

Encrypt the hard drive to protect your data

Encrypting the hard drive gives your data store an extra layer of protection in addition to setting up the system password.

Encrypting the hard drive gives your data store an extra layer of protection in addition to setting up the system password.

Hard drives and USB flash drives are personal data stores. They are also among the most common sources of data leakage. If you lose a flash drive, an external hard drive or a laptop containing sensitive personal information, you will be in danger. Fortunately, hard drive encryption can give your data an extra layer of protection in addition to setting the system password. Encryption will hide your drive data, making people who don't know your encryption password almost impossible to access the file.

Ultimate and Business versions of Windows 7 and Windows Vista come with BitLocker - a tool that allows you to encrypt the entire hard drive. If you don't have an Ultimate or Business version, another alternative is to use TrueCrypt - the free open source tool that can encrypt an entire disk, disk part or external drive. For its part, Mac OS X has FileVault - Home directory encryption tool. Lion - the next Mac OS X version is coming soon - will be able to encrypt the entire hard drive.



LaCie's Rugged Safe hard drive has a fingerprint reader that can be used to securely protect data.

Another option is to purchase external hard drives, flash drives equipped with encryption tools. Some of these drives have an integrated fingerprint reader that increases security.

You finished reading the article "**Encrypt the hard drive to protect your data**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
