Dr.Backup™
online backup service

Microsoft OneDrive: A Safety Net With Too Many Holes

Microsoft OneDrive is a file transfer program that automates the process of storing digital documents online (in the "cloud") so that they can be shared across multiple devices that have an internet connection. OneDrive is now included with the latest version of Microsoft Windows 10.

If you own/operate a business, your livelihood depends heavily on the digital information you maintain about your products, services, employees and customers. Don't be lulled into thinking that the use of OneDrive on your PC alleviates the need for you to follow proper data protection and backup processes. Relying exclusively on OneDrive to secure your digital assets is a huge mistake that might cost you your business!

Here are some key facts you need to know about OneDrive:

1. Microsoft clearly states in the OneDrive service terms and conditions that they are NOT responsible for your data. They explicitly tell you to **use third party tools and services to protect and ensure data availability**. Furthermore, they absolve themselves of virtually any legal liability associated with losses you may encounter should their OneDrive service fail. This is a classic "buyer beware" warning signal!

2. Out-of-the-box, OneDrive operates in "Files On-Demand" mode. This means that files created/edited in the OneDrive folder on your device will be automatically replicated to the cloud – **after which they are DELETED from your local system** (thereby saving local disk space.) The reference you see remaining in Windows file explorer is only a shortcut to the cloud. Without continuous access to your online account, you cannot read or update your data. Warning: Failure to update your credit card information could result in deletion of all your data!

3. Most OneDrive accounts use your email address and password as credentials for authentication**. If for any reason your password is compromised, your data is vulnerable.** These days, hackers can go to the "Dark Web" and gain access to millions of compromised email passwords. See "I've Been Pawned" for more information.

4. A backup is a complete copy of a digital file at a specific date and time. A true backup service will maintain an immutable version of each **file backed up in a secure format that is read-only.** OneDrive does not operate in this manner. This means that financial documents stored online in last year's folders can be altered -- making your small business more susceptible to embezzlement and fraud.

5. If you lose data or save a corrupted version of a file in OneDrive – and don't discover it for 30 days – your ability to recover **your data is severely limited or non-existent**. Only a true backup solution will offer you full file versioning over a configurable time period AND the ability to quickly recover prior versions of lost files that have been previously deleted.

6. The standard version of **OneDrive that ships with Windows 10 is NOT HIPAA compliant.** If your business services the healthcare industry, you must purchase Office 365 or the business-class version of the OneDrive software AND request that Microsoft execute a Business Associate Agreement (BAA) with you to help ensure compliance.

7. There are significant limitations to the operation of OneDrive. Any file which you would like stored on the cloud MUST be placed inside of the OneDrive file folder – or a subfolder under it. This means that **SQL databases, email stores, program data and vertical application data** which cannot be relocated into the OneDrive folder are only stored on the local machine.

8. **There is no easy way to audit the efficacy of the OneDrive** offsite data transfer. It is exceedingly difficult for you to verify when the last copy of local data was synchronized with the cloud – nor if there were any copy or file protection errors encountered. At this time, there is no automatic reporting on the contents of OneDrive making it challenging to obtain a list of all files held on the service, their size, full file path specification, etc.

9. Shared folders secured by only a common password, are highly susceptible to virus/ransomware infection. Just a **single rogue file stored in a OneDrive folder can facilitate the spread of a virus** across an entire organization. For example, how likely is it in your environment that a virus-container file named "Payroll Salary Report.doc" would be casually opened?

The United States Computer Emergency Readiness Team (US-CERT) recommendations are the gold standard for small business backups. The US-CERT "Backup 3-2-1 Rule" states that you should always have three (3) copies of all critical data files, the original plus two (2) backups residing on different sets of backup media, and one (1) of the backups being stored offline.

For more information, see our online resource at:
https://drbackup.net/resources/data-backup-options-the-3-2-1-rule/