How To Password Protect Your USB Stick: 3 Easy Ways

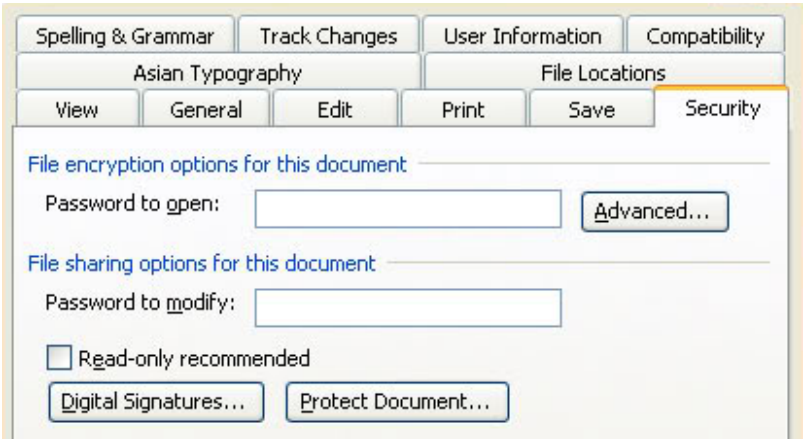
USB thumb drives are small, portable, and can be read on any device with a USB port. These features make them the perfect vehicles to transport data between computers. Due to their portability, however, they are also easily lost. Thus sensitive files callired on a USB stick should always be protected.

Unfortunately, you cannot simply password protect your entire USB stick, like you have password protected your Facebook account. Tools that will seriously protect your data, all work with encryption. Unless you want to invest in a secure flash drive with hardware encryption, you can use freeware applications to achieve a similar level of protection. This article summarizes some of the easiest ways to password protect files and folders on your computer.

1. Manually Save Files with a Password

As mentioned above, you can't safely password protect your entire USB stick without using encryption. However, if you shy away from the time consuming encryption process of entire folders and need a really quick way to only protect a few selected files, maybe you can simply save those with a USB password.

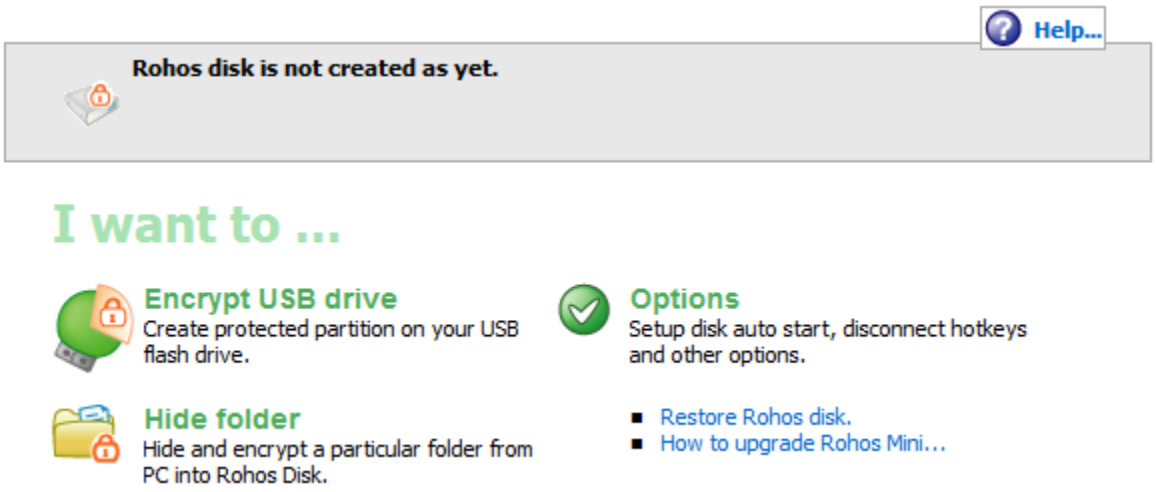
Many programs, including Word and Excel, allow you to save files with a password. For example in Word, while the document is open, go to > *Tools* > *Options* and switch to the *Security* tab. Now enter a *Password to open*, click OK, re-enter the password when asked, and finally save your document and don't forget the password.



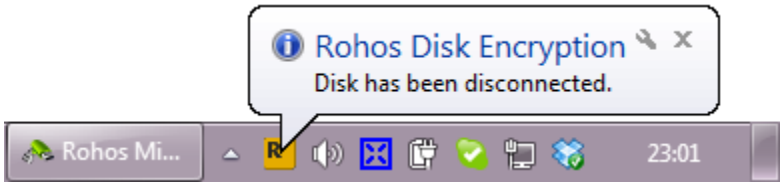
2. Create an Encrypted & Password Protected Partition with Rohos Mini Drive

Many tools can encrypt and password protects your data. Most, however, require Administrator rights to run on any given computer. Unfortunately, this is also the case for one of the best encryption tools: TrueCrypt. Tools like these are not a viable solution if you need to securely transfer data to a computer where you do not have Administrator rights.

Rohos Mini Drive, on the other hand, is a tool that will work whether or not you possess Administrator rights. The free edition can create a hidden, encrypted, and password protected partition of up to 2GB on your USB flash drive. The tool uses automatic on-the-fly encryption with AES 256 bit key length. Thanks to the portable Rohos Disk Browser, which is installed directly on your flash drive, no encryption drivers need to be available on the local system. Subsequently the protected data will be accessible anywhere.



Once you have created a password protected and encrypted container on your external drive, you can open it by clicking the *Rohos Mini.exe* icon from the root folder. After entering the password, your Rohos disk will be mounted and accessible via your *Computer*, i.e. the directory of all drives and partitions connected to your system. To close your Rohos partition, right-click the Rohos icon in the Windows taskbar notification area and select *Disconnect*.



.

3. Lock Your Flash Drive with USB Safeguard

Like Rohos Mini Drive, USB Safeguard is a portable app that runs directly from your flash drive and thus does not require Administrator rights on the local computer. It uses on-the-fly AES 256 bit encryption. The free version is limited to drive size of 2GB.

Download the *usbsafeguard.exe* and copy it to your USB flash drive. Run it from your flash drive and enter a password to lock the drive. To unlock it, run the file again and enter the password. The locking procedure must be

repeated every time you want the drive to be locked as the tool will remember its last status, i.e. locked or unlocked. This also means that you can change the password every time you use USB Safeguard.