Instructions for USB encryption with VeraCrypt

USB (removable drive) is a place to store your important files. What will happen if you lose it? The result will be extremely bad so it is better to encrypt your USB. In this article, TipsMake.com will guide you how to simple and effective USB encryption.

USB (removable drive) is a place to store your important files. What will happen if you lose it? If you have not created a backup, all the important data will be lost, or worse, you do not know who will use them.

Better yet, you need to protect yourself by encrypting your USB stick. If you use this method, unless the person who gets the USB has a rich resource to break the advanced password or because you have not enough security settings, you can rest assured that your data is in good condition. Safe state.

1. Using USB to lock or unlock Windows computer, have you tried it or not?
2. Instructions for encrypting USB or memory cards with Bitlocker on Windows 10

Download and install VeraCrypt

VeraCrypt is the easy and safe way to encrypt your USB and other storage devices. Besides, this is a very reliable application

In this article, I will guide you to use VeraCrypt in Linux and Windows, but this application is also available on Mac.

Windows and Mac users can download the installer from the download page of the project, and Linux users can find VeraCrypt in their distribution repositories.

If you are concerned about security, you can use the signatures provided on the download page to verify the installer before running it.

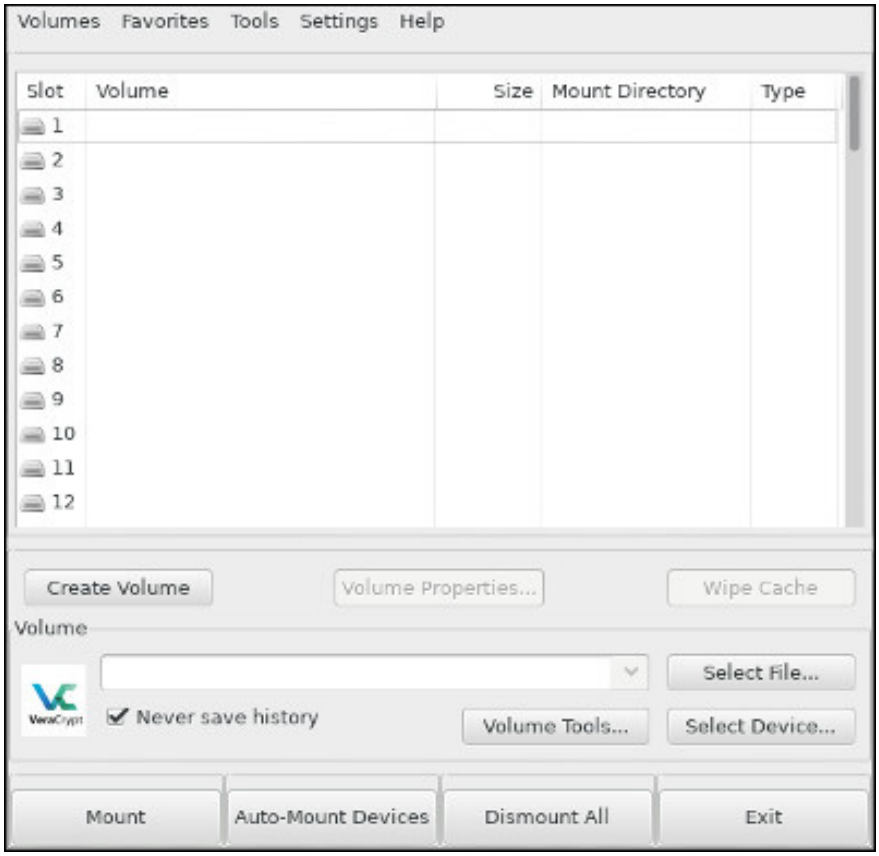
VeraCrypt provides a fairly simple installer, just click and follow the instructions. The "Next" keyword will work in most cases.

USB encryption

Once you have installed VeraCrypt, you can open and start your USB setup.

Before starting, remember to copy everything from the USB because this process will format the USB and you will lose all the files on it.

Create Volume



When opening VeraCrypt for the first time, you will see a window with a list of available drives. However, this is not all real drives. They will show up where you mount the encrypted drive, so don't worry!

Just below, you'll see the **Create Volume** button, click it.

Then you will see the Volume Creation Wizard window appear. There will be 2 options for you to choose from. However, you should select the second option because you will create encrypted volumes on the USB, then click **Next.**

Standard and Hidden

VeraCrypt supports 2 different encoding volumes. First, you have the standard volume. They are just basic encoded volumes that are freely seen. Hidden volume is not visible. For most programs, they are just like random data or unformatted drives. These hidden volumes will provide additional security for your USB.

Select USB

The next screen allows you to select the volume you want to encrypt. This is also where you need to select a USB device from the list of available drives. Make sure you make the right choice, because there will be problems if it accidentally formats and encrypts an important hard drive.

In addition, you have the choice between encrypting the entire device or a single partition on that device. If you want to encrypt the entire device, select the device on the menu and not any partition.

Choose encryption

This is a very important step. The type of encryption you choose will protect your file. If you are not knowledgeable about encryption, choose **AES** as the ' *Encryption Algorithm* ' and **SHA512** as ' *Hash Algorithm* .'

You can also use group coding options if it is not safe enough. However, they will slow down your drive.

Create a password

The next window allows you to set a password. You need a password to open the encrypted USB and need to balance between security and the memory's password. Password containing about 15 characters is best.

If you forget your password, your data will be lost and there is no way to retrieve it.

Format and complete

The last two windows will help you create encryption, select the format for the drive and format it.

The installer will ask if you need to save files larger than 4 GB. It will default to create a FAT32 partition if you choose not, because this is the most popular option. However, you should choose an **NTFS partition** for Windows or an **EXT4** partition for Linux.

When creating entropy for encryption, move the mouse randomly in the settings window to help VeraCrypt create the most secure encryption key possible.

Finally, select **Finish** and let VeraCrypt create an encrypted volume.

Use USB

Return to the main screen and attach the USB to the computer. Click **Select Device** , then select your encrypted **USB** and click **Open.**

Go back to the main menu and click on **Mount** at the bottom of the window.

VeraCrypt will mount your drive where you specify. After that, you can use it like any other USB drive.

By using VeraCrypt, your USB will be encrypted and you can be assured of your data!

You finished reading the article "**Instructions for USB encryption with VeraCrypt**" 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.