10 tips to keep cloud storage safe and secure

Cloud storage has made it easy to sync files, share them, keep multiple versions of a file, etc. Not only limited to backups, cloud storage has also completely replaced disk storage. physical storage for some users.

You can choose to use a cloud storage service like Google Drive or OneDrive for free, or choose a paid plan for more storage and features.

While cloud storage providers offer good security measures to keep your data safe and secure, what else can you do to ensure that no one gets unauthorized access? go there?

The following article will list some tips that you should follow to protect your files in the cloud.

1. Secure your account with a strong password

To protect your cloud storage account from unauthorized access, make sure you have a strong password.

A strong password is a combination of letters, numbers, and special characters (!, #, $). You can also add a variety of upper and lower case letters to make it complicated.

You can use available online tools to check password strength. In either case, you can also use a password manager to create your own strong passwords.

2. Enable Two-Factor Authentication (2FA)

Once you have a strong password, you should enable two-factor authentication for an extra layer of account protection.

Unless you lose your device, an attacker won't be able to access your cloud storage account. The authentication code is usually generated by the 2FA app or sent to you via email or SMS.

Two-factor authentication using a hardware security key is also an option if you're comfortable with that.

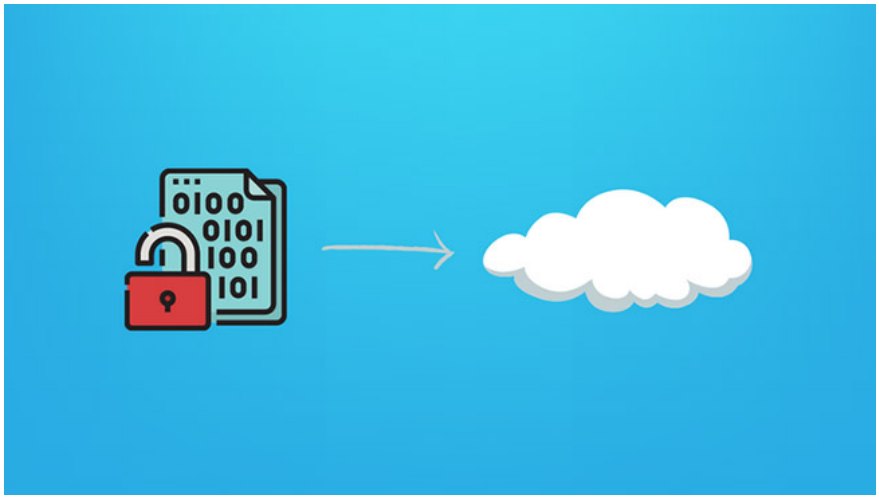
If your online hosting provider doesn't offer 2FA protection, you should consider switching to another service.

3. Avoid storing important information

Cloud storage is a reliable way to have a backup of your data accessible from anywhere.

However, you should not upload sensitive information to keep it safe from any potential attacks. Physical storage will prove to be more effective at keeping your valuable information private.

4. Encrypt data before upload



To prevent access to files, you can choose to encrypt them before uploading to a file hosting service. You can use tools like Cryptomator and Veracrypt to locally encrypt your files and then upload them as needed.

This way, even the cloud storage provider can't access your files without the master password (or decryption key). So even if your data is leaked (worst case scenario), the files are still protected with encryption.

5. Choose an encrypted cloud storage service

Some of the most secure cloud storage services offer encryption by default. If your hosting provider encrypts your files, you may not need to do this locally.

However, in most cases, online hosting services that offer encryption can be very expensive.

This may not be the most cost-effective method, but if you want ease of use, encrypted cloud storage services will help.

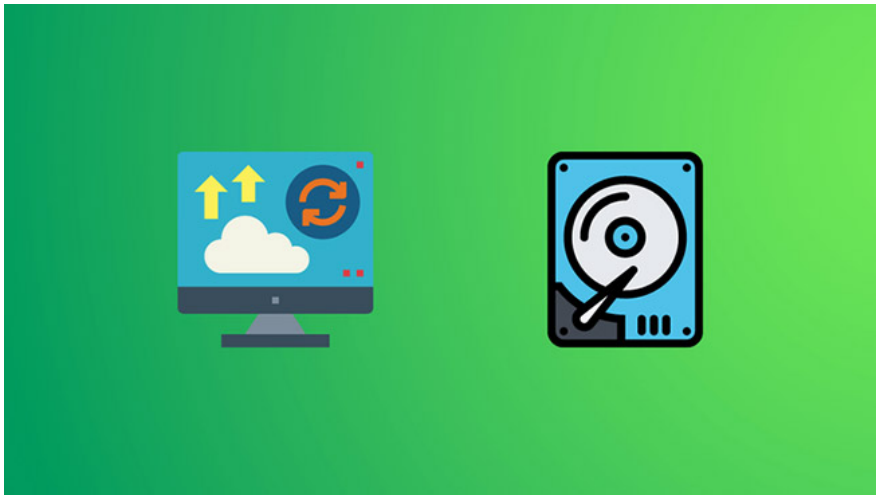
6. Actively manage shared files

When you share a folder or file, it's usually in the form of a link or permission with an email address. If you've shared something via email, it's safe from any future unauthorized access (unless the user you're sharing with has been hacked).

However, if you have shared links for some of your files and folders, you may want to disable it later. If you don't, an attacker can come across the link and easily download files that you don't intend to share with the world.

Every cloud storage service offers a way to manage shared files and links, so you should keep an eye on those files and links.

7. Have a Cloud Data Backup



Many people rely on the cloud as a convenient way to back up data, and often delete those files from storage to free up space.

While it's a smart way to manage your device's storage space, it may not be the safest method.

You should always have a copy of your data in your physical storage in case you lose access to your cloud storage for any reason.

8. Review connected apps

To automate backups or use integration options in other web services, you may have to grant permissions to different applications for your cloud storage account.

To reduce the security risk of such permissions, you should regularly review and revoke your application's access to your file storage service.

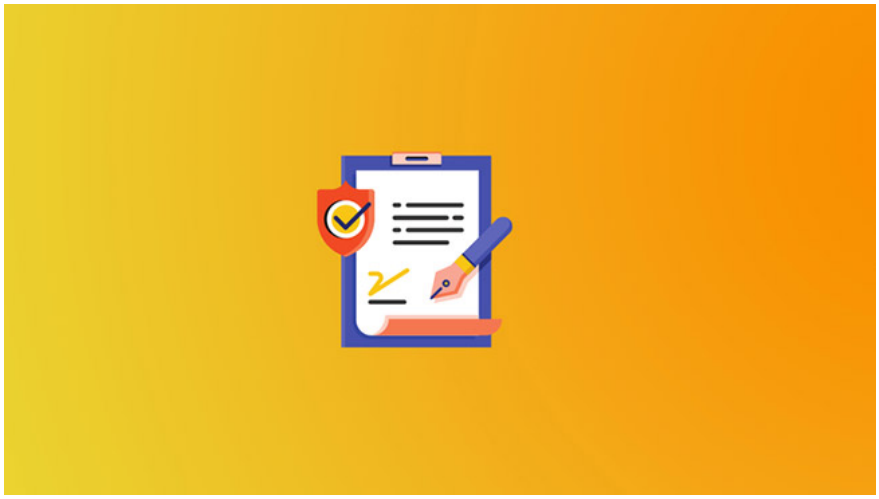
9. Manage device access to cloud storage

The convenience of being able to access files from anywhere can also become a security risk.

If you forget to sign out of a public computer or lose one of your devices, it could be a disaster.

So, to protect your account from unauthorized access, you should manage the devices connected to your account and revoke sessions that you think might be a security risk.

10. Read your cloud storage provider's policy



No matter how popular a cloud storage provider is, you need to review the policies of the service you trust.

It can be a tedious process, but it will give you confidence in how the cloud storage service works, storing the data and information the service collects about you.

Some suggestions to look for in official policies might be:

1. How long do they keep the account active in the event of inactivity?
2. What file types do they allow or restrict?
3. What data do they collect about your files?
4. How long do they keep your data when you request to deactivate your account?
5. What happens to your files when the subscription expires?

You finished reading the article "**10 tips to keep cloud storage safe and secure**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com