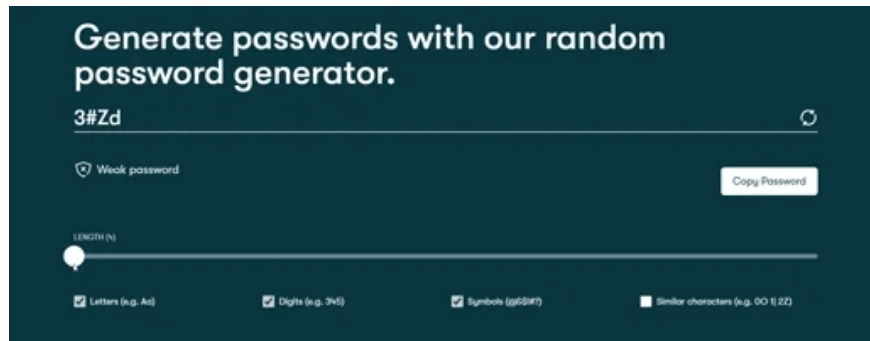


4 Mistakes to Avoid When Setting Up a Password Manager

When setting up a password manager, there are a few things to keep in mind to ensure you have a secure and effective setup to avoid frustration later on.

1. Use a strong password

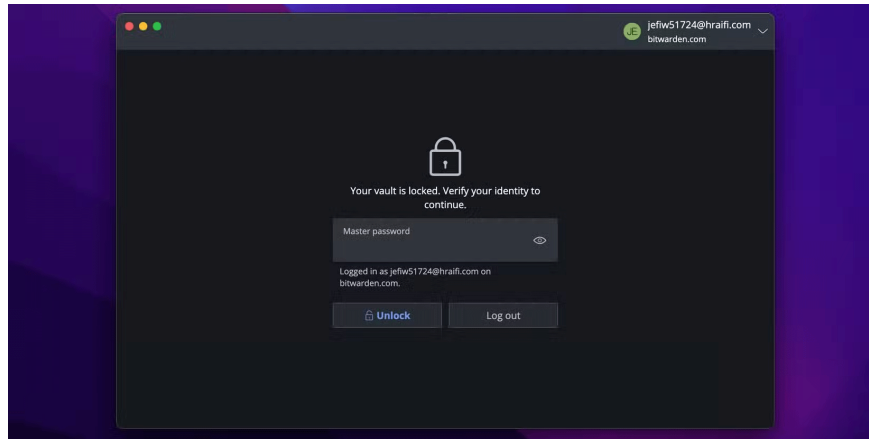


You've set up a password manager, but your master password is 'p@55w0rd123'. Oh dear! Remember, you're setting up this password manager to store all of your passwords - passwords to your bank accounts, social media accounts, etc. Your master password is essentially access to your entire digital life.

Think of it as something that only you can create – a unique combination of letters, numbers, and special characters. Now, the only problem you have to solve is remembering this password (which can be a bit difficult, but it has to be done), and of course, there are methods to make sure you never forget it.

2. Storing your master password in an unsafe manner

If you create a special master password, no one, now or ever, will be able to crack your password. But it's a big no-no to keep your passwords in the bottom of your desk, for the simple reason that if someone finds it, they have access to your entire digital life. It's almost like leaving your laptop unlocked in a coffee shop while you drink. Physical security is incredibly important.



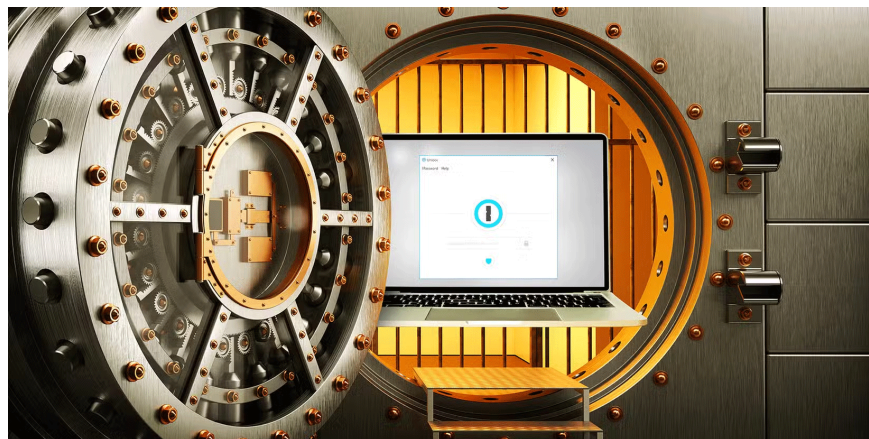
Likewise, storing your master password in a text file on your computer is a bad idea. So where should you store it?

Ideally, you should memorize your master password, as no one can read your mind. If that seems too much trouble, your next option is to write it down on a piece of paper and keep it somewhere safe, preferably a safe in your home. Even better, you can keep it on an encrypted USB flash drive.

Just don't keep it somewhere where someone can easily access it and you'll be fine.

3. Not properly backing up your password repository

A password vault is a place to store all your sensitive information in a password manager. While password managers are generally reliable, you can never be sure that your data will be 100% safe and secure all the time.



Problems beyond your control can happen. Password managers can crash, causing data loss and corruption. Cyberattacks can also happen – criminals can target the company that provides your password manager, destroying the data they have access to. So when setting up your password manager for the first time, keep this in mind, and make sure to back up your password vault regularly.

4. Use the same password manager for personal and work accounts

When you're at work, avoid logging into any personal accounts, as you definitely don't want your personal login information synced to your company computer. Use two separate password managers: One for work and one for personal use at home. Many companies also have privacy policies, especially on work computers. They can request access to anything you've stored on them at any time.

If the company you work for requires access to your computer and you have a password manager, this may not be a good idea, especially if you value your privacy. Not only is there a privacy concern, but there are also security concerns. If your password manager is compromised and contains both personal and work passwords, it could put your company at risk. So it's best to keep your work and personal lives separate.

You finished reading the article "**4 Mistakes to Avoid When Setting Up a Password Manager**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.