Published on *University of Colorado* (https://www.cu.edu)

Consider Using a Password Manager [1]

Most of us maintain dozens—sometimes hundreds—of online accounts. Keeping track of passwords is challenging, and cybercriminals count on people reusing simple passwords across many sites. Reusing passwords allows criminals to log into well protected sites using passwords they stole from poorly protected sites. Security experts recommend strong, unique passwords for every account. A password manager helps you do that without having to memorize dozens of logins.

A password manager is one of the simplest tools you can use to protect sensitive information and reduce the chance that a single stolen password leads to multiple compromised accounts.

What is a password manager?

A password manager is a secure application—available as a mobile app, browser extension, or desktop program—that creates, stores, and auto fills passwords for you. Instead of juggling countless logins, you only need to remember one strong master password (or passphrase).

Password managers simplify your digital life by:

- Generating strong, unique passwords for every account.
- Storing passwords in an encrypted vault that only you can unlock.
- Auto filling credentials on legitimate websites and apps. (If the login page looks right but your password manager will not autofill, treat that as a warning sign and double-check the URL.)
- Syncing passwords securely across devices (if you choose to enable syncing).
- Supporting MFA and other security features for additional protection.
- Saving time with only a few clicks to log in across your devices. No more guessing or relying on frequent resets.
- Storing passkeys, recovery codes, secure notes, and other sensitive items in an encrypted vault.

Misconceptions about password managers

Common Myth	In Reality

If someone breaks into the password manager company, they get all my passwords.	Many reputable password managers use a design where your vault is encrypted before it leaves your device (often called 'zero-knowledge'). That means the provider is not able to read your vault contents. Even if a provider is breached, cybercriminals typically still need your master password (and, ideally, your vault MFA) to unlock your data. Your master password and MFA are critical. Choose a strong passphrase and enable MFA.
A spreadsheet, notebook, or notes app is safer.	Spreadsheets, notebooks, and notes apps are easy to copy, steal, or accidentally share. Password managers are built to protect secrets using encryption and access controls.
My browser can save passwords, so I do not need a password manager.	Browsers can be convenient, but dedicated password managers generally offer stronger security features (such as robust vault encryption, better controls, and vault MFA) and a smoother experience across devices.

Considerations when selecting a password manager

- Security features (strong encryption, MFA support, and regular security updates).
- Ease of use and intuitive design.
- Cross-device compatibility (mobile, desktop, and browser).
- Reputation and independent reviews from reliable sources.
- Cost (free and paid tiers may be available).

Explore these articles to learn more

- Can Your Passwords Withstand Cybercrime? [2]
- MFA: Added Protection from Cybercrime [3]

Published Feb. 6, 2026

Groups audience:
Office of Information Security
Right Sidebar:
Campus May Offer Password Manager
IT Departments Campus Contact

Links
[1] https://www.cu.edu/security/consider-using-password-manager [2] https://www.cu.edu/security/can-your-passwords-withstand-cybercrime [3] https://www.cu.edu/security/multi-factor-authentication-added-protection-cybercrime