



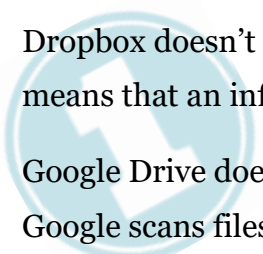
5 Safety Tips for Your Online File Storage

Who doesn't appreciate the convenience of storing your important files online? Popular cloud storage services like Dropbox and Google Drive make it easy to access and share documents and files with anyone anywhere anytime. But with convenience comes risk.

Knowing how to protect your valuable files as well as the people you're sharing your files with should be part of your company's security plan.

Here are 5 practical tips to help you safeguard your online file storage.

Virus Scanning



Dropbox doesn't scan your files for viruses when you upload or download them. This means that an infected file can live indefinitely in Dropbox.

Google Drive does some scanning but not enough to provide the protection you need. Google scans files smaller than 100mb before they are downloaded. Like Dropbox, Google Drive doesn't scan files when they are uploaded.

If a file is infected, Google will warn your users when they attempt to download the file. However, your user can ignore the warning and continue the download. You know what this means.

Why is this important?

One of the benefits of online file storage is that changes are automatically synced to all devices associated with the account. One infected file quickly spreads to all your company's devices when they sync.



5 Safety Tips for Your Online File Storage

The most effective defense is [proactive antivirus](#) running on every desktop, laptop, and server. Relying on [legacy reactive antivirus](#) solutions like Windows Defender is not adequate protection today.

Sharing Links

A Dropbox file can be shared with anyone who has a link to it. This link can be freely passed along through email, text, social media, whatever tool is handy. By default, the shared file is view only, but anyone can download it.

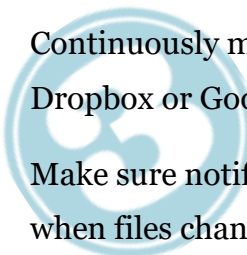
Protecting who has access to your valuable files and what they can do with them are obvious. One way to wrap more security around file sharing is by enforcing link passwords. The Dropbox Business plans allow for both passwords and password expiration.

Adopt a need-to-access approach. Create user groups in Dropbox Business Standard and Business Advanced versions to manage who has file access and what they can do.



5 Safety Tips for Your Online File Storage

Monitor Activity

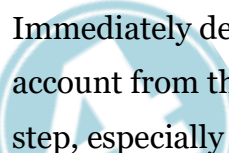


Continuously monitoring your company's online file activities is the role of your Dropbox or Google Drive admin.

Make sure notifications are enabled. It is important your admin receives a notification when files change or are accessed. This allows for immediate action when an unexpected or questionable event occurs.

Continuous monitoring is especially important when employees can access online storage using [public wi-fi](#). The potential for unauthorized access to your valuable data is high.

Terminated Employees



Immediately delete a terminated employee from the online account and wipe the account from their device. It seems obvious enough, and yet it's easy to overlook this step, especially when employees use their own devices to access company files.

This includes their phones and other mobile devices too.

5 Safety Tips for Your Online File Storage

Be Careful What You Upload

Google Drive allows users to upload executables (such as .exe, .sh) and compressed files (with extensions like .zip, .gz). While these are standard file types for installing and executing the software we use every day, they can also be potentially dangerous. These file types run when clicked so an unsuspecting user can easily launch a piece of [malware](#).

We strongly recommend that you do not allow users to upload or download these file types in Google Drive.



If you would like to learn more about online storage and security, we're ready to answer your questions.

Quest Technology Group

315 E. Robinson Street, Suite 525

Orlando, FL 32806

Email: learning@quest-technology-group.com

Call: 407.843.6603

Chat: quest-technology-group.com