
Cloud Storage

Agenda

- Introduction to Cloud Storage
- Cloud Storage Security and Safety
- Overview of Major Cloud Storage Providers
- Cloud Storage Providers - Pros and Cons
- Cloud Storage Providers – Pricing & Security
- Summary & Best Practices
- Questions

Introduction to Cloud Storage

What is it?

Cloud storage is a simple way to save your files and data on the internet instead of just on your computer's hard drive, phone, or a USB stick. All of these local devices can **break, get stolen, or be lost**.

Imagine your important photos, documents, videos, or music aren't trapped inside only one device. Instead, they're safely stored on multiple servers in big data centers somewhere else in the world and you can reach them anytime you have an internet connection.

Introduction to Cloud Storage (cont.)

How does it work?

- You create an account with a cloud service.
  (Google Drive, Dropbox, iCloud, OneDrive, etc.)
- You upload files using their app, website, or it happens automatically.
- The files travel over the internet to the company's secure servers.
- The company makes many copies of your data in different locations. If one server fails your files are **still safe**.
- Whenever you want your file, you open the app or website and there it is!

Cloud Storage Security and Safety

Cloud storage is generally very safe when you use reputable providers and follow good security practices.

In many cases, it is more secure than storing data on a personal hard drive, laptop, or local server. Because major cloud providers invest heavily in security infrastructure.

Cloud Storage Security and Safety (cont.)

Key Security Features

- **Encryption at rest and in transit**

  Your files are scrambled (usually with strong standards like AES-256-bit encryption) both while stored on the provider's servers and while being uploaded/downloaded

- **End-to-end encryption (in some services)**

  The strongest option: your data is encrypted on your device before it ever leaves your computer/phone, and only you hold the decryption key. The provider is unable to access your files.

- **Multi-Factor Authentication (MFA / 2FA)**

  Logging in requires more than just a password. For example, a code from your phone or biometrics. Something you know and something you have.

Cloud Storage Security and Safety (cont.)

Key Security Features

- **Access Controls and Permissions**

  You control who can view, edit, or share files. Shared links often expire or require passwords.

- **Redundancy and Automatic Backups**

  Data is usually stored in multiple locations across different datacenters or regions. Many services also keep version history so you can recover deleted or old files.

- **Advanced Threat Detection**

  Providers use AI, constant monitoring, and security teams to detect unusual activity, malware, ransomware attempts, or hacking in real time.

Cloud Storage Security and Safety (cont.)

It is NOT 100% Risk Free!

- **The biggest risk usually come from the user side**
  - Weak or reused passwords – use a password manager!
  - Phishing attacks
  - Misconfigured sharing settings (e.g. accidentally making a folder public)
  - Not enabling Multi-Factor Authentication (MFA)
  - Choosing a low-quality or unknown provider

Overview of Major Cloud Storage Providers

Microsoft OneDrive

- Deep Windows & Office Integration
  - Built into Windows 10 and 11 with seamless links to Word, Excel, PowerPoint and other products.
- Sync, Backup, and Version History
  - Automatic photo/document backup across devices with moderately easy file restore.
- Security and Collaboration
  - Personal Vault protects sensitive files.

Apple iCloud

❖ Seamless Sync & Backup

- Automatically backs up photos, documents, and app data across all devices. Mac, iPad, & iPhone.

❖ Privacy and Security

- End-to-End Encryption protects sensitive data for trusted, private syncing (if enabled).

❖ Integrated Sharing & Apps

- Works natively with Photos, Mail, and Notes. Also, Family Sharing and photo albums.

*** *No Android support*

Google Drive

❖ Seamless Sync & Backup

- Real-time co-editing in Docs, Sheets, and Slides with comments and version history.

❖ Smart Search & Security

- Powerful Google search and AI suggestions, backed by robust cloud infrastructure.

❖ Real-time Collaboration

- Multiple people can edit Google Docs, Sheets, and Slides simultaneously.

DropBox

- **Ease of Use**
  - Simple interface for quick sharing and organized file access.
- **Syncing & Smart Sync**
  - Reliable cross-device sync plus on-demand files to save space.
- **Integrations & Recovery**
  - Connects with leading apps, with version history and restore.

Cloud Storage Providers - Pros & Cons

Microsoft OneDrive

- Pros
  - Excellent integration with Windows and Microsoft 365 apps
  - Affordable with Office apps bundled
    - Microsoft 365 Family - $129.99 / Year
      - Up to 6 people - 1 TB each of storage and MS Office apps
  - Familiar Interface

- Cons
  - Only 5 GB free
  - Less ideal for non-Microsoft users

Apple iCloud

- Pros
  - Seamless for the Apple ecosystem
    - iPhone/iPad/Mac auto backup, sync
  - Strong privacy focus
  - Family share easy

- Cons
  - Only 5 GB free
  - Mainly for Apple devices. Weaker cross-platform support
  - More expensive per GB at higher tiers

Google Drive

- Pros
  - Most generous free storage (15 GB)
  - Great for collaboration (real-time Docs/Sheets)
  - Integrates deeply with Gmail / Photos / Android
  - Affordable scaling + family sharing
- Cons
  - Privacy concerns
    - Google scans for AI/ads in some cases
  - Storage shared with Gmail / Photos
  - Occasional Sync issues reported

DropBox

- Pros
  - Reliable, fast syncing
  - Excellent file sharing / collaboration
  - Strong version history and recovery
  - Platform-agnostic (works well everywhere)

- Cons
  - Lease free storage (2 GB)
  - More expensive for similar storage amounts.
  - Fewer bundled productivity tools
    - No built-in office suite

Cloud Storage Providers - Pricing & Security

Microsoft OneDrive

Prices

- 5 GB – FREE
- 100 GB - $19.99 / Year
- 1 TB - $99.99 - $129.99 / Year (Family plan)

Security

- Encryption in transit
- Encryption on servers using AES-256. Microsoft manages the keys.

Apple iCloud

- **Prices**
  - 5 GB – FREE
  - 50 GB - $0.99 / Month
  - 200 GB - $2.99 / Month
  - 2 TB - $9.99 / Month
  - 6 TB – $29.99 / Month
  - 12 TB - $59.99 / Month
- **Security**
  - True end-to-end encryption enabled with Advanced Data Encryption (ADP)
  - Otherwise
    - Encryption in transit
    - Encryption on servers using AES-256. Apple manages the keys.

Google Drive

- **Prices**
  - 15 GB – FREE (shared with mail / photos)
  - 100 GB - $1.99 / Month
  - 200 GB - $7.99 / Month
  - 2 TB - $9.99 / Month
- **Security**
  - True end-to-end encryption enabled with paid Client-Side Encryption (CSE)
  - Otherwise
    - Encryption in transit
    - Encryption on servers using AES-256. Google manages the keys.

DropBox

Prices

- 2 GB – FREE (shared with mail / photos)
- 2 TB - $9.99 / Month
- 3 TB - $16.58 / Month
- 5 TB - $15.00 / Month per user for a team of 3 or more
- 15 TB - $24.00 / Month per user for a team of 3 or more

Security

- True end-to-end encryption enabled with paid business plans
- Otherwise
  - Encryption in transit
  - Encryption on servers using AES-256. DropBox manages the keys.

Summary & Best Practices

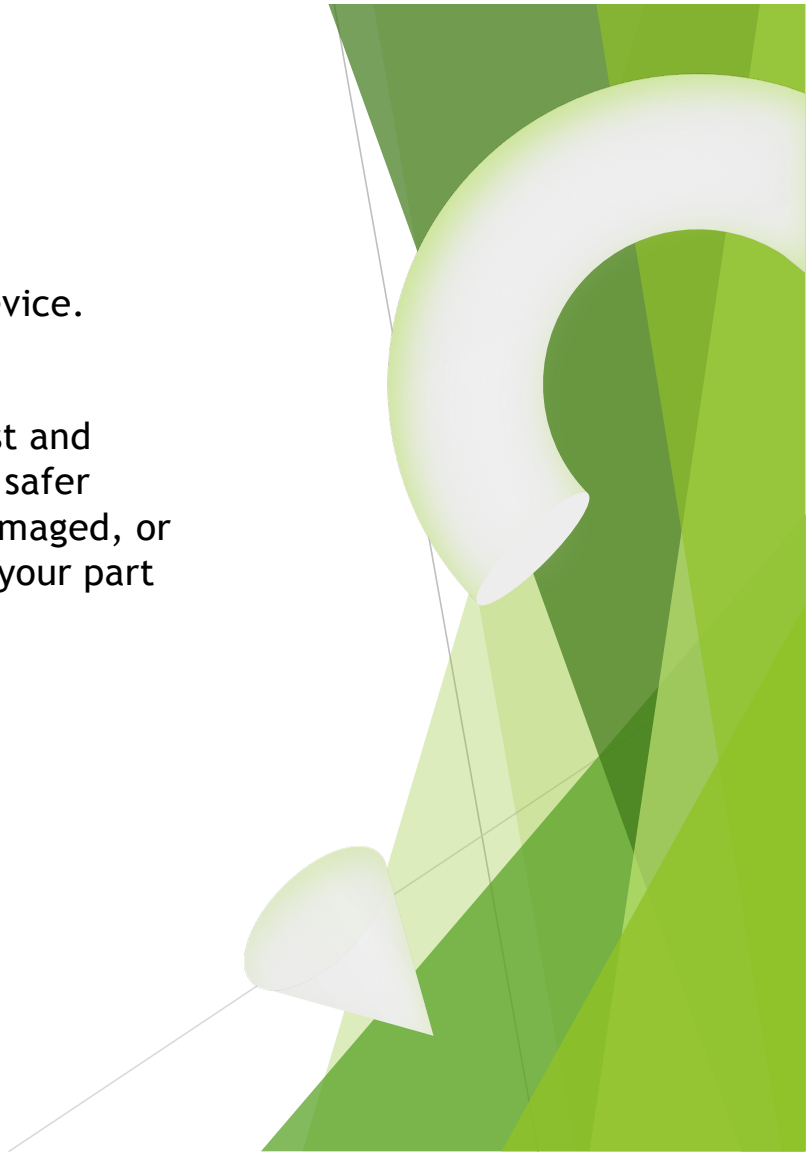
- Maximum free space – Google Drive
- Best for Android – Google Drive
- Best for iPhone/iPad/Mac – Apple iCloud
- Best for Windows/Office Suite – Microsoft OneDrive
- Speedy Sharing – DropBox

Best practices

- Maintain a local version of your cloud storage on your local device.

- In short, when used properly, cloud storage is one of the safest and most convenient ways to store and back up data today—often safer than relying solely on a local hard drive that could be lost, damaged, or poorly secured. The key is choosing good providers and doing your part on account security.

- **AND…**



Cloud Storage Security and Safety (cont.)

It is NOT 100% Risk Free!

- **The biggest risk usually come from the user side**
  - Weak or reused passwords – use a password manager!
  - Phishing attacks
  - Misconfigured sharing settings (e.g. accidentally making a folder public)
  - Not enabling Multi-Factor Authentication (MFA)
  - Choosing a low-quality or unknown provider

Thank you!!!

Questions???