Can a Cyberattack Damage Your Backup, Too?

Backing up your computer is one of the most important things you can do to protect your files. If malware, a hacker, a software failure, or even your own mistake damages or deletes important information, a good backup can help you restore the computer and get back to work.

But there's a catch that is sometimes overlooked: **What happens if your backup drive is connected to your Mac when the damage occurs?** A backup connected to the computer isn't necessarily beyond the reach of whatever is affecting the computer itself.

A Connected Backup Is Still Connected

An external hard drive attached to your Mac and mounted by macOS is accessible to the computer. That's what allows backup software to save your files automatically. That accessibility, however, can also create a vulnerability.

Malicious software operating with sufficient permissions may be able to alter, encrypt, delete, or corrupt files on storage devices accessible from the computer. A particularly serious attack might therefore damage not only the files on the Mac but also files on an attached external drive.

The danger isn't limited to ransomware. Other malware can delete or corrupt information, and an attacker who gains sufficient control of a computer may deliberately try to damage files or backups. Even ordinary problems can spread to backups. If a file becomes corrupted and the damage isn't noticed immediately, later backups may contain the corrupted version. That's one reason maintaining older versions of files is so valuable.

Time Machine Gives Mac Users an Advantage

Mac users already have an excellent backup system built into macOS: Time Machine. Rather than simply maintaining a single duplicate of your current files, Time Machine preserves historical versions as space permits. That history can be extremely useful. Suppose you discover that an important document was damaged several days ago. Instead of restoring today's damaged copy, you may be able to go back and retrieve an earlier, undamaged version.

Time Machine can also maintain local snapshots under appropriate circumstances, providing another possible route to earlier versions of your files. Version history is an important safeguard, but it shouldn't be confused with complete isolation. If an external backup drive is connected and accessible to the Mac, a sufficiently powerful attack could potentially affect it.

Encryption Adds Another Kind of Protection

Encrypting your backup drive is an excellent security measure, particularly if it contains personal information, financial records, correspondence, photographs, or other private material. If someone steals the drive, encryption prevents that person from simply connecting it to another computer and reading your files without the password.

For a locally connected Time Machine backup drive, Apple provides a relatively simple way to turn on encryption for an existing backup. In Finder, locate the backup drive in the sidebar or on the desktop. **Control-click the drive and choose Encrypt.** Enter and verify an encryption password, add a password hint if desired, and click **Encrypt Disk**. The Mac then encrypts the existing drive. Depending on how much information is stored on it, the process can take some time.

If you are setting up a new Time Machine drive instead, go to **Apple menu > System Settings > General > Time Machine**. Choose **Add Backup Disk**, select the external drive, and click **Set Up Disk**. When the setup options appear, turn on **Encrypt Backup** and create a password. Apple recommends APFS or APFS Encrypted for modern Time Machine backup disks.

There is another method using Disk Utility, but be careful with it. Formatting a drive as **APFS (Encrypted)** in Disk Utility requires erasing the drive first. That is appropriate when preparing a new or empty drive, but not something to do casually with a drive already containing the only copy of your Time Machine history.

Most important of all, **don't lose the encryption password.** You will need it to unlock the backup and restore files. Keep a secure record of it somewhere other than on the backup drive itself.

Encryption Doesn't Make a Connected Drive Invulnerable

Encryption solves a different problem from an offline backup. Once you've unlocked an encrypted drive and macOS has mounted it, the computer can use it, and software running with sufficient privileges may potentially be able to alter its contents as well.

Think of encryption as protecting the **confidentiality** of your information, while a disconnected backup protects something different: the **survival** of your information. Both are important.

The Simplest Defense: Disconnect One Backup

There is a remarkably effective defense against an attack spreading from your Mac to a backup drive: **disconnect the drive.** A backup drive sitting unplugged on a shelf cannot be reached electronically by malware or by someone remotely controlling your Mac. This is commonly described as an **offline or air-gapped backup**.

There is an obvious drawback, of course. An unplugged drive can't perform automatic backups. That's why keeping a second backup can provide considerably stronger protection than relying on a single external drive.

Consider Rotating Two Backup Drives

A practical arrangement for a home computer is to use one external drive for regular automatic Time Machine backups and periodically make another backup to a second external drive. When the second backup is finished, properly eject the drive, disconnect it, and put it somewhere safe. Periodically reconnect it, allow the backup to update, and then disconnect it again.

Now suppose something seriously damages the Mac and its currently connected backup. You still have another copy that was physically beyond the reach of the affected computer. It might not contain everything you've created since the last time you updated it, but losing a week's work is considerably better than losing years of photographs, financial records, correspondence, manuscripts, and other irreplaceable files.

Don't Forget Physical Disasters

Cyberattacks aren't the only reason to keep more than one backup. A computer and an external drive sitting beside it can both be lost to fire, theft, electrical damage, or another physical disaster. For especially important information, consider keeping another copy in reputable cloud storage or at a different physical location.

This leads to a familiar backup principle known as the **3-2-1 rule**: keep three copies of important information, use more than one type or location of storage, and keep at least one copy separate from the computer. You don't need a corporate computer department to follow the basic idea. A Mac, a regularly updated Time Machine drive, and another backup kept offline can provide a strong foundation. Cloud storage can add still another layer of protection.

Backups Protect Against More Than Hackers

It's easy to think of backups primarily as protection against a failed hard drive, but today they serve a much broader purpose. A backup may save you after malware corrupts files, a hacker gains access to the computer, software goes haywire, an important document is accidentally overwritten, or you simply make a mistake and delete something you wanted to keep.

The important lesson is that **a backup shouldn't share every vulnerability of the computer it is protecting.** Keep making automatic backups. Keep macOS and your applications updated. Use the security protections built into your Mac. Encrypt backup drives that contain private information. And if your files would be difficult or impossible to replace, periodically make another backup and disconnect it.

Sometimes one of the strongest pieces of cybersecurity technology you can own is surprisingly simple: **an unplugged backup drive.**