

The Vault in Your Pocket

Getting to Know Password Managers



DEER
BROOK



The requirements for a good password are tough.

Upwards of 15 characters, including alphanumeric and special characters, and no phrases or easy substitutions (0 for o) either. And that's just to start. It might be easy to manage one or two passwords of that kind, but keep in mind it's best practice to be using a totally unique password for each website and service you use.

Now, managing your passwords becomes a headache.

That's why we're going to tell you about password managers, what they are, and why you should strongly consider using one.

What's a Password Manager?

A password manager is like a vault, storing your passwords for each website and account you have.

Most password managers also have the ability to create strong passwords for you, allowing you to store them right alongside your others in the vault. You access your vault with a master password, one that must fit stringent requirements and should be arguably the strongest password you've ever come up with.

Password managers can also sometimes have built-in, optional features like prompting you to auto-fill

credentials on a login screen, although features such as these come with an inherent security risk.

Overall though, password managers are an excellent alternative to storing your passwords physically or using slight variations of your primary password across multiple websites.

Why should I use a Password Manager?

Reliance on a password manager means you can give your brain a break having to remember all your passwords.

It also creates an opportunity for you to have long, unique, and extremely secure passwords for each of your websites and accounts. Using these unique passwords, nearly unrememberable to the human mind, makes it drastically harder for hackers and credential stuffers to break into your accounts.

On top of that, a centralized password manager at the hub of all your account credentials means the only impetus on you, the user, is to remember your master password and not all of these convoluted (but secure) account passwords.

Security is all about minimizing your risk, and although the prospect of having a master password might seem like a concerning one, password

managers offer a wide berth of password security that nothing else can.

Are Password Managers safe to use?

There's no such thing as 100% secure in the realm of cybersecurity, but password managers are reliably safe to use.

Password managers receive your master password and store your other passwords in an encrypted, scrambled state, so if a hacker does manage to exfiltrate your password data, it's pretty useless for them and it's nearly impossible for them to decrypt.

The main benefit of a password manager is that you can have unique, long, complicated passwords for each account you use. Brute force methods that do often work for many people's account credentials will instead take a lot longer for accounts you have stronger passwords for.

And in the instance one of your accounts does get hacked, the damage will be relatively small and isolated to that one website or service since you have unique passwords for each of your accounts.

Trusted, vetted password managers are safe to use and there's a lot of benefits to doing so.

Where do I get a Password Manager?

There's a lot of contenders on the market for the "strongest" or "best" password manager, but we won't dictate which one you should use; consider your motives, objectives, and potential features you'd like to have in a password manager and seek one out that checks as many of those boxes as possible.

Start your search on a trusted, credible source that has an article or a page dedicated to directly comparing multiple password managers like CNET or Consumer Reports. Be wary of videos by YouTube influencers or articles that feature a "preferred choice," because these features and positions are often paid for by the companies being highlighted.

Once you've done some research, which can include soliciting opinions from those you trust on this subject, do some final research to verify that the password manager you're looking to get is trustworthy and hasn't fallen victim to any data breaches or hacking attempts.

From there, utilize your password manager in the best way possible: diligently add your passwords to the vault, update your insecure passwords, and remember to create an exceptionally strong master password.

It's time to make a choice

In the realm of cybersecurity, a lot of prevention boils down to "when," not "if."

On one hand, strong passwords might not mean much if hackers exfiltrate data from a company and reveal they stored your account password in plain text.

But on the other, that doesn't mean you shouldn't take steps personally to ensure your passwords are strong and not worth the effort for rudimentary brute force attacks and credential stuffing. Strong passwords can be the difference between falling victim to every attack under the sun, or just those that are incredibly nuanced and thorough.

The requirements for a password are tough, and rightfully so.

