

Securing your Backups

Section: 3.5

Veracrypt (File/folder/ hard-drive/USB encryption)

In the list of open-source software, Veracrypt is one of the most useful and recommended tools from the community of security researchers. Any type of data can be stored in an encrypted format using veracrypt, which means no one can read out the data until he/she got the correct password or decryption keys. The need for encrypted file storage is essential.

For instance, if you accidentally lose your hard drive on the way to your home, there are high chances that someone will extract all the data like your pictures, videos, or even sensitive documents associated with your organisation and then upload it all on the internet without your consent which can put yourself in danger too.

Veracrypt

Veracrypt encrypts the entire disk drive, which means you do not have to encrypt your data every time you add any folder or file because veracrypt automatically does that. A fascinating feature of Veracrypt is that we can make a hidden partition or virtual hard drive in a local drive. In short, if someone forces you to open your encrypted hard drive, then actually he/she can't see the exact information because you have already made it hidden. The only thing anyone can see is what you want them to see. It is complicated to prove that any confidential data exists in the hidden volume if required safety measures are taken.

This tool (veracrypt) is available for Windows, MAC, and Linux which means unlike other built-in encryption tools in these platforms, veracrypt provides you with the ability to use your encrypted drive with any of the mentioned platforms. For better understanding, let's suppose you have enabled encryption for your external hard drive using BitLocker in windows OS. After encrypting the external hard drive using BitLocker, the drive cannot be opened on a machine running MAC OS because it does not have the utility to decrypt it until we use any third-party tool which leads a user to the complex solution. In such situations, veracrypt comes with the multiplatform solution.

Veracrypt

There were few reports which indicated that hidden volumes encrypted by veracrypt are detectable by forensic experts but still even if it appears to be true, no one can access the data due to the industrial encryption standard used in veracrypts.

It goes without saying that, it is entirely understandable that whatever tool we use to protect our data, we put our trust in that service by using their products, and there are still chances of residing any vulnerability.

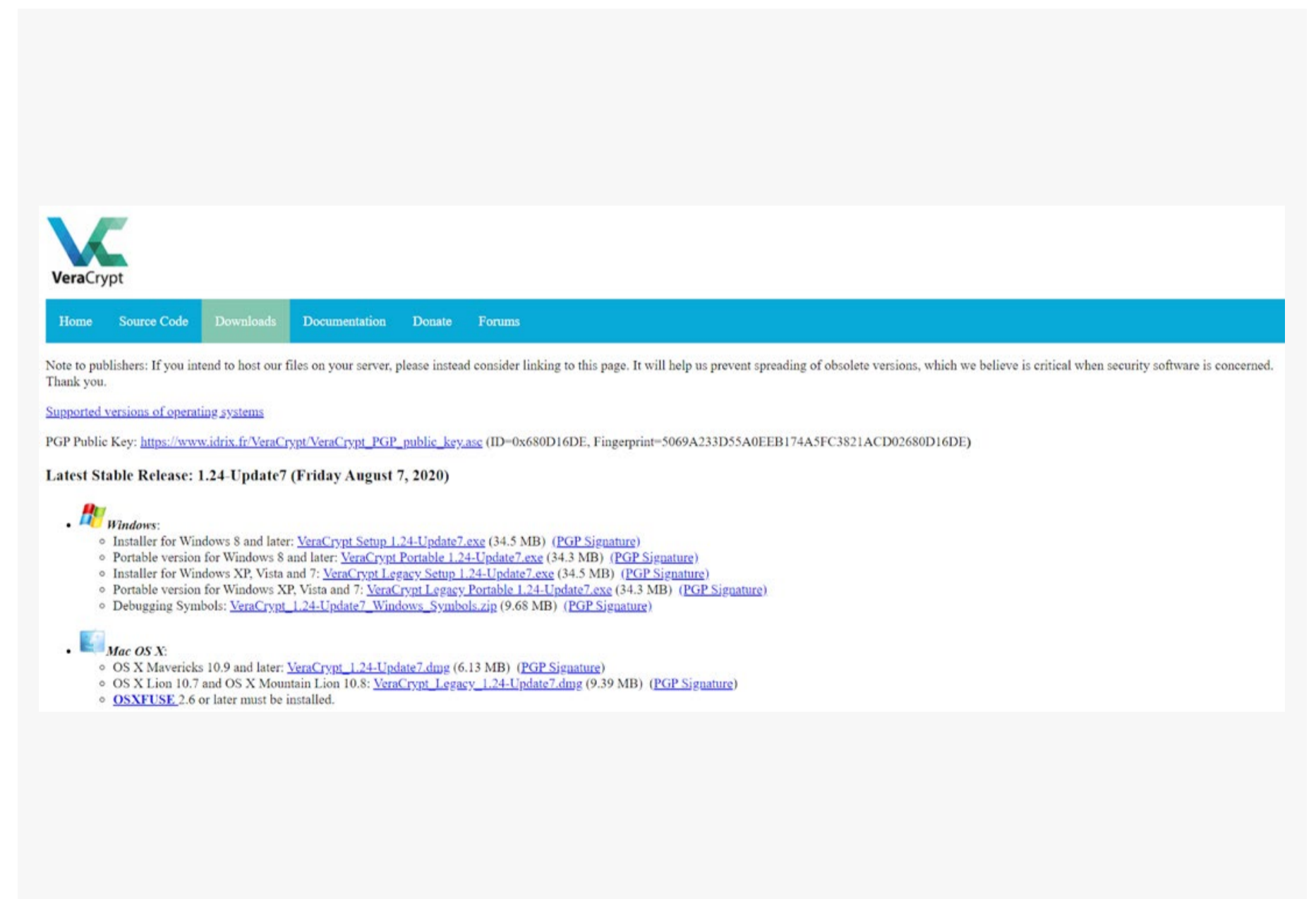
Step by Step Guide to Using Veracrypt

Note: This guide refers you to the installation and configuration of veracrypt only on Windows platforms.

You can download any veracrypt version from the official veracrypt website.

Installation and configuration:

To download the veracrypt installer for Windows 10 go to this link. You can see multiple veracrypt versions available for Windows and MAC below.

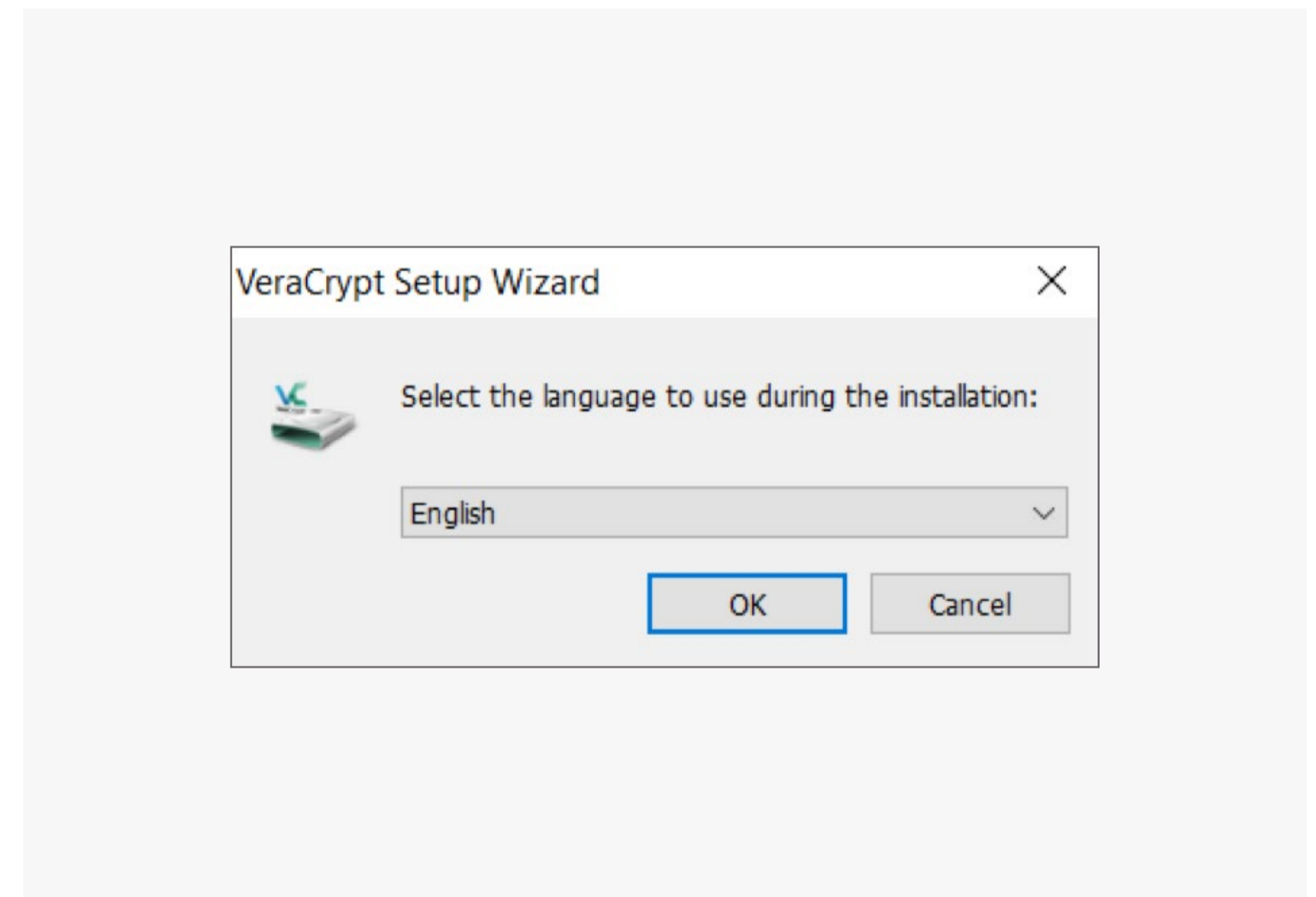


The screenshot shows the VeraCrypt website's download page. At the top left is the VeraCrypt logo. A navigation bar contains links for Home, Source Code, Downloads, Documentation, Donate, and Forums. Below the navigation bar is a note to publishers and a link to supported operating systems. The page lists the latest stable release as 1.24-Update7 (Friday August 7, 2020). Under the Windows section, there are five download links: VeraCrypt Setup 1.24-Update7.exe (34.5 MB), VeraCrypt Portable 1.24-Update7.exe (34.3 MB), VeraCrypt Legacy Setup 1.24-Update7.exe (34.5 MB), VeraCrypt Legacy Portable 1.24-Update7.exe (34.3 MB), and VeraCrypt 1.24-Update7 Windows Symbols.zip (9.68 MB). Under the Mac OS X section, there are three download links: VeraCrypt 1.24-Update7.dmg (6.13 MB), VeraCrypt Legacy 1.24-Update7.dmg (9.39 MB), and OSXFUSE 2.6 or later must be installed.

Step by Step Guide to Using Veracrypt

After downloading the setup from the website, open it using "run as administrator". It will ask you to make changes on your PC. Click "Yes"

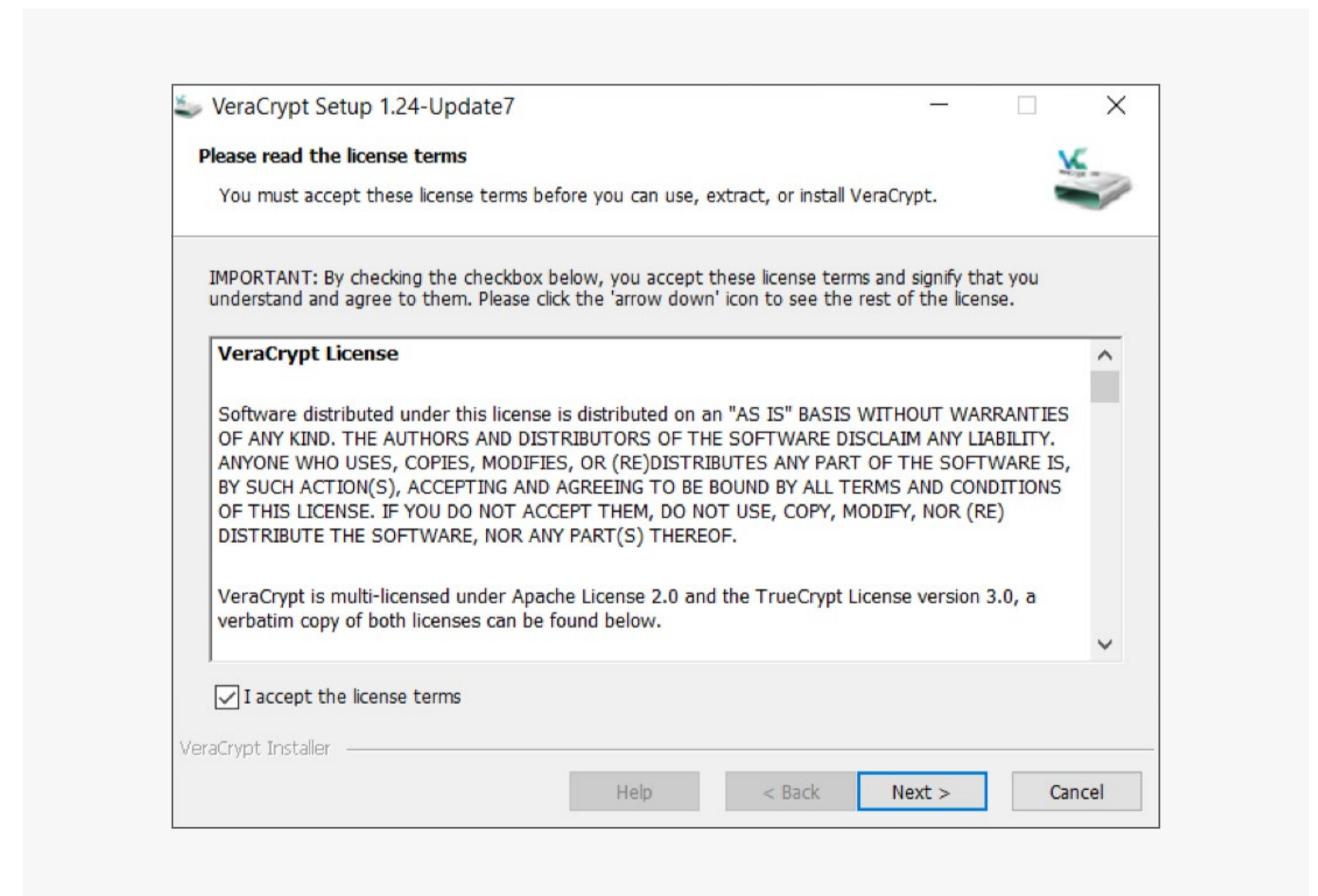
Select the language you prefer and click on "OK."



Step by Step Guide to Using Veracrypt

After selecting your preferred language, A pop up will appear for license terms.

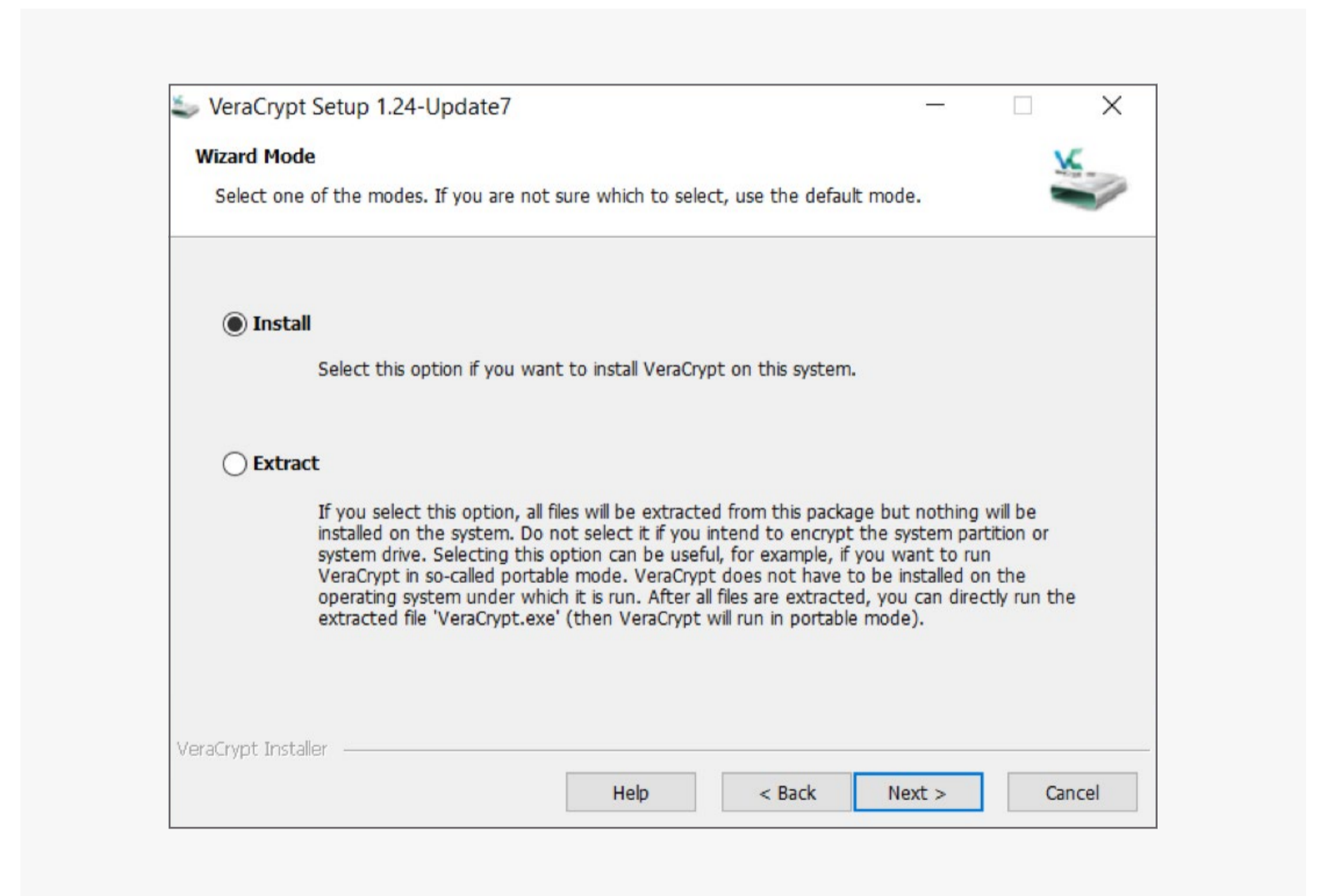
Please give it a read and after selecting the license terms, click on next.



Step by Step Guide to Using Veracrypt

Now in wizard mode, you can see two options: select "install" and click on next.

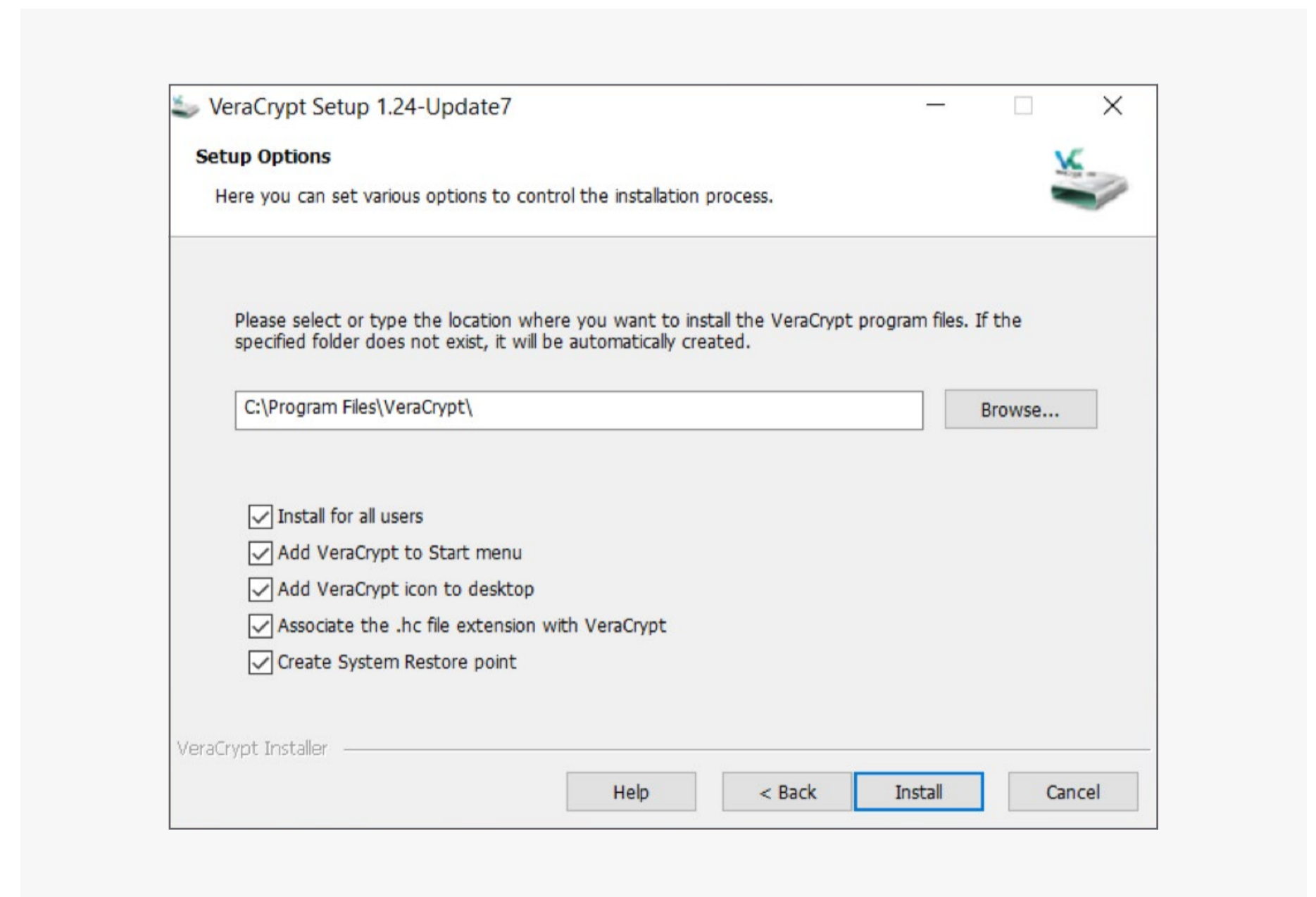
It has clearly been mentioned in the below picture that if you select "extract", All the files will be extracted but veracrypt will not be installed on your system.



Step by Step Guide to Using Veracrypt

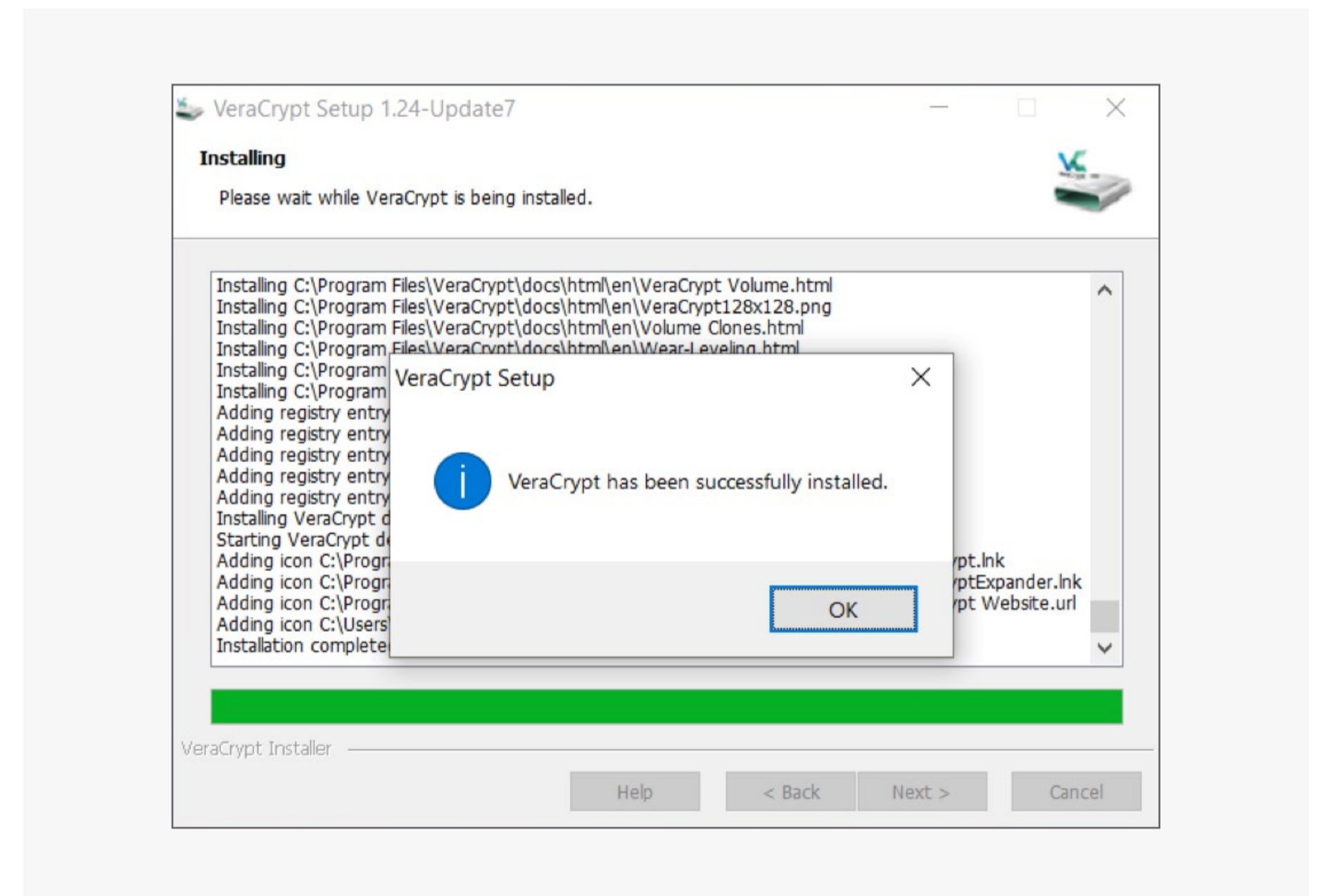
Now you have entered into the setup options, where you can select the installation directory for veracrypt. Select any available partitions and click on install.

Here we will install it on our "C" partition drive.



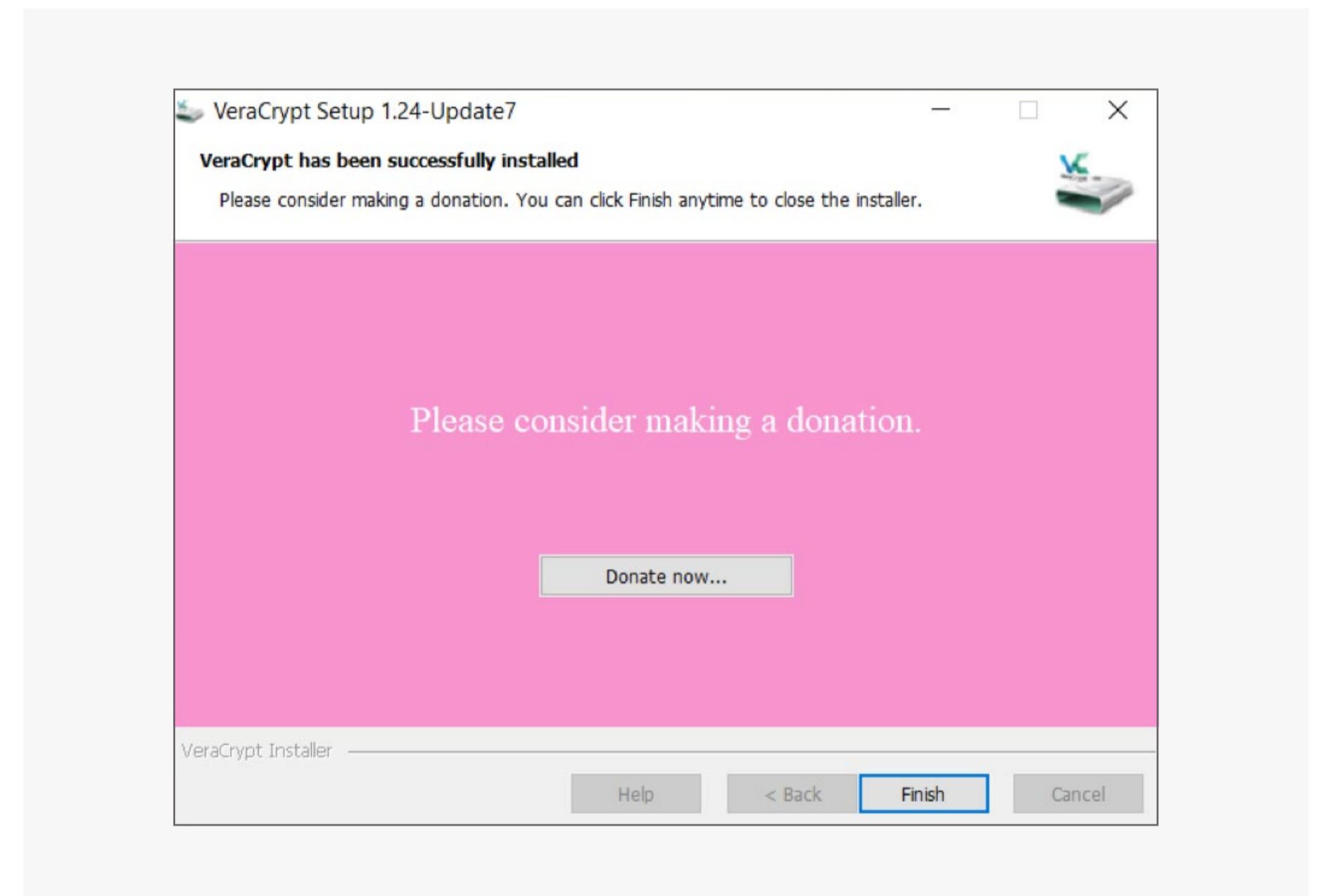
Step by Step Guide to Using Veracrypt

After clicking on the “install” button, the installation phase begins and a dialogue box will appear of a successful installation.



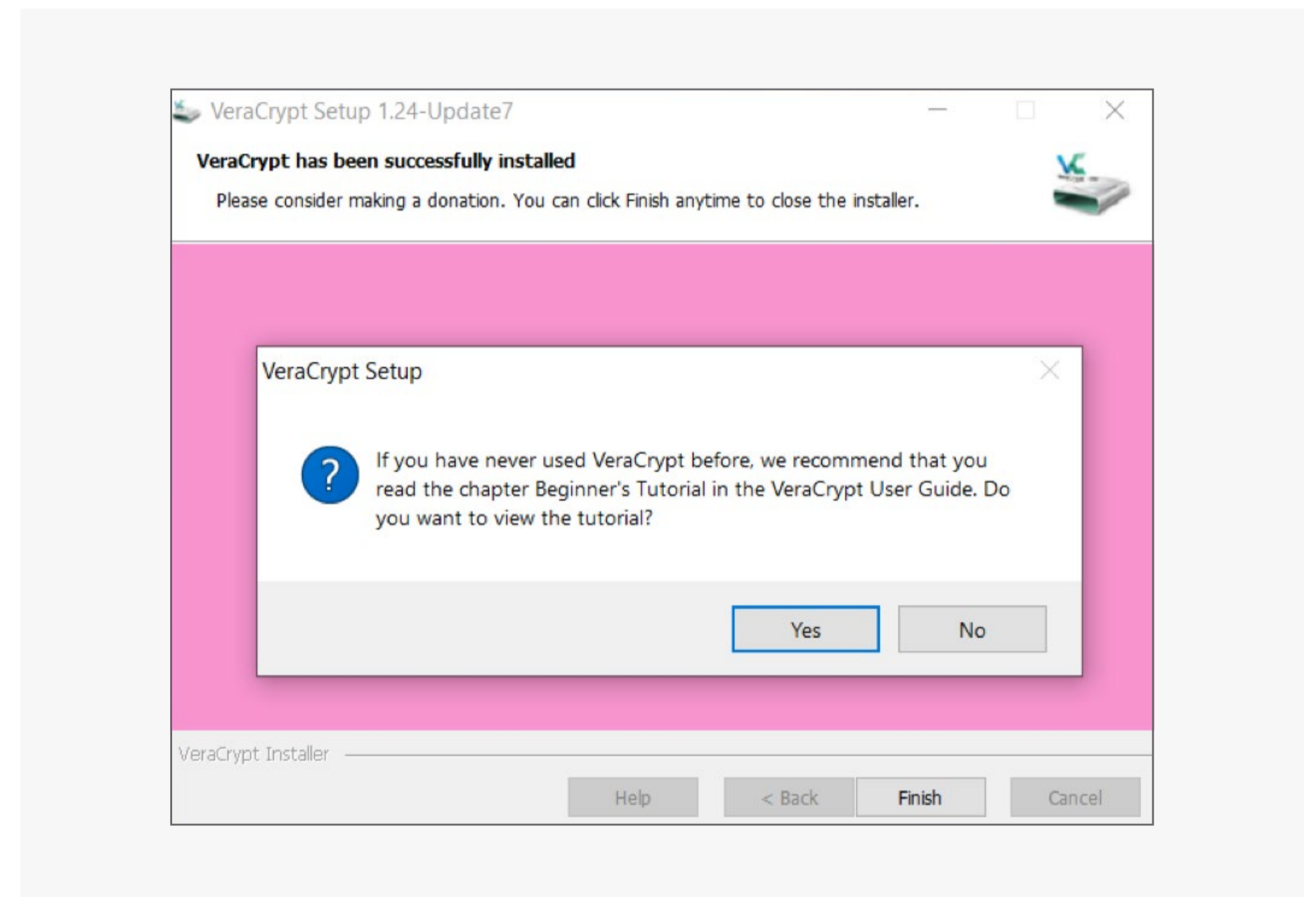
Step by Step Guide to Using Veracrypt

Now, as veracrypt is installed on your computer, it will ask for donations as mentioned below. You can skip if you want and click on finish.



Step by Step Guide to Using Veracrypt

After clicking on “finish”, veracrypt might ask you to read the beginner guide written on their website. On your preference, you can select any of the buttons, and there will be a veracrypt shortcut on your desktop.



Creating encrypted file container using Veracrypt

As veracrypt provides different options to encrypt your data on external hard drives and USBs, you can start simply by creating a container on your existing virtual volumes.

Secure Cloud backup

Clouds are the best way to back up your data and help you to store it if the user does not have enough space on his local storage device. When your device connects to the internet, it becomes more vulnerable, and chances get increased for different attack vectors which can be initiated against your device and data. Now, most of the services you used daily are synchronised with online cloud backups. For instance, WhatsApp supports backup with google drive and iCloud in case of iOS devices.

Secure Cloud Backup

Another example is google drive and dropbox, which provide you with free space on their cloud storage infrastructure so you can easily upload your data from your local device to their platforms. If your device gets lost or your hard drive gets damaged, then you do not have to worry about the data if you have already uploaded it to cloud storage.

Every individual or organisation has a different threat level depending on the nature of their work, and that's why it'll take some extra precautionary measures while uploading your data to the cloud. It gives you proper support to access your data from any compatible device and any location. There are many pros and cons to cloud storage which every individual needs to understand before using it.

Benefits of Cloud Storage

- If you use cloud storage, you can upload your data in an organized way to the cloud. There is no need to set up a huge server physically on your location or maintain them.
 - Sharing any file or folder with the other person becomes very easy and only far away at a few clicks.
 - If you accidentally delete your data from the cloud, there are high chances that it can be recovered by discussing the matter with the company.
- There are many subscription packages available on the platform with different free space. You can choose any package according to your preferences.
 - Suppose you have any sensitive information in your local hard drive or flash storage. In that case, there is a possibility that your device can be stolen or seized by authorities at any point of time or accidentally lost somewhere. Which means you lose access to your data until you find that device.

Disadvantages of Cloud Storage

- As a journalist, you need to be extra careful before uploading your data to the cloud. The cloud service you choose might have a backdoor policy for government or law enforcement agencies which clearly stated that the company is under obligation to provide data of any user if they asked by the authorities.
- Cloud storage is on the internet, and millions of users can easily access the platform, which includes journalists, freelancers, lawyers and even hackers.
- Cybercriminals are always looking for such services which can, by manipulating, get them a massive amount of financial benefit and information. Any vulnerability within the cloud platform infrastructure can lead to the breach of sensitive data.
- If your data volume is extensively high, you might need a stable and high bandwidth of internet connection to upload it to the cloud. A slow internet connection might not be able to upload your data in easy time, and it might take days to upload it all.

Best practices to secure your data on the cloud

- Before choosing cloud storage, you must be aware of their basic security infrastructure. Otherwise, your files can be exposed publicly if there is any security loophole or data breach incident.
- You must use a strong password for your cloud storage account. Make it random and unique so it can be avoided easily by the basic password cracker techniques like the dictionary or brute force attack.
- Make sure to enable two-factor authentication on your cloud storage account so even if an attacker manages to get hold of your password, he/she still needs access to the OTP codes generated or sent by your authentication app or telecom provider respectively.
- One of the best and useful practices is to encrypt your data by any third party open-source tool, before uploading it to the cloud. This helps you to protect your data even if the cloud platform faces an incident like a data breach.

Secure Cloud Storage Platforms: SpiderOak one

SpiderOak one is an online backup solution and was established in around 2006, which provides end to end encryption and some strong privacy protection features to combat any digital threat.

It can be used for multiple platforms including Windows, MAC and Linux. Also, SpiderOak strictly sticks to the “Zero-Knowledge” policy, which clearly states that any third-party and even employees of companies are unable to access the data of any individual.

It gives a free trial of 21 days including 250 Gb of free space to new users. When you install client side software of SpiderOak one on any of the platforms (windows, macOS or Linux). It encrypts your data automatically before uploading it to the cloud server.

SpiderOak has many open source products but when it comes to spiderOak one, they haven't disclosed the source code for their desktop application which actually puts a big question of the reliability of end-to-end encryption.

Secure Cloud Storage Platforms: Sync

In recent years, Sync has become so popular due to its stable support as a cloud storage platform. The design of the Sync client program is very user friendly, and unlike spiderOak one, its support for mobile apps is fully featured and functional. By following the encryption methodology of spiderOak one, Sync also supports end-to-end encryption which means before your files leave your system (device or mobile), and on its way to the cloud server, they will get encrypted. If there is any situation which requires your files to be exposed to the legal authorities, it will just be in an unreadable format which no one (including the company itself) can get the useful information by manipulating your files.

The downside of this cloud storage service is that it is a closed source client-side application; however the web portal is open source. This means security researchers are unable to deeply investigate the program.

Sync provides 5GB of free space to new users and can be upgraded further if additional storage is needed. It also supports real-time synchronization from your local device to the server.

Sync is available for both Windows and MAC but does not provide a feature to upload files directly from Linux until you use their web portal using a supported browser on Linux OS.

Secure Cloud Storage Platforms: NextCloud

Nextcloud is one of the leading open-source cloud storage offers many different cloud services. It helps you to backup and store your data anywhere you want like on your personal device, on an online virtual machine, or at any of the providers offered by nextcloud. To configure nextcloud self-hosted server, you can find complete guides and recommendations on the website, so it becomes a bit easy for the users to set up a self-hosted server in a secure way.

Nextcloud synced your data through various devices and platforms using strong end-to-end encryption methodology. Unlike Sync, Nextcloud is available for all the major platforms including Windows, macOS, Linux and an online web portal is also available to access the data.

NOTE:

Before uploading your data on the cloud, make sure to encrypt it using any of the third party open source tools to ensure the safety of your data.

The **next** section will highlight the importance of privacy, particularly privacy in digital space.