEPASS - https://keepass.info/help/v1/setup.html

ROBOFORM - https://www.roboform.com/