

Password Manager Myth Debunker



Know the truth about password managers!

High-quality password managers are the safest way to store your passwords and ensure that you use strong, unique passwords for each of your many accounts.

But there are many misconceptions about password managers floating around, but we'll help you separate fact from fiction. Password managers are not like putting all your eggs in one basket, because baskets don't have MFA or zero knowledge architecture.

MYTH	REALITY
Don't use a password manager because all your passwords are compromised if it gets hacked.	Because of the technology password managers use, the company doesn't even know your master password. So make it a long and unique password! And when you turn on MFA on your password manager, it's even more secure. Even when a password manager company gets hacked, cybercriminals can't access your passwords.
My spreadsheet/notes app/notebook is safer than a password manager.	No other method of storing passwords is as safe as a password manager because of their encryption. Physical notebooks and sticky notes can be lost, damaged, or stolen. Password managers also let you create long, complex, and unique passwords easily for every online account. With other methods, you'll likely reuse passwords or depend on short, less random ones.
Password managers are expensive and hard to use.	The leading brands of password managers all have free versions, and they have the same security features as the paid versions. Once you start using a password manager as a web browser extension, you'll see how simple they are to incorporate into your web surfing.
My workplace won't let me use a password manager.	Many workplaces use password managers now -- ask your security or IT team what they recommend. Even if your workplace doesn't have a password manager, you should definitely use one for your personal accounts.

You have a lot of passwords, but you can start small! Research your password manager options, install one you like, and start adding a few passwords at a time. The program will help you change weaker passwords and create great passwords for new accounts.

Take a few minutes today and get started -- your online safety is worth it!

OUR FAV PASSWORD MANAGER SETTINGS:

- MFA: Enabled
- Minimum password length: 16 characters
- Recovery codes: Saved in a safe place (like a safe!)