Keep Your Documents Secure in Cloud Storage

Instead of trying to find a safe place for paper copies of your important documents you can utilize cloud storage that is safe and accessible from most devices where you have an internet connection. Overall, most cloud storage options have good security enabled. All of the major providers use secure datacenters and security practices to store data. Many of us already have access to cloud storage included in subscriptions already owned, such as through Office 365 or Google Services, or as part of the ecosystem with the devices we own (i.e., Apple products - iCloud).

Common Security Measures in Cloud Storage

In transit data encryption – All services encrypt data when it is communicated from your computer or device to the cloud storage servers.

At rest data encryption – Most services also encrypt data when it is stored on the server as well. Currently the exception is personal Microsoft OneDrive subscriptions. Users would need to upgrade to a business plan to get encryption on their stored data.

Two factor authentication – All major services offer two factor authentication for extra security beyond passwords. Most often the second factor is a text message containing a verification code sent to the device of your choosing.

Zero knowledge authentication – This newer security feature employs a security key for encryption that is unknown to the service provider. This protects from hackers, rogue employees and government intrusion.

Common Cloud Storage Providers Security Comparison

Service	In Transit Encryption	At Rest Encryption	Two Factor Authentication	Zero Knowledge Authentication
Microsoft One-Drive (personal)	Yes	No	Yes	No
Microsoft One-Drive (business)	Yes	Yes	Yes	No
Google G-drive	Yes	Yes	Yes	No
Apple iCloud	Yes	Yes	Yes	No
Dropbox	Yes	Yes	Yes	No
SecureSafe	Yes	Yes	Yes	Yes

You can increase the security of your storage by:

- Using a long password (greater than 12 characters)
- Using a unique password (not used for any other login)
- Turning on two factor authentication (not turned on by default)

Sharing your information in cases of emergency

If you become incapacitated or die suddenly, your family or trusted executor may need access to your information in the cloud. Sharing access before an unfortunate event will make difficult situations more manageable. Password managers like **LastPass** and **Dashlane** offer emergency account access to your stored passwords after going through a validation process. These services will share all your passwords with the designated contact.

Another interesting service is **SecureSafe**. This service combines secure file storage with Zero Knowledge Authentication, a password manager, and emergency access to passwords. Unlike other password managers, **SecureSafe** allows you to pick and choose which passwords to share with your emergency contact.

(DHJJ Financial Advisors does not recommend or endorse a specific storage service. You should determine what your needs are and explore these and other options to find what best suits you.)