# How to protect sensitive files

Many human rights activists have sensitive information that could have serious consequences if seen by the wrong people. The [Managing Information lesson](umbrella://lesson/managing-information) can help you determine your threat model. Following the steps laid out in the Home/Office section and the [Malware](umbrella://lesson/malware) lesson will help you to protect your computer physically and digitally. However there may be situations where these precautions fail or you need to show your computer to someone whom you don?t want to see the files. This is why you should also protect the files themselves. You can do this by encrypting them so that only you can read them.

Encryption is a way to enhance the security of a message or file by scrambling the contents so that it can only be read by someone who has the right encryption key to unscramble it.Many activists use TrueCrypt, but serious vulnerabilities have recently been found in it. [VeraCrypt](https://veracrypt.codeplex.com/wikipage?title=Downloads) is a good, free, open-source, alternative that we recommend instead. Much like a safe, VeraCrypt creates an encrypted container on your computer or hard drive, that you can put as many files as you like into.

We will shortly be creating a tool guide for VeraCrypt. For now, users can get a step-by-step guide of how to use and install it [here](https://veracrypt.codeplex.com/wikipage?title=Beginner%27s%20Tutorial).

# Tips on using file encryption safely

There are a few things you should bear in mind when using TrueCrypt and tools like it. No matter how sturdy your safe is, it won't do you a whole lot of good if you leave the door open. When your TrueCrypt volume or container is 'mounted' (what it calls open to view your files), your data may be vulnerable, so you should keep it closed except when you are actually reading or modifying the files inside it.

There are a few situations when it is especially important that you remember to ?dismount? (what it calls close) your encrypted volume:

* Dismount it when you walk away from your computer for any length of time. Even if you typically leave your computer running overnight, you need to ensure that you do not leave your sensitive files accessible to physical or remote intruders while you are gone.
* Dismount it before putting your computer to sleep.
* Dismount it before allowing someone else to handle your computer. When taking a laptop through a security checkpoint or border crossing, it is important that you disconnect all encrypted volumes and shut your computer down completely.
* Dismount it before inserting an untrusted USB memory stick or other external storage device, including those belonging to friends and colleagues.
* If you keep an encrypted volume on an external hard drive or a USB stick, remember that just removing the device may not immediately disconnect the volume. Even if you need to secure your files in a hurry, you have to dismount the volume properly, then disconnect the external drive or memory stick, then remove the device.

# A secret safe within a safe

One of the weaknesses with some encryption tools is their visibility ? you may be worried that someone could find the encrypted volume, see that you were trying to conceal information, and use intimidation, blackmail or interrogation to force you into opening it.

However VeraCrypt allows you to create a secret volume, inside your regular encrypted volume, to hide your most sensitive information. It is similar to installing a secret 'false bottom' inside your office safe. If an intruder steals your key, or intimidates you into giving them the safe's combination, they will find some convincing decoy material, but not the information that you truly care about protecting.

You open this secret volume by providing an alternate password that is different from the one you would normally use. Even if a technically sophisticated intruder gains access to the standard volume, he will be unable to prove that a hidden one exists.

# Hiding your encryption

If you are concerned about encryption software being found on your computer regardless of what?s in it, there are a few tricks to help disguise VeraCrypt.

* You can rename your encrypted volume to look like a different type of file. Using the '.iso' file extension, to disguise it as a CD image, is one option that works well for large volumes of around 700 MB. Other extensions would be more realistic for smaller volumes.
* You can also rename the VeraCrypt program itself, assuming you have stored it as you would a regular file, rather than installing it as a program. The [VeraCrypt Guide](umbrella://lesson/truecrypt) explains how to do this.

# When encryption is illegal

Encryption is illegal in some countries, which means that downloading, installing or using software of this sort might be a crime in its own right. Any time that merely being associated with encryption software would be enough to expose you to accusations of criminal activity or espionage (regardless of what is actually inside your encrypted volumes), then you will have to think carefully about whether or not such tools are appropriate for your situation.

If that is the case, you have a few options:

* Store only non-confidential information
* Use a system of code words to protect key elements of your sensitive files
* Store all of your sensitive information in a secure webmail account ? you would need a reliable network connection and an advanced understanding of computers and Internet services
* Keep sensitive information off of your computer by storing it on a USB stick or portable hard drive ? carrying around sensitive, unencrypted information is usually a very bad idea so you would need to keep the device in a very secure place

Swipe right for this lesson's checklist

### RELATED LESSONS/TOOLS

* [Managing Information Lesson](umbrella://lesson/managing-information)
* [Office Lesson](umbrella://lesson/office)
* [Malware Lesson](umbrella://lesson/malware)
* [TrueCrypt Tool Guide](umbrella://lesson/truecrypt)

### FURTHER READING

* [EFF - Encryption](https://ssd.eff.org/en/module/what-encryption)
* [Security in a Box - Chapter 4, Encryption](https://securityinabox.org/chapter-4)