Safe Storage Options

Last Modified on 10/18/2022 3:49 pm EDT

This article reviews ways to protect your external storage options (e.g. usb drives, external hard drives).

Table of Contents

External & Portable Storage Media

Physical storage media that connects to a device using a USB port or other connectivity option -- such as external hard drives or thumb/flash drives -- are a convenient way to back up, move and store data. However, if you lose your media and it is accessed by the wrong person, it presents a security concern.

^Top

Encryption

While we primarily recommend using cloud storage to store and protect your data, there may be instances where external media such as a USB flash drive is needed. In these instances, we recommend encrypting your flash drive so that if you misplace it, no one will have access to the information it contains.

Note: Many manufacturers offer hardware-encrypted flash drives. While more expensive than regular flash drives, these are a good option if you do not want to encrypt the drive yourself or do not have access to an OS that has software encryption.

Windows

If you have Windows 10/11 Professional, you can use **BitLocker** to encrypt your flash drive (or external hard drive). BitLocker allows you to choose whether to encrypt the entire drive (good for flash drives/external drives that are already in use) or used disk space (good for new flash drives/external drives that do not have any data on them). Media encrypted with BitLocker is readable on any Windows 10/11 computer regardless of whether the OS is the Home or Professional version.

Note: When encrypting any media with BitLocker, it's a good idea to save/back up the recovery key to your Microsoft account in case you forget the password.

Mac

FileVault is Apple's encryption solution and offers a similar experience to Microsoft's BitLocker, however you cannot encrypt a flash drive (or external hard drive) that already has data on it as FileVault will require it **to be**

completely erased before it can be encrypted. FileVault also does **not** provide a recovery key for encrypted external media, so make sure to securely store your password somewhere such as LastPass. Media encrypted with FileVault is readable on any Mac running Mojave (MacOS 10.14) or higher.

Note: If you encrypt an external device using FileVault, you will **not** be able to connect it to an AirPort base station for use with Time Machine. If enabling FileVault for your Startup Disk, it's a good idea to save your recovery key to your iCloud account in case you ever forget your password.

^Top

Additional Considerations for Storage Media

1. Always keep your storage media in a secure place.
2. Physical storage media can be easy to damage or lose. Make sure you have backup copies of everything.
3. Storage media lost on the Wharton campus are taken to the lost and found and destroyed at the end of the year. Label your storage drive with your name and contact information in case it's found.
4. If using unencrypted media, you can follow these instructions from ISC to securely erase it.

If you are traveling with physical storage media, please read this guidance from ISC.

Questions?

For questions or advice on portable storage media, contact your Wharton Computing representative.