

FAQ: USE A STRONG PASSWORD AND A PASSWORD MANAGER

1 Why should I use a password manager?

Your password manager will become your favorite tool as you navigate the digital world. With a password manager, you only need to remember one master password to unlock your secure vault of stored passwords.

Benefits of using a password manager

- **Convenience:** No more struggling to remember dozens of passwords.
- **Enhanced security:** Automatically generate and store long, unique, and complex passwords.
- **Time-saving:** Browser extensions and smartphone apps autofill credentials for quick and secure logins.
- **Safe vaults:** You might be wary of storing all your passwords in one place, but high-quality password managers use encryption and zero-knowledge architecture to keep you secure. Password managers are safer than notebooks, sticky notes, spreadsheets, or reusing passwords because you're trying to remember them all.

2 How often should I change my passwords?

If your passwords are already long, unique, and complex, there's no need to change them unless:

- You suspect unauthorized access to your account.
- You receive notification of a data breach involving your account.

Changing passwords too frequently can lead to weaker habits, such as reusing old passwords or creating overly simple ones. Stick with long, strong passwords and update them only when necessary.

3 What about passkeys?

Passkeys are an exciting new technology that remove the need for passwords. Instead of entering a password, with passkeys you typically log in by having a secure device handy (like a phone) and using biometrics, like a facial scan.