Password Management

Managing passwords can be overwhelming. With so many accounts to remember, it's tempting to reuse passwords, write them down, or store them in unprotected files—but doing so puts your personal and institutional data at risk.

Security experts and the Gulf Coast ITS team strongly discourage:

- Reusing the same password across multiple accounts
- Storing passwords in easily accessible or unencrypted files

Instead, we recommend using a password manager.

What Is a Password Manager?

A password manager helps you:

- Securely store all of your passwords in one encrypted "vault"
- Use one master password to unlock access
- Auto-fill login information across websites and apps
- Generate strong, unique passwords for every account

Types of Password Managers

Local Storage

Locally stored password managers save your encrypted vault as a file on your device. The vault is only accessible on the device where it's stored unless you manually place it in a secure location like Microsoft OneDrive.

Pros:

- Full control of your data
- No reliance on third-party servers

Cons:

- Manual syncing required across devices
- If the file is lost or the master password is forgotten, your data is unrecoverable

Cloud-Hosted

Cloud-based password managers store your encrypted vault on secure, third-party servers. They offer convenient access across all your devices and typically include mobile apps, browser extensions, and automatic syncing.

Pros:

- Access from anywhere
- Built-in backups and recovery options
- Frequent security updates and support

Cons:

- Relies on third-party service availability
- Small risk of data exposure (data remains encrypted)

Use Microsoft OneDrive for Secure File Storage

As part of your Gulf Coast Microsoft account, you receive OneDrive cloud storage at no additional cost. While OneDrive is not a password manager, it provides a secure location for storing encrypted vault files (e.g., KeePass databases).

Storing Your Gulf Coast Password

College policy prohibits sharing your Gulf Coast password with others or third parties. Approved password managers do not share your password. Instead, your credentials are encrypted, and only you hold the decryption key.

If your preferred password manager isn't listed below, please contact us at netsystems@gulfcoast.edu.

Recommended Password Managers

KeePass

- Platforms: Windows, macOS, Linux, iOS, Android
- Storage: Local only
- Price: Free
- Ideal for users who prefer not to store data in the cloud. Store vaults in OneDrive or another service, but ensure files are closed before reopening elsewhere.

Bitwarden

- Storage: Local or Cloud
- Price: Free (Premium $10/year)
- Open-source, strong security, cross-platform. Premium features include password health reports and support for families.

LastPass

- Storage: Cloud
- Price: Free (Premium $36/year)

- Supports biometric logins, password audits, and shared vaults. Free version available.

1Password

- Storage: Local or Cloud
- Free Trial: 30 days
- Price: $36/year (Individual)
- Includes Watchtower alerts and Travel Mode. Good mobile and desktop support.

Apple iCloud Keychain

- Platforms: macOS, iOS
- Storage: Cloud
- Price: Free
- Ideal for Apple users. Use strong passcodes and disable iCloud key recovery for Gulf Coast credentials.

Not Recommended

Google Password Manager is not recommended at this time, as Google may have access to your unencrypted credentials.

Using Word or Excel to Store Passwords

While not recommended, if you choose to store passwords in Word or Excel files:

- Store them in your Gulf Coast OneDrive account
- Apply password protection and encryption via File > Info > Protect Document/Workbook > Encrypt with Password
- Use a strong, unique password (not your Gulf Coast password)
- Close the document when not in use

Better alternative: Use a dedicated password manager for better security and convenience.

Tips for Choosing a Strong Master Password

DO:

- Use a long, unique passphrase (e.g., Treehouse!Moon8$Coffee)
- Include uppercase, lowercase, numbers, and special characters
- Choose something easy to type
- Enable 2FA on your password manager

DON'T:

- Use your Gulf Coast password as your master password
- Use common phrases or lyrics
- Forget your master password—recovery may not be possible