How to use VeraCrypt's advanced features to secure important files

Many security experts recommend VeraCrypt to secure sensitive files. It's not hard to see why: VeraCrypt offers users the ability to encrypt files 'military-grade'.

It's free, open source, and available on all major desktop operating systems. Anyone can use VeraCrypt's basic functions for files that need to be kept safe. But if you're looking to take file security to the next level, VeraCrypt can also protect you with many advanced features.

How to encrypt a partition or an external hard drive

Picture 1 of How to use VeraCrypt's advanced features to secure important files

Users often create container files encrypted with VeraCrypt. But the program is also capable of encrypting entire drives and partitions. Windows users can encrypt their system drives and partitions.

VeraCrypt users on any platform can also encrypt USBs and other types of external drives. In fact, it is one of the best programs for USB encryption. To begin this process, open **the VeraCrypt Volume Creation Wizard** . Select **Encrypt a non-system partition/drive** and click **Next.**

Picture 2 of How to use VeraCrypt's advanced features to secure important files

When choosing a location for the encrypted volume, VeraCrypt will prompt you to select a drive or partition. Click **Select Device.**

Picture 3 of How to use VeraCrypt's advanced features to secure important files

You have the option to choose an entire non-system drive or a partition in the drive to encrypt. You can choose to create multiple partitions in any external hard drive. Then you can encrypt just one partition of the drive. Click **OK** once you have selected the drive or partition to encrypt.

Picture 4 of How to use VeraCrypt's advanced features to secure important files

Please note that any drive or partition you select will have its data erased and its files destroyed.

Like any other file or drive, VeraCrypt is also prone to unwanted data deletion or corruption. This is why you should always back up your files.

Only click **Yes** on the pop-up warning if you are sure about encrypting your selected drive.

Picture 5 of How to use VeraCrypt's advanced features to secure important files

If you are going to encrypt a non-system drive with multiple partitions, make sure you format the drive first to delete those partitions. Click **Next** on the wizard.

Picture 6 of How to use VeraCrypt's advanced features to secure important files

As usual, VeraCrypt will prompt you to choose your drive's encryption options, password, and file format. Click **Format** , then select **Yes** when you're ready to create your encrypted external hard drive.

Picture 7 of How to use VeraCrypt's advanced features to secure important files

Once you format your encrypted device, it will no longer be accessible outside of VeraCrypt. To mount your encrypted device, select it with **Select Device** , click **Mount** and enter your password.

Picture 8 of How to use VeraCrypt's advanced features to secure important files

You can use the encrypted device like any other VeraCrypt volume and unmount it as usual. To decrypt your device, format the drive/partition using your desktop's built-in drive management software.

How to use other protections for VeraCrypt volumes

Picture 9 of How to use VeraCrypt's advanced features to secure important files

VeraCrypt's default volume settings combined with a strong password provide high security for most users. But they may not be enough if you, your team, or your business are vulnerable to certain threat actors. To ensure that your precious data is safe, VeraCrypt has even more features to make encrypted volumes uncrackable.

Using encryption and hashing algorithms

Picture 10 of How to use VeraCrypt's advanced features to secure important files

On **the Volume Creation Wizard** , you can choose between many options to encrypt and hash your volume. The default AES algorithm is a common but secure type of encryption. But you are free to use other ciphers like Twofish and Serpent. You can even stack multiple algorithms on top of each other.

Picture 11 of How to use VeraCrypt's advanced features to secure important files

You can choose to add your own password hashing algorithm or method. The hash algorithm determines how your password is converted into a hash that VeraCrypt can use to decrypt your volume. Using a strong hashing method like SHA-512 or Whirlpool, along with a high PIM number, will slow down any brute-force attacks on your volume.

Picture 12 of How to use VeraCrypt's advanced features to secure important files

You can test the speed of the hash and encryption on your machine by clicking **Benchmark.** Faster encryption and hash times mean shorter drive load times, but slower hash times mean better protection from brute-force attacks.

Use PIM . number

Picture 13 of How to use VeraCrypt's advanced features to secure important files

To put a Personal Iterations Multiplier (PIM) Number on the volume, tick the **Use PIM checkbox on the Volume Password** window . Clicking **Next** will take you to a window where you can set the PIM for your volume.

Picture 14 of How to use VeraCrypt's advanced features to secure important files

The volume's PIM determines how many times VeraCrypt will need to hash your password from plain text. The password of the default VeraCrypt volume (SHA-512) will be hashed 500,000 times. You can set the PIM volume even higher for better security.

Make sure you remember the volume PIM numbers if they are not set to default. Entering the wrong PIM number will result in the wrong hash. VeraCrypt cannot decrypt volumes with the wrong hash, even if your password is correct.

Using Keyfiles

Picture 15 of How to use VeraCrypt's advanced features to secure important files

You can get even better security by using files that act as keys for your encrypted volume. To add a keyfile for a volume, mark the **Use keyfiles check box on the Volume Password** window , and then click **Keyfiles.**

Picture 16 of How to use VeraCrypt's advanced features to secure important files

On the Select Security Token Keyfiles screen , you can set any file or directory path to use as the keyfile volume. You can use **Add Token Files** to set a hardware security key as your keyfile. If you keep your keyfile in a USB external to the volume's drive, your USB can also act as a physical security key. If you need VeraCrypt to generate a new keyfile, click **Generate Random Keyfile** .

Picture 17 of How to use VeraCrypt's advanced features to secure important files

When mounting a volume with a custom Volume PIM and keyfile, you need to tick the **Use PIM** and **Use keyfiles** checkboxes , and then click the **Keyfiles button.** This will allow you to enter the correct PIM and key file, along with the password, to open the encrypted volume.

Make changes to existing VeraCrypt volumes

Picture 18 of How to use VeraCrypt's advanced features to secure important files

After you create an encrypted volume, you can still make changes to the way you decrypt it. To do this, click **Volume Tools** on the main VeraCrypt window. You will have the option to change or delete the password, PIM and keyfile of the volume. You can do this if you need to change your password often.