Science Translations
Established 1990
PC410.COM™
PC Updater News

Immutable Cloud Backups

Immutable: Adjective. Unchanging over time or unable to be changed.

That's what we want in a data backup. An immutable backup is created and then stored for a specific amount of time, and it cannot be deleted, edited, encrypted, or generally messed with until that clock has run out. Ransomware can't damage it. Employee error can't wipe it out. A employee on the way out, or a contractor with network access, can't hurt it. So immutable backups are the best defense against ransomware, malicious encryption, lightning strikes, fire, or employee error. The only actual way to get rid of it is to close the cloud backup account that holds it.

The goal of immutable backups is to have backups that are impossible to mess with. Not impossible to read or decrypt, because they're always readable. All that's blocked is the ability of anyone to write over them or delete them. But there are limits; Immutable backups that run on a schedule are cloud-based, always. For offline periodic backups, like monthly, the only immutable option is to backup to an external drive and then disconnect it from power and lock it up offsite. That's great if you have the discipline to do it, but I've only seen one office do it successfully, ever. So daily or continuous 'in real time' immutable backups are always cloud backups.

So a cloud backup service provides immutable backups by setting limits on the software running at the cloud service that determines that the only way to delete a backup is to let it expire. Usually, the expiration is set as something like "keep every version of every file until it is removed from my computer, plus some number of months." Could be one month, or a year, depending on the backup cloud service, and some services have more than one option. For BackBlaze, the default is one month, and there's a one year option.

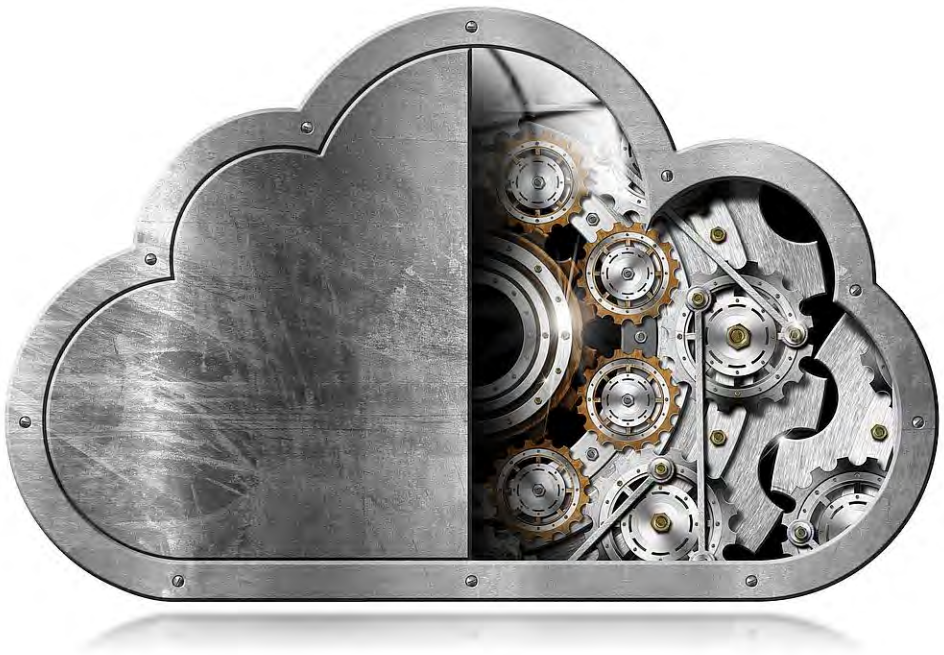
Call if you need help selecting a cloud backup, or changing the options for how long to keep your backups. As a rough guideline, when I get a call for "We messed up the big spreadsheet and need an older version," we usually end up using a restored copy that's either three days old, or two months old. It's usually not the last backup, from the previous day.

Sync is Not a Backup

These cloud services are for online storage, and have file sharing features, but they are not backup, and are not immutable.These are syncing services. Don't use these for backups, because ransomware can see the online files and encrypt them:

- DropBox
- Google One (also known as Google Drive, or Google Backup & Sync)
- iCloud (Apple)
- OneDrive (Microsoft)
- Others–there are hundreds of syncing drive services.

Too Many Clouds

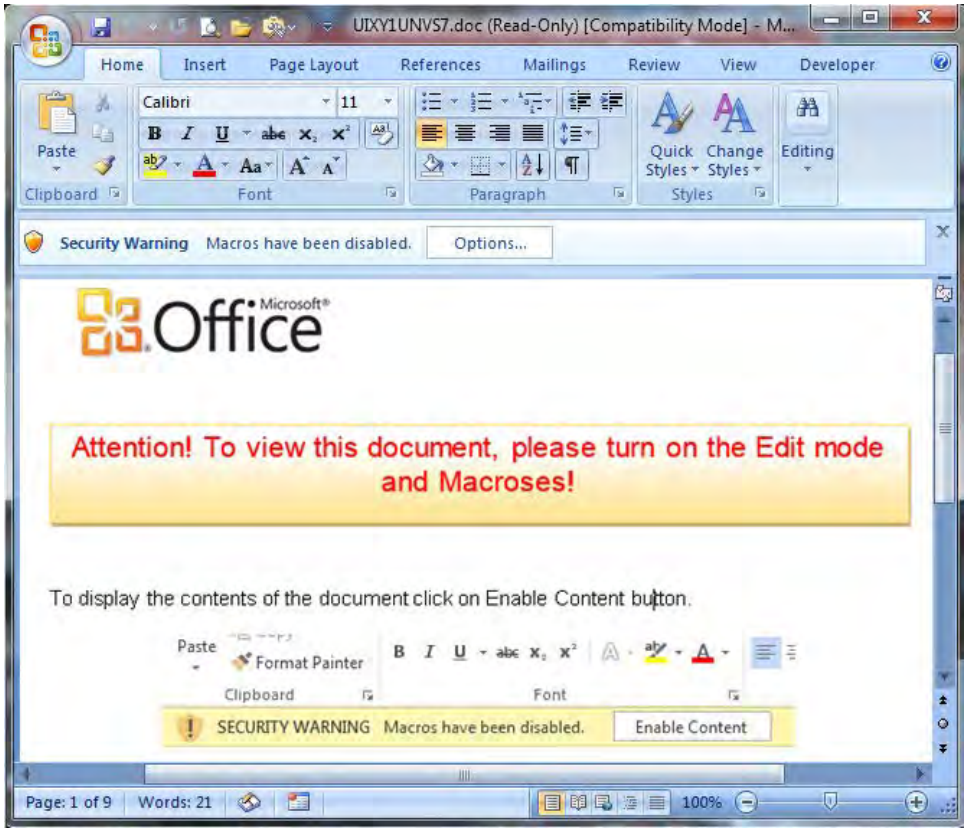


Most Windows computers I see are running multiple cloud sharing services in the background. If you're not actively using these products, they should not be there, and should be turned off or uninstalled. Each of these products leaves an icon in the system tray, next to the clock, and can be controlled from there, or uninstalled from Control Panel.

- OneDrive (Microsoft) installs itself by default in Windows 10 & 11, and reinstalls itself during feature updates, and can be turned off from the options menu after right-clicking the cloud icon in the system tray. Keep it if you're using Microsoft 365 (basically Office on the monthly payment plan) and storing documents in it to share between multiple computers and phones.
- iCloud has similar features, and I don't recommend it on Windows at all. Some users have it for syncing Outlook with iPhones for contacts and reminders, but there are far more reliable ways to do that by using the free Outlook app on the iPhone instead, which does not require ANY Apple software on a Windows computer. iCloud also syncs aggressively, and I've seen it copy every picture on a phone back to a Windows computer and fill the drive; check your options.
- DropBox is also a sync program. If you are only using it for looking at shared photos, that can be done from the DropBox.com web site, and installed software is not required at all.

Overall, one sharing program from ONLY a service provider you absolutely trust is quite enough, and all others should be turned off or removed.

Coming in April: Office is Breaking Macros



Macros in Microsoft Office have been a problem for decades. Allowing a word processing program to include a macro that runs as soon as the document loads is as powerful as it is stupid. There are better tools for programing; there's not a lot of use for autoplay macros. They're not even possible, never have been, in WordPerfect or LibreOffice. (I would know; my Graphcat Photo Album Builder for WordPerfect is basically a 23-page macro.)

So for a long time now, Office has had an option to ask permission before running an autoplay macro in a document, and that option is on by default. No one I'm aware of has used the autoplay feature for a good reason. Bad reasons, yes, constantly. Fake invoices arrive daily, and these include nothing more than a graphic, example above, that says to enable a macro and then a download link to ransomware, which then can install with all the rights that were used to run Office. The protections against these things are employee education to never enable macros, setting all computer users to have only non-admin accounts that cannot install software, and a good endpoint protection (antivirus) program. But these fake invoices are updated hourly, so software can't keep up, and the non-admin accounts and employee training are very important.

Finally, starting in April, Microsoft will change the settings in Outlook to disable macros in documents downloaded from the internet, by default, without a prompt to enable them. A sufficiently-determined user might still be able to run a macro-enabled document by changing permission settings in Word or Excel, but it will generally be beyond the skill level of most users that are inclined to believe fake emails from strange email addresses.

The changes will apply only to current versions of Office, in the Word, Excel, Access, PowerPoint, and Visio programs, in Office versions 2013 and newer. The next-older version of Office, from 2010, is no longer receiving security patches, since October of 2020. Office 2013 will continue to receive security patches to April 2023.

No action should be needed for this change to happen, other than allowing Office updates to install during April. There is more information here, which starts with a good overview, and becomes very technical later: https://docs.microsoft.com/en-us/deployoffice/security/internet-macros-blocked

For computer help, call 410-871-2877
Missed a newsletter? Back Issues