TECH BRIEF

Seven ways to back up
your data

ESET ENJOY SAFER TECHNOLOGY®

SEVEN WAYS TO BACK UP YOUR DATA

By Alan Martin, ESET Staff

Are you doing regular backups of your data? You should be.

Not only does it make sense in case your laptop is stolen, or your hard disk fails, but it also means that you have more options for recovery should your computer become infected with ransomware. This is a particularly nasty strain of malware that encrypts your files and threatens to delete them if you don't pay a ransom within a certain time period.

ESET doesn't recommend giving in to ransomware demands for many reasons both ethical and practical (not least because you mark yourself as a possible target for future attacks), but if your files are all safely backed up, you won't even feel tempted to negotiate with them in the first place.

There are plenty of options available for people looking to back up their data, all with their own pros and cons. Here are some of your options, but remember: it's best to have more than one backup method to be safe.

1. USB stick

Small, cheap and convenient, USB sticks are everywhere, and their portability means that they're easy to store safely, but also pretty easy to lose. There are questions about the number of read/write cycles they can take, so they should be supplemented with other backup methods.

Pros:
+ Extremely portable
+ Very cheap
+ Can easily transfer data to other sources

Cons:
– Portability means they're small and easy to lose
– Questions over read/write cycle longevity

2. External hard drive

External hard drives are just what they sound like—hard drives that live outside your computer, meaning they can be plugged in to other sources. If using them for backup, its best not to use them as an "extra everyday hard drive"—instead, designate one particular drive solely for backup and always disconnect it when the backup has finished. This is particularly true in the case of ransomware. For example, if you back up your computer to an external hard drive, but leave that drive connected when you are not doing backup, some ransomware will try to encrypt those backup files as well.

Pros:
+ Relatively cheap
+ Plenty of storage space for larger files

Cons:
– Potentially open to problems which lost files in the first place (a power surge or malware)

3. Time machine

For the Mac® users out there, Time Machine is an option that backs up to external hard drives automatically. Apple sells its own brand of dedicated wireless Time Capsules, but you can use any hard disk for it. Using this method, you'll automatically keep backups hourly for the last 24 hours, daily for the last month and then weekly backups until the machine is full.

Pros:
+ Automated, meaning you don't have to remember to stay up to date
+ Frequency of backups means you should never be too out of date
+ Backs up whole drive, not just the key files

Cons:
– Dedicated wireless machine is expensive
– Mac only

4. Network attached storage

It used to be that only businesses tended to back up their files to network attached storage, but with more and more homes having multiple computers, the idea is appealing, especially for those looking to save files from more than one source. With prices coming down, a dedicated wireless storage solution is a convenient option which requires less thought.

Pros:
+ Automatic backups mean you don't risk forgetting
+ Wireless solutions also work with phones and tablets

Cons:
– Can be expensive
– Can be awkward to set up and maintain

5. Backup and recovery solutions

Backup and recovery solutions such as StorageCraft® ShadowProtect® reliably back up everything from systems to data, enabling a fast recovery in the event of natural disaster, hacking attack or computer failure. StorageCraft is a data-, applications- and systems-recovery solution for both physical and virtual Windows® IT environments. It creates sector-level backup images of a disk drive, including not just data but also the operating system, applications, services and configuration settings. Suitable for businesses of any size, backup and recovery systems may also be implemented by home users who want comprehensive backup of all their data and systems or want to ensure business continuity for a small or home office.

Pros:
+ Backups can be scheduled to occur automatically
+ Backup includes entire disk drive: systems, applications, services, configurations, settings, and data
+ Allows you to quickly and easily boot any backup image as a virtual machine

Cons:
- Can be expensive

6. Cloud storage

While network attached storage is essentially your own cloud server, there are plenty of third party cloud storage options around: free, paid, or free with paid extras. iCloud, Dropbox, Google Drive and OneDrive are big names, but others are available.

Pros:
+ Can be done automatically
+ A certain amount of space is usually free
+ Device agnostic

Cons:
– Requires an Internet connection to work
– You can't account for their security breaches
– Companies aren't obliged to keep these services around forever

7. Printing

At a first glance, this might sound a facetious inclusion. But while considerably less technically advanced, printing offers you a hard copy of your most important documents that will survive power outages, and are easy to store and access even if your computer is out of action for a few days. Of course it's hard to keep documents up to date this way, and it won't work for video or audio files, but for that novel you'd be devastated to lose, it's certainly worth considering.

Pros:
+ A backup that won't be affected by hardware outages or tech headaches
+ Impossible for hackers to access

Cons:
– Impossible for certain file types
– Awkward to manage
– Less practical for longer documents
– Not great for the environment

However you choose to backup your data, make sure that you do it. Often people don't think about what would happen if their valuable files were to be lost, until it's too late. So add back up to your list of regular tasks to make sure your files are all safe and accounted for.