Password Managers

1. NordPass

Function: To ensure that you never lose access to sensitive information, all of your passwords, passkeys, credit card information, secure notes, and other data are stored in the cloud.

Use Case: Access your passwords on desktop, mobile, browser, and even when you are offline

Open Source/ Paid: Open Source

Pros	Cons
● Uses advanced XChaCha20 encryption, more future-proof than unbreachable 256-bit AES encryption ● Multi-platform functionality ● Secure Sharing ● Password Recovery ● Ample storage	● Uncustomizable Vault ● Poor Performance ● High price

2. RoboForm

Function: uses symmetric cryptography to safeguard user data while it is on user devices, in transit, and on the server. Every RoboForm data item is contained in a single, AES-256 encrypted file.

Use Case: It provides two-factor authentication (2FA), data breach scanning, and unlimited password storage.

Open Source/ Paid: Closed Source

Pros	Cons
● Password generator is highly useful for creating complex, secure passwords. ● Secure Cloud Storage ● Cross-Platform Synchronization	● Frequent 429 errors (unable to handle high volume of requests) ● Slow Response Times ● Limited Customer Support

3. 1Password

Function: stores a copy of data on each device for quick access and takes advantage of the cloud to make it accessible across all of your devices without compromising security. On the servers, all the data including the name of the vault and website URLs is fully encrypted.

Use Case: It makes it easy to generate, store, and autofill passwords for all your online accounts, on all your devices.

Open Source/ Paid: Paid

Pros	Cons
● Intuitive User Interface ● Cross-Platform accessibility ● Strong Security Measures	● No free version ● No live support

4. Keeper

Function: With zero-knowledge security and encryption software, it offers features like encrypted messaging, privileged access control, password and passkey management, secure remote access, and secrets management.

Use Case: enables users to create and manage strong passwords, securely store files, and autofill credentials across all devices and platforms. It also allows for secure sharing of confidential information between users and teams.

Open Source/ Paid: Open Source

Pros	Cons
● Extensive authentication and security options ● Useful one-time share feature ● Intuitive User Interface	● Feature Add-Ons ● Limited Autofill

5. Dashlane

Function: syncs and stores your passwords for use on computers, tablets, smartphones, and other devices—including ones that you own.

Use Case: Dashlane remembers your complex and unique passwords and enters them into websites when you log in. It can help you create passwords for both personal and professional accounts.

Open Source/ Paid: Paid

Pros	Cons
● Secure Password Vault Encryption ● Intuitive User Interface ● Handy Password History feature ● Includes dark web monitoring for compromised accounts ● No recorded data breaches	● Individual and business plans expensive ● Buggy android app login

6. Bitwarden

Function: generates, stores, and secures important digital assets in an end-to-end encrypted vault.

Use Case: Users can access their data from anywhere, on any device (desktop, laptop, mobile devices) with secure cloud syncing.

Open Source/ Paid: Open Source

Pros	Cons
● Clean security reputation ● Easy to use emergency access feature ● Encrypted file sharing system	● Desktop UI not intuitive ● Autofill functionality can be better ● Does Not have many extra features

7. KeePass

Function: can generate strong random passwords. You can define the possible output characters of the generator (number of characters and type). User input is used for random seeding, including random keystrokes and mouse movements.

Use Case: Usernames, passwords, and other data, such as file attachments and free-form notes, are stored in an encrypted file. Any combination of a master password, a key file, and the details of the active Windows account can be used to protect this file.

Open Source/ Paid: Open Source

Pros	Cons
● KeePass uses industry-standard encryption and local storage, ensuring the company never has access to your information. ● Consistently updated	● Difficult to use ● No live support