

Password Manager 101

A quick guide to choosing and using a password manager safely

Why Use a Password Manager?

Stores all your passwords securely in one place.

Helps you create strong, unique passwords for every account.

Saves time by auto-filling logins across devices.

Protects you from phishing by only filling passwords on legitimate sites.

Why Use a Password Manager?

Look for strong encryption (AES-256 is standard).

Cross-platform support works on phone, tablet, and desktop.

Browser integration for easy logins.

Family or business sharing options if needed.

Transparent reputation and regular security audits.

Tips for Safe Use

Create a very strong master password — at least 16 characters.

Enable Multi-Factor Authentication (MFA) on your password manager account.

Use cloud sync if you need access everywhere, but make sure it's encrypted end-to-end.

Store your emergency recovery key or backup codes in a safe place (like a fireproof box).

Never share your master password with anyone.

💡 Remember: Your password manager is the key to your digital life. Treat it like the front door to your home — lock it with the strongest key you can make.