

Forum:[Hack Forums](#)

Thread: [How to hide ANYTHING with Veracrypt \(OPSEC GUIDE \)](#)

Chorozon - February 27, 2025, 2:13 pm

Another OPSEC guide for you guys , hopefully you have been following along and you are not in a south American jail or hiding in a embassy

Want to know how to stop the Federals cold booting your PC ? Need to keep files hidden just in-case someone IRL just to interrogate you for your loot !?

Step 1: Backup Your Files (Trust Me, You'll Thank Me Later)

Before doing anything, back up your data to an external drive or cloud storage. No encryption tool is perfect, and if the process gets interrupted (e.g., power failure, accidental shutdown), you don't want to risk losing everything. Make sure you have multiple backups of anything crucial.

Step 2: Download and Install VeraCrypt

Download VeraCrypt from the official site and run the installer.

During installation, you can keep the default settings, so just follow the prompts and install it on your computer.

Once installed, launch VeraCrypt from the Start Menu or desktop shortcut.

Step 3: Start the Encryption Process

In the VeraCrypt interface, click System from the top menu, then select Encrypt System Partition/Drive.

A window will pop up asking if you want to encrypt your system drive. Click Next.

Step 4: Choosing Between Normal and Hidden Encryption

Here's where things get interesting. VeraCrypt lets you choose between two types of encryption: Normal Encryption:

This is the most straightforward option. You'll create a single password that encrypts your entire system. Every time you start up your PC, you'll need to enter this password to unlock your drive.

Use this unless you specifically need a hidden system.

Hidden Encryption (for Plausible Deniability):

This is the cool part. A hidden VeraCrypt volume lets you create a second, hidden operating system within your encrypted partition.

The idea is that you'll have two passwords: one for a decoy system and one for your hidden system. The decoy system is the one you'd reveal if someone forces you to unlock your computer (for example, if you're in a dangerous situation or being extorted).

The hidden system is where your actual sensitive data is stored, and it's completely undetectable — unless you give the correct second password. You can't access the hidden system without the right password, and there's no way to tell it even exists unless someone knows what to look for.

This provides plausible deniability: you can claim you only have a decoy system and that the hidden one doesn't exist.

Step 5: Choose What You Want to Encrypt (System Partition vs. Whole Drive)

You'll be asked if you want to encrypt the system partition (where Windows is installed) or the entire drive.

System Partition is the usual option for most people.

If you have more than one partition (say, C: for the OS and D: for your files), you might want to choose Encrypt the whole drive to protect everything.

Most people will select Encrypt the Windows system partition, but if you need to encrypt more partitions, go for the whole drive option.

Step 6: Choose Your Encryption Algorithms

VeraCrypt will prompt you to choose an encryption algorithm. For most users, the default option of AES (Advanced Encryption Standard) is more than sufficient. AES is highly secure and widely trusted.

You can also use a combination of algorithms for extra security, but AES is typically strong enough for most personal needs. Just click Next when you're ready.

Step 7: Setting Up Your Passwords

This is where you get to create your two passwords (if you're using a hidden volume).

Create your password for the decoy system. This password will unlock the decoy system, which will look and feel like your real system. If someone is forcing you to unlock your PC, you'll enter this password.

Important: The decoy system should be a strong password (long and complex), but it doesn't need to be the one you'll use for your sensitive data.

Create your password for the hidden system. This password unlocks the real system, the one that holds all your sensitive files.

Important: This is the password that matters most. Make sure it's even stronger than the decoy password. It should be long, complex, and completely unique.

Step 8: Set Up Keyfiles (Optional)

VeraCrypt allows you to use keyfiles. These are files that must be present on a USB drive or external storage for the system to unlock, in addition to your password.

Keyfiles make it even harder for an attacker to break into your system.

Important: Don't lose these keyfiles. If you do, you won't be able to unlock the drive, even with your password.

Step 9: Moving the Mouse to Strengthen Encryption

Next, VeraCrypt will ask you to move your mouse randomly around the screen. This is to help generate more entropy (randomness) for your encryption keys. Just move your mouse around until it fills the progress bar and then click Next.

Step 10: Create a Rescue Disk

Now, you'll need to create a rescue disk. This is super important. The rescue disk helps you recover your system if anything goes wrong, such as bootloader corruption or other errors during the

encryption process.

VeraCrypt will guide you through the process of creating the rescue disk. It's recommended that you use a USB drive or CD/DVD for this.

Don't skip this step — having a rescue disk is your safety net if things go sideways.

Step 11: Wipe Your Drive (Optional but Highly Recommended)

If you're dealing with sensitive data, VeraCrypt will give you the option to wipe your drive. This wipes any unencrypted data and overwrites it with random data, making it extremely hard for anyone to recover your files after encryption.

Wipe mode: If you choose a 1-pass wipe, it'll overwrite data once with random data. You can also opt for more passes (like 3 or 7), but these take longer.

If you're not overly concerned about data recovery, select None (fastest).

Step 12: Test the Encryption Process

Before VeraCrypt actually begins the encryption, it will run a pre-test. This is an important step, so it can make sure everything is set up correctly.

VeraCrypt will install the bootloader and restart your PC.

When it boots up, you'll need to enter the decoy password to verify that everything works.

If everything checks out, you can proceed to the encryption process.

Step 13: Let the Encryption Begin

Once the pre-test is successful, VeraCrypt will begin the actual encryption process. Depending on the size of your system drive, this could take a while (several hours or even overnight).

Remember: You can't use your computer while the encryption is running, so you'll need to step away and let it finish.

Step 14: Accessing Your Encrypted System (and Two Passwords)

After encryption is complete, every time you boot your computer, you'll be prompted to enter your decoy password first. This gives you access to the decoy system, which looks and feels like your normal operating system.

If you enter your hidden system password, you'll unlock the real system — the one that contains your sensitive files. If you don't type the correct password, you'll never know the hidden system exists.

This two-password system ensures that no one can get access to your real data unless they know the correct password.

OpSec Tips to Keep in Mind:

Backup Your Data: Always back up your important files. If you lose your password or something goes wrong during the encryption process, you'll need a way to recover your files.

Choose Strong, Unique Passwords: Your passwords are your first line of defense. Use long, complex passwords, and don't reuse them.

Use Keyfiles for Extra Security: Consider using keyfiles as an added layer of security, especially for the hidden system.

Keep the Rescue Disk Safe: Store the rescue disk in a secure location. It's your safety net in case something goes wrong.

Don't Reveal the Hidden System Unless Absolutely Necessary: The hidden volume is for plausible deniability. Use it only if you need to and keep it secret.

Pr0m3th3us - *March 2, 2025, 7:49 pm*

I use vera, great tutorial as usual.

Chorozone - *March 2, 2025, 7:50 pm*

(Mar 2, 2025 08:49 PM)EliteH4X Wrote: [\[CITE\]](#) I use vera, great tutorial as usual.

Thanks brother if you have any suggestions just drop it in the comments