

Published based on [Hard Drive Encryption Software](#)

Hard Drive Encryption Software

If you don't want your secret files on your disk to be publicly readable to anyone who gets a grip of your disk. A technique named disk encryption will be a good solution for you. Disk encryption is an encryption method which encrypts every bits of data that is stored on a disk, hard drive or removable media. There are many software packages which will do the disk encryption for you. The software encrypts all the data that is stored on a hard drive, or any other removable medium which can store data. When the user wants to access a file the software automatically decrypts the files the user wants to access only an passwords needs to be provided at the beginning of the session. The password is used to decrypt the files so no one else can decrypt them.

This kind of software is used so that a hacker who broke through your firewalls and other security programs, still can't access your private files. Because he doesn't has the password the software uses to decrypt the files. Encryption software also prevents trojans, keyloggers and other viruses to read your confidential files.

It allows you to protect the privacy of sensitive files, folders, or messages, by encrypting them with up to four strong encryption algorithms. Once the information has been encrypted, it can be stored on insecure media or transmitted on an insecure network -like the Internet- and still remain secret. Later, the information can be decrypted into its original form. Simple, reliable, and versatile, disk encryption program allows you to create multiple encrypted disks that contain confidential information. Your files and documents are hidden from unwelcome eyes, while Disk Firewall ensures that undetected Trojans, viruses or spyware will not get access to your protected data.

Disk Firewall protects your data from illegal copying, viruses and spyware by maintaining a white-list of applications which are allowed to access the encrypted disk. The disk firewall has a self-learning mode feature that keeps track of the user actions and composes the white-list of applications automatically.

AES 256-bit encryption is the most secure encryption algorithm applied today, chosen as a state standard due to its strength and efficiency.

There are various free / open source software packages and there are paid / commercial software packages which will do the encryption for you.

Free / OSS disk encryption software packages:

- TrueCrypt (<http://www.truecrypt.org/>)
- cryptoloop (WIKI)
- DiskCryptor (<http://en.wikipedia.org/wiki/DiskCryptor>)
- FreeOTFE (<http://www.freeotfe.org/>)
- FlexCrypt (free version)
- AxCrypt (<http://www.axantum.com/AxCrypt>)
- CCrypt (<http://sourceforge.net/projects/ccrypt>)

For detailed description and review visit the following page: Free / open source disk encryption software packages.

Commercial disk encryption software packages:

- Dekart Private Disk (<http://www.private-disk.net/>)
- Rohos Disk Encryption [30 day free trial] (<http://www.rohos.com/products/rohos-disk-encryption/>)
- SafeBit disk encryption [30 day free trial] (<http://www.safebit.net/>)
- PGP WholeDisk encryption (http://eu.store.pgp.com/whole_disk_encryption.html)
- Guardianedge Hard Disk encryption [demo available on contact] (<http://www.guardianedge.com/products/guardianedge-hard-disk-encryption.php>)

Source:[hard drive encryption](#)

Grab helpful advice about [penis enlargement](#) - give a look to hyperlinked page.

You can also find this article published on [Hard Drive Encryption Software](#)