How to create hidden, password-protected virtual drives using VeraCrypt

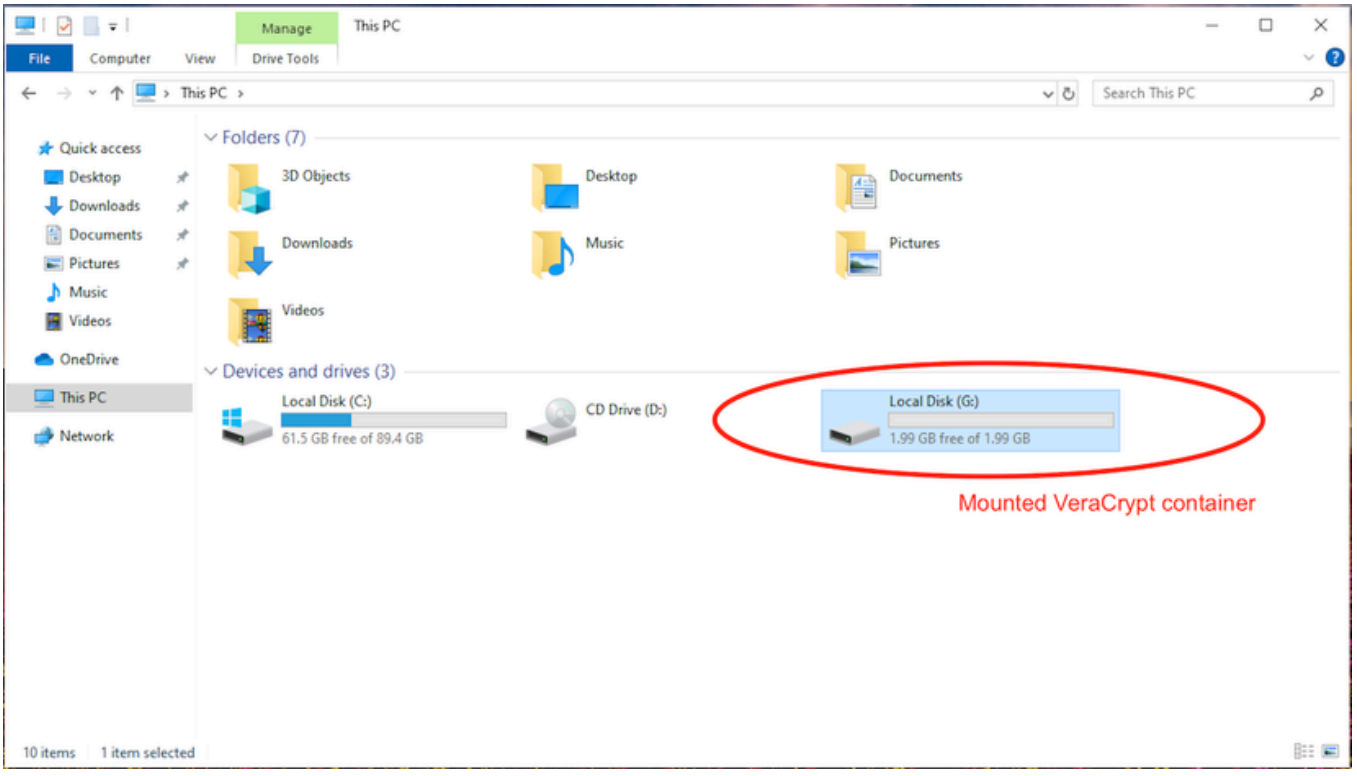
Summary

- Use VeraCrypt to create encrypted virtual volumes that mount like drives and vanish when unmounted.
- Choose a 20+ char passphrase, add key files for 2FA, and generate entropy with random mouse movement.
- Prefer exFAT for big files, keep vaults on removable drives if desired; portable VeraCrypt and 26-mount limit.

The safest way to secure your data on Windows is by keeping it in encrypted vaults. You can create hidden, password-protected virtual drives. Put your data in there, access it when you need to, and then hide the virtual drives again. This is everything you need to know to create and use super secure storage vaults on Windows.

How Veracrypt works

Our tool of choice is Veracrypt. Instead of locking individual folders or files, Veracrypt creates encrypted volumes. These volumes look and behave just like normal storage drives on your storage, except they're virtual and obfuscated.



We start by creating a new virtual volume using Veracrypt, which is just an innocuous file that resides somewhere on the machine's disk storage. You can keep it on a removable drive too and plug in the removable drive when you need to access the vault.

You then load the same file into Veracrypt, enter the password, and Veracrypt mounts it as a storage volume. You can interact with it, access your files, and move them around using File Explorer or the Terminal. When you're done, you can unmount the same volume using Veracrypt, and it'll vanish from the drive directory.

Veracrypt uses unbreakable algorithms to encrypt the volume, and you can even set up a 2FA system by supplying a 'key file.' A key file can be anything—text, image, video, Excel sheet. To unlock a double-locked volume like that, you need to provide the correct password and upload the right file. So even if someone manages to steal your password, they won't be able to unlock the vault until they supply the correct 'key' file too.

Install Veracrypt

Start by installing Veracrypt. It's a free and open-source app, available for all desktop platforms, including Raspberry Pi. On Windows or macOS, you can just download the installer packages and install Veracrypt like any other app. Linux users won't find Veracrypt in the official APT or Pacman repositories, but its prebuilt distro-specific packages and binaries are available on the Veracrypt website.

The Veracrypt interface shows a list of drive letters. These are the points where the volume will be mounted (naturally, pre-mounted volumes like C:\ are excluded from the list).

Set up Veracrypt volumes

We'll start by creating a fresh Veracrypt vault. Click the 'Create Volume' button on the dashboard or select 'Create New Volume' from the 'Volumes' menu at the top. It'll open the Volume Creation Wizard. The 'Create an encrypted file container' option should be selected by default. Leave it selected and click 'Next.'

The next window has the 'Standard Veracrypt Volume' selected by default. Keep it that way and click 'Next.'

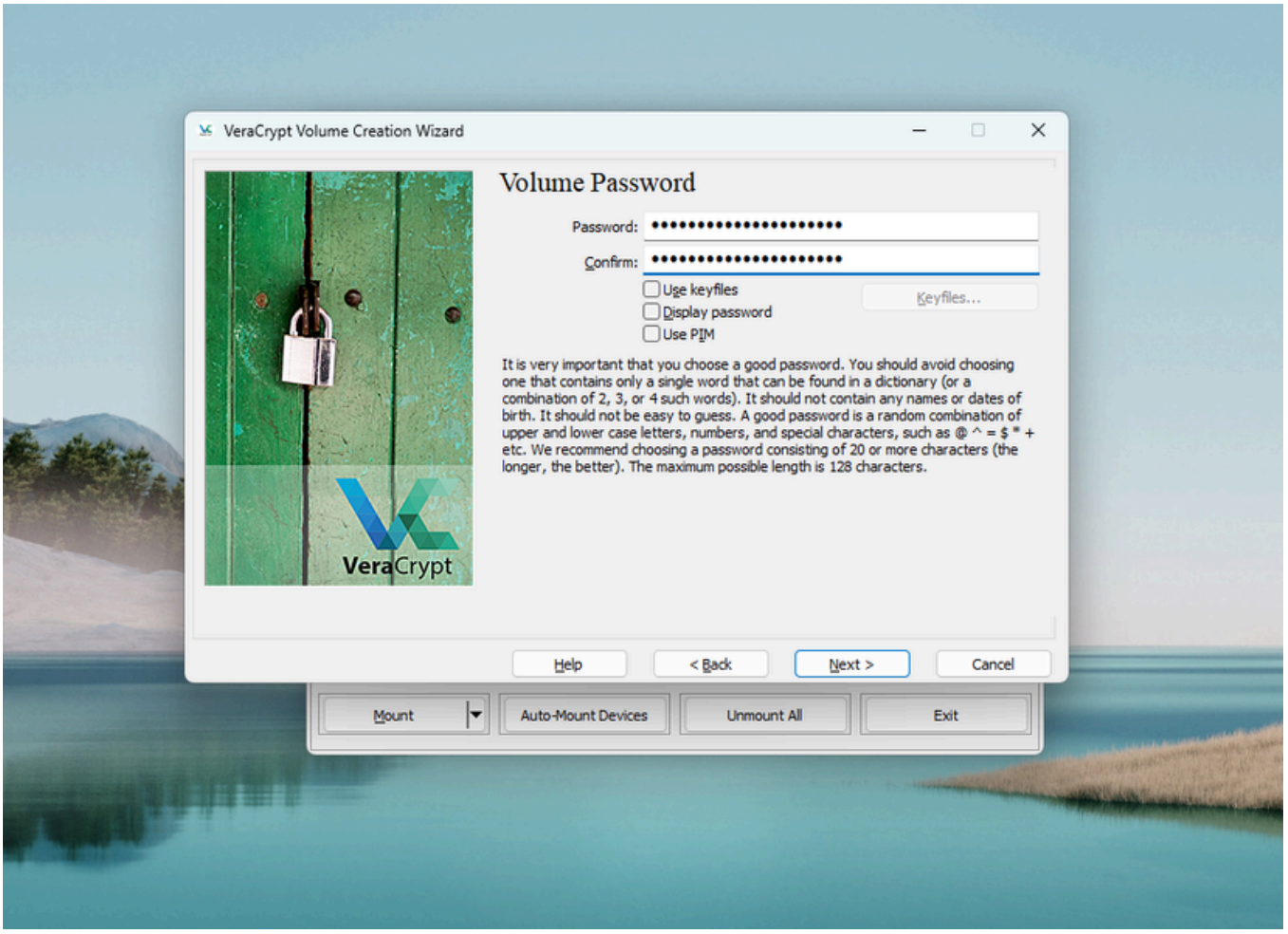
Now we'll create the file that'll act as our 'vault.' Click 'Select File' and browse to a destination you want to save the volume to. Give the file a name by typing it in the Explorer window and then clicking 'OK.' A new file (without an extension or icon) should be created in that destination.

You can also choose an existing file if you want the volume to blend in with the rest of your directory, but remember that all the contents of that file will be overwritten. So only choose a file you don't mind losing. Proceed with caution here.

The next step is locking this container with an encryption algorithm and storage size. By default, Veracrypt chooses the AES encryption method, which will do for our purposes. Also, you can choose any size for your vault, but you can't change that later. Make sure you give the vault enough space to hold your files.

You can choose more advanced algorithms too, which have their uses, but that might make the volumes slow to mount and unmount.

I recommend choosing a passphrase of 20 characters or more to secure your volume against brute force attacks. Also, include special characters and numbers in your passphrase.



You can also add 'key files' at this point for the extra layer of security I described.

Computers can't generate truly random numbers, so when software needs true randomness, it often relies on noise from the real world. Veracrypt uses random mouse movements to create truly random encryption keys for locking the vaults. You'll want to move the cursor within the Veracrypt window in random patterns. Select 'exFAT' from the drop-down menu and then click 'Format.'

By default, Veracrypt uses the FAT file system for the vault, which can't handle files bigger than 4GB. The exFAT file system doesn't have that restriction. If you'll only be accessing the vault on Windows machines, you can also choose NTFS, but it might leave some traces of the volume's existence in the Windows user space. I'd stick with exFAT in most cases.

Wait for Veracrypt to fully format the volume and exit the Veracrypt Volume Creation Wizard. Your vault is now ready for use.

Load and use a Veracrypt volume

To load a Veracrypt volume, select a drive letter from the list. For example, 'A:,' then click 'Select File' to find and select the volume container file you created earlier.

Click 'Mount.' Supply the password (and key files if you chose any during the setup process) and click 'OK.' If all goes well, the volume should be mounted and show up in File Explorer right away.

You can copy files here, access existing files, or point other apps to this directory. For all intents and purposes, this volume will function just like any other storage volume on your computer.

When you're done, you can open Veracrypt again and click 'Unmount' to lock and hide the volume again.

-
-
-