how to protect what you upload: End To End Encryption

You can find those slides on wiki.estaca.net, then End To End Encryption workshop

Contents

- 0) Why those workshops ?
- 1) general security advises
- 2) Hands on: Set up a local password manager and a strong passphrase with KeepassXC and the DiceWare method
- 3) What is End To End Encryption (E2EE) ? Which tools that you already know are and which ones aren’t E2EE ?
- 4) Hands on: How to encrypt files, folders and external storages easily with veracrypt and cryptomator
- 5) (if time allows): How to protect your devices themselves: Full Disk Encryption

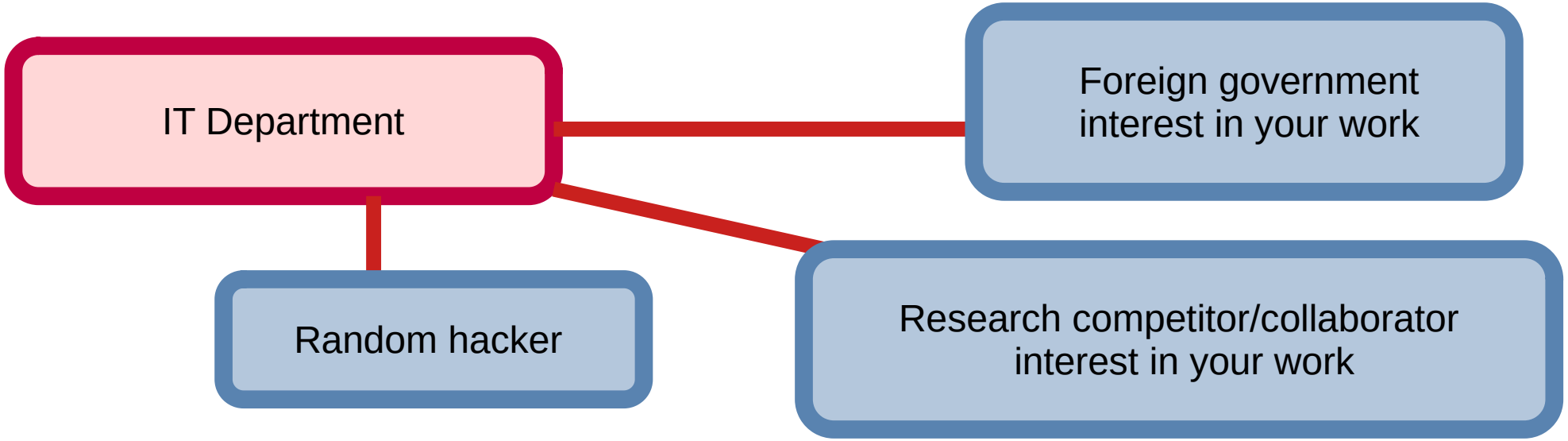
Important ressources

- The Electronic Frontier Foundation (EFF): https://www.eff.org/pages/surveillance-self-defense

- The freedom of the Press Foundation guides: https://freedom.press/digisec/blog/file-security/

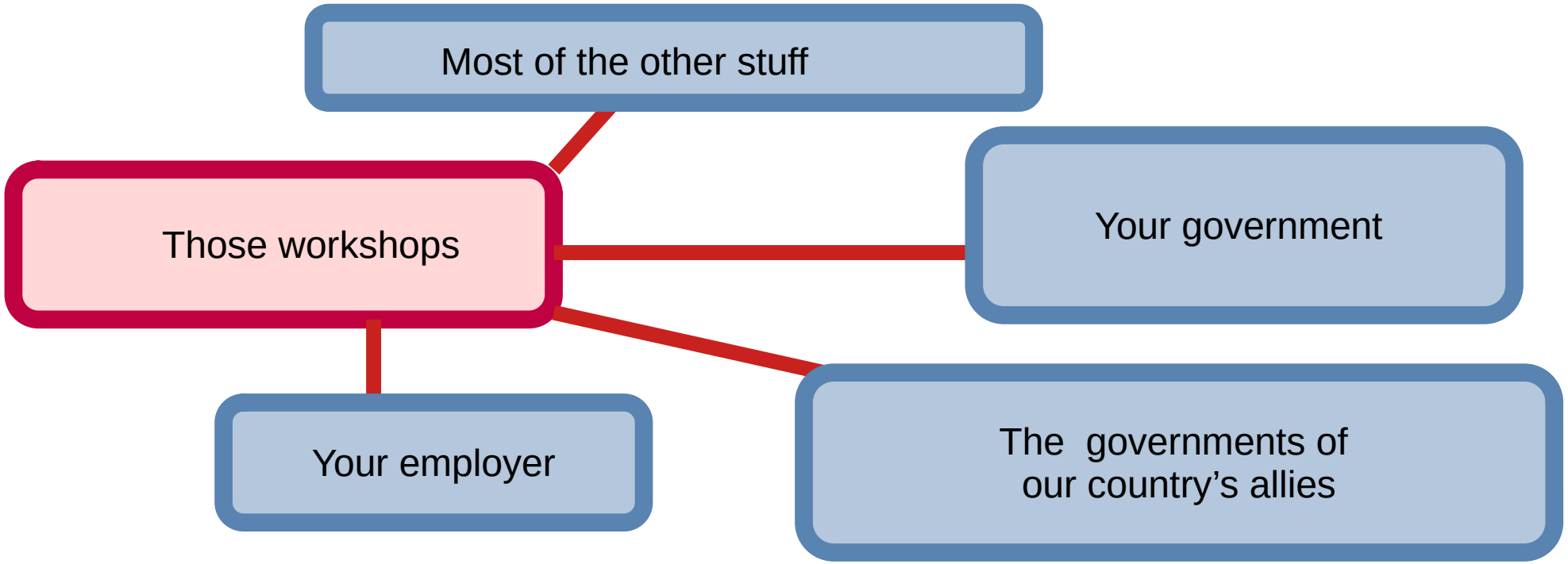
Why me ?

- I am not an expert on those topics
- There are much more talented people in the IT department
- But they do not protect you exactly against the same threats



Why me ?

- I am not an expert on those topics
- There are much more talented people in the IT department
- But they do not protect you exactly against the same threats



Why those workshops ?

- To fight against a growing set of state surveillance policies and take control of the technologies we use

Why those workshops ?

- To fight against a growing set of state surveillance policies and take control of the technologies we use
- To be able to choose what we share and when

Why those workshops ?

- To fight against a growing set of state surveillance policies and take control of the technologies we use
- To be able to choose what we share and when
- To fight also surveillance from private companies who can sell collected data for money, or your employer who can possibly use collected data against you.

Why those workshops ?

- To fight against a growing set of state surveillance policies and take control of the technologies we use
- To be able to choose what we share and when
- To fight also surveillance from private companies who can sell collected data for money, or your employer who can possibly use collected data against you.
- To protect the people we communicate to

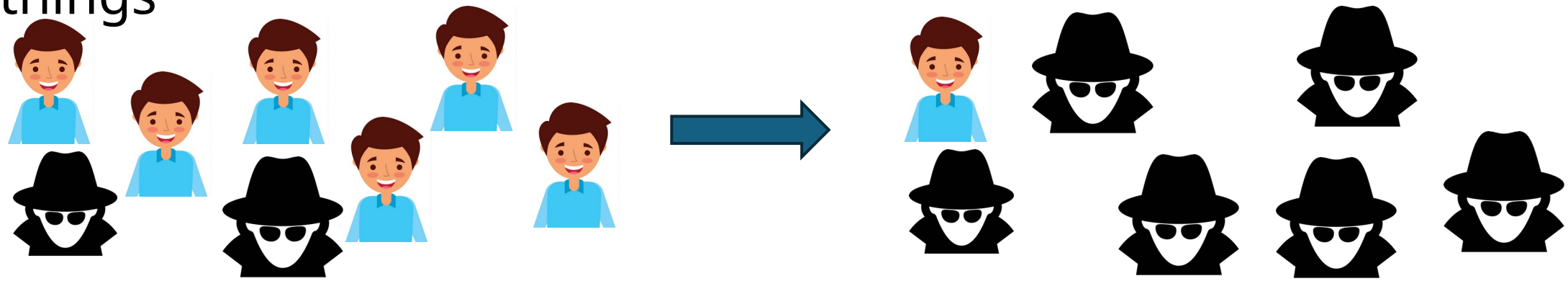
Why those workshops ?

- To fight against a growing set of state surveillance policies and take control of the technologies we use
- To be able to choose what we share and when
- To fight also surveillance from private companies who can sell collected data for money, or your employer who can possibly use collected data against you.
- To protect the people we communicate to
- To be able to talk about safety without simply excluding people based on their nationalities

Why those workshops ?

"Actually, the data I am sharing is not very sensitive,
I do not mind other people seeing it"

- Even if we do not think to have sensitive data, some people have, and the more spread-out privacy is, the harder it is to find out who is actually hiding sensitive informations.
- This is why you should push for everyone to use privacy tools, and use them even for the most apparently irrelevant things



general security advises (and disclaimer: we are not going to see all of those things in details today)

- Use Tor for browsing anonymously (covered in a future workshop)
- Try to lean towards open source softwares in your tools choices (and if you have not already, consider switching to linux ! -> separate workshop to install it if you want)
- Keep all your softwares up to date
- Encrypt your external drives too with Veracrypt (this will be covered later)
- Use Tails (covered in a future workshop)
- Activate Password lock on your phones, and encrypt your sd cards if you have one
- Consider your phone less secure
- Consider mails very unsafe ! Use Signal to communicate with other people (If you do not want to use a smartphone, you can still install signal on a computer, there is a separate optional workshop available !)
- Keep an eye on your devices: physical access without you knowing can be dramatic
- Backup your datas in encrypted backups -> separate workshop to do it if you want

Having a strong password

- We should always use a password identification at the very least on every device.
- Do not activate fingerprint, faceID, or quick pattern drawing as identification on your devices. If the police have you and your device, they can force you to open them.
- You need a password m trong passw ssXC, it is open source and cross it locally and oud.
- What matters is to hav ord that you ows, and all the other password ly generated manager.
- Pay a special attention of your mail d for password reset

- Automatically generated passwords are also easier to share when needed, as opposed to the one weak password that you use everywhere

How to generate it?

- We should use the DiceWare method:
  - Using a D20
  - We roll it three times
  - We take the corresponding word in the word list
  - We repeat the operation 6 times
  - Our password is those 6 words separated by spaces
  - No need to have capital letters or special characters

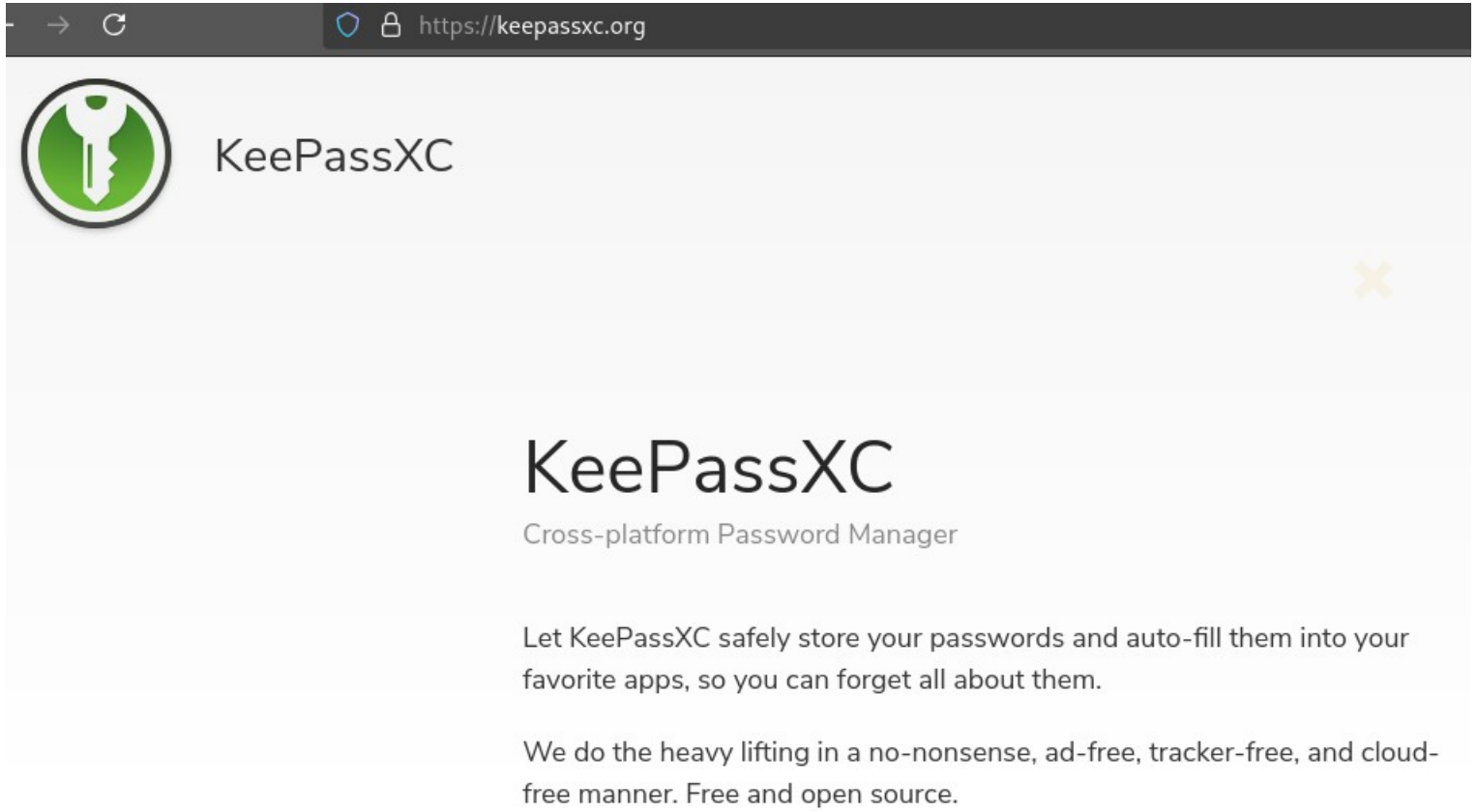
You can find the list of words, and an offline generator, In wiki.estaca.net, then click on The diceware method


```
1-1-1 aided
1-1-2 child
1-1-3 foul
1-1-4 four
1-1-5 woods
1-1-6 sleep
1-1-7 hanging
1-1-8 captain
1-1-9 saved
1-1-10 bestowing
1-1-11 demotes
1-1-12 disobeying
1-1-13 opulence
1-1-14 uscru
1-1-15 presents
1-1-16 fingernails
1-1-17 bike
1-1-18 under
1-1-19 lord
1-1-20 pride
1-2-1 speeder
1-2-2 lure
1-2-3 lack
```

```
1-2-10 blasters
1-2-11 gunray
1-2-12 vasp
1-2-13 month
1-2-14 bringing
1-2-15 encounter
1-2-16 starships
1-2-17 doubts
1-2-18 jacket
1-2-19 disfiguring
1-2-20 skills
1-3-1 cause
1-3-2 satchel
1-3-3 magnaguard
1-3-4 red
1-3-5 relics
1-3-6 sub-chamber
1-3-7 inaction
1-3-8 stuns
1-3-9 commented
1-3-10 plaza
1-3-11 parted
1-3-12 irises
```

KeepassXc

The password manager that I personally use

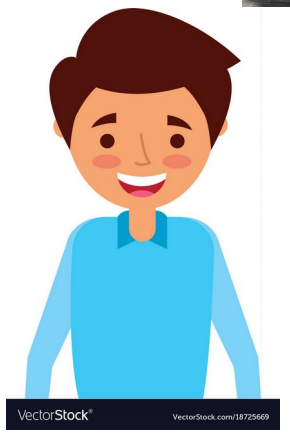


If you do not have any, or only use the one from google or Microsoft, I suggest you start a database With KeepassXc, with the passphrase you just generated

What is End To End Encryption?

- This is how you typically interact with someone:

server



What is End To End Encryption?

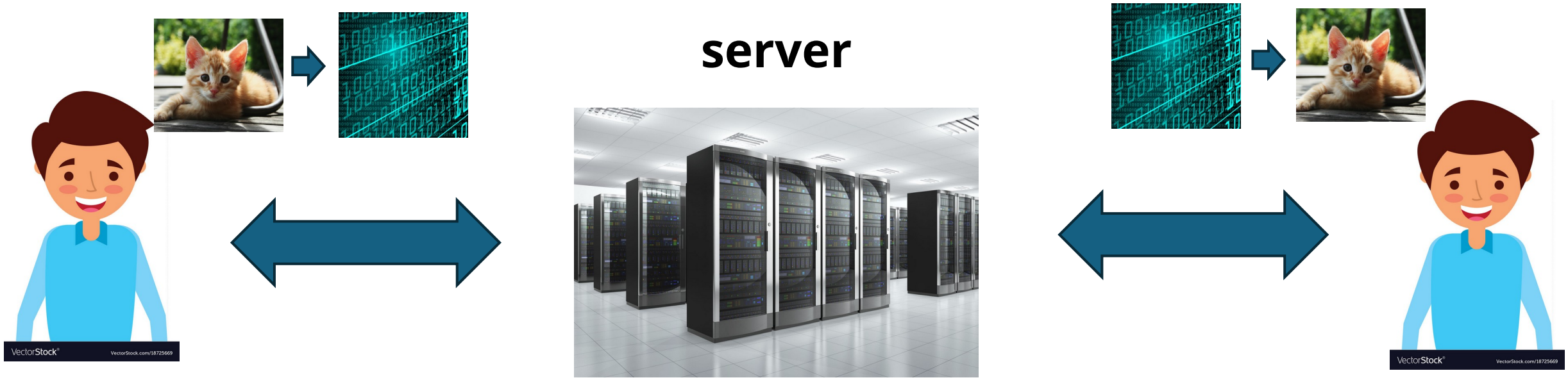
- The entity that administrates the server can see everything that passes by.
- If it is your employer, it can use this to repress you
- If it is a private company it can sell informations to other ones
- In any case most server administrators will collaborate with the police if asked to

server

What is End To End Encryption?

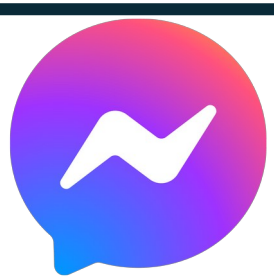
- End To End encryption means encrypting your data before sending it to the server, and the receiver would receive it and decrypt it after fetching the encrypted data from the server

  Note: usually, with simply End To End encryption, it is still easy to know who is talking to who



What is End To End Encryption?

Some services are already End to End encrypted and easy to use



(Careful about those two: they are proprietary and steal a lot of metadata)

What is End To End Encryption?

Some have a reputation of security but do not deserve it, as they are not end to end encrypted

You can also do E2EE manually yourself !

1) encrypt your files in your computer in an encrypted folder

2) Send it using a cloud storage for example (since those are encrypted data, you do not have to worry about how safe is this cloud storage)

3) Send the password with Signal

4) The receiver will decrypt it on his computer

How to encrypt/decrypt ?

- Today we are going to try two open source softwares that can do it:
  - Veracrypt (https://veracrypt.fr)

  - Cryptomator (https://cryptomator.org)

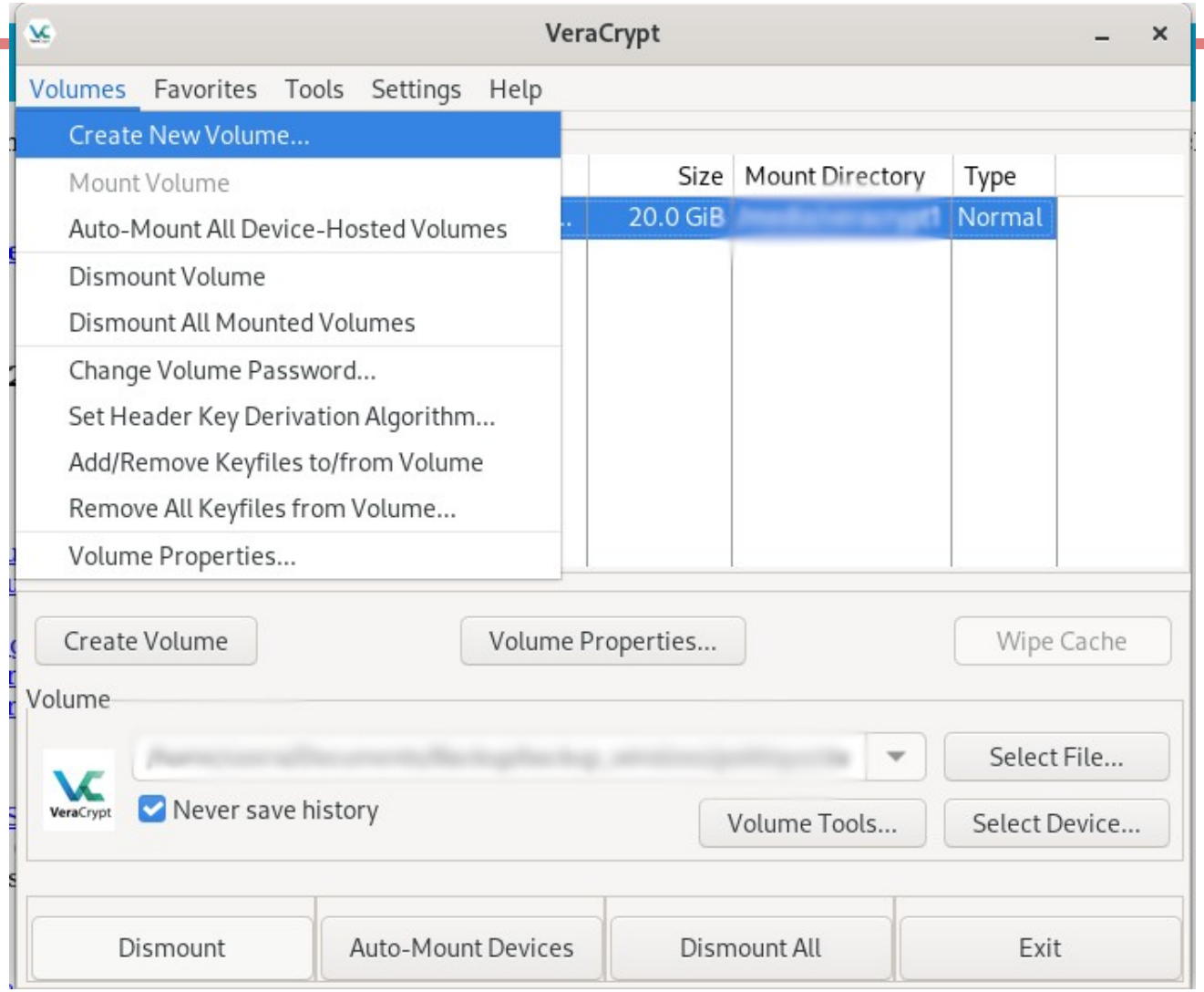
Both are cross platform: they can be used on Windows, Mac, Linux, Android, ...

Veracrypt

- Start by downloading and installing it: https://veracrypt.fr/en/Downloads.html

Veracrypt

- Then let's create a volume



Veracrypt

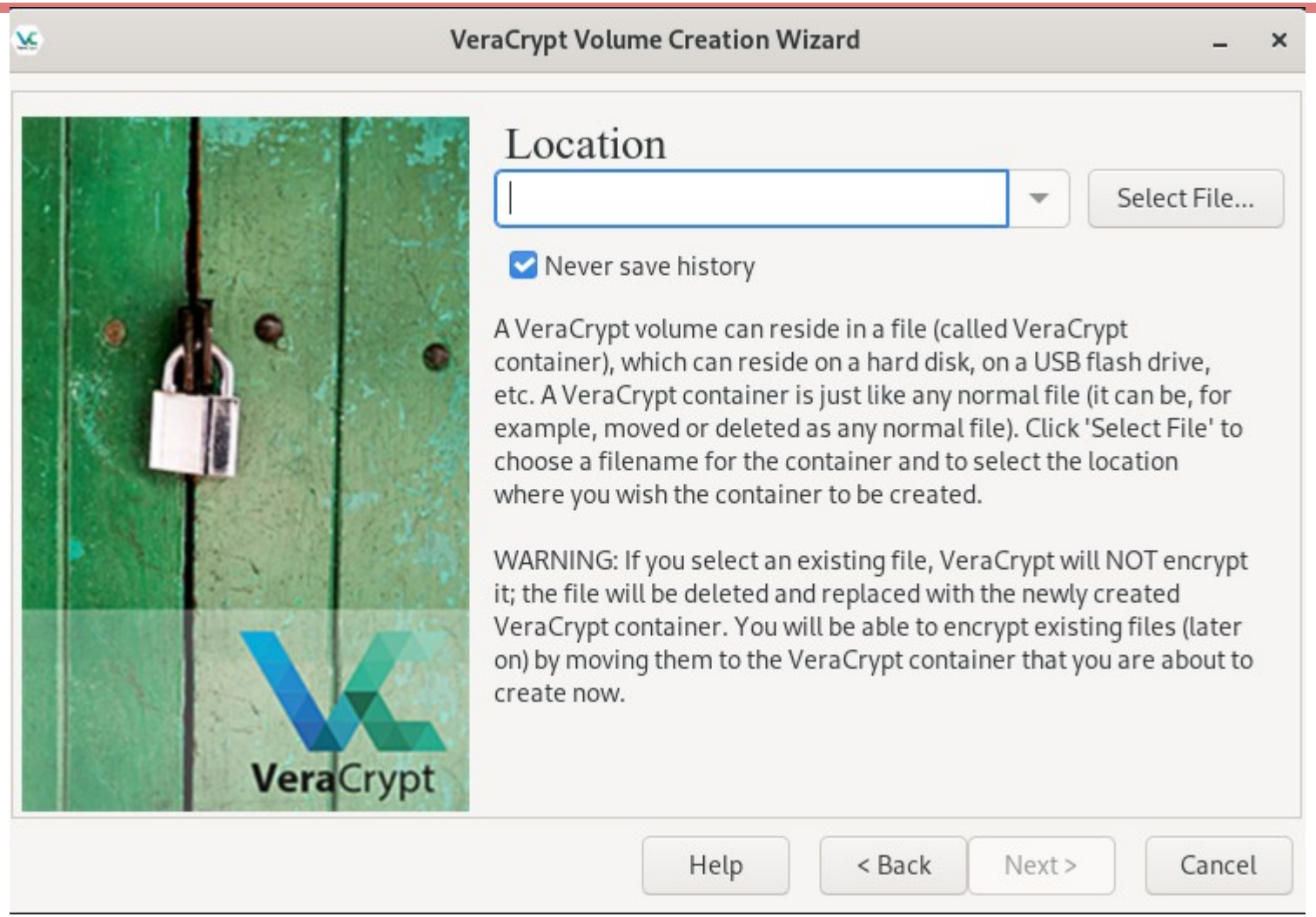
- Then let’s create a volume

Veracrypt

- Then let's create a volume

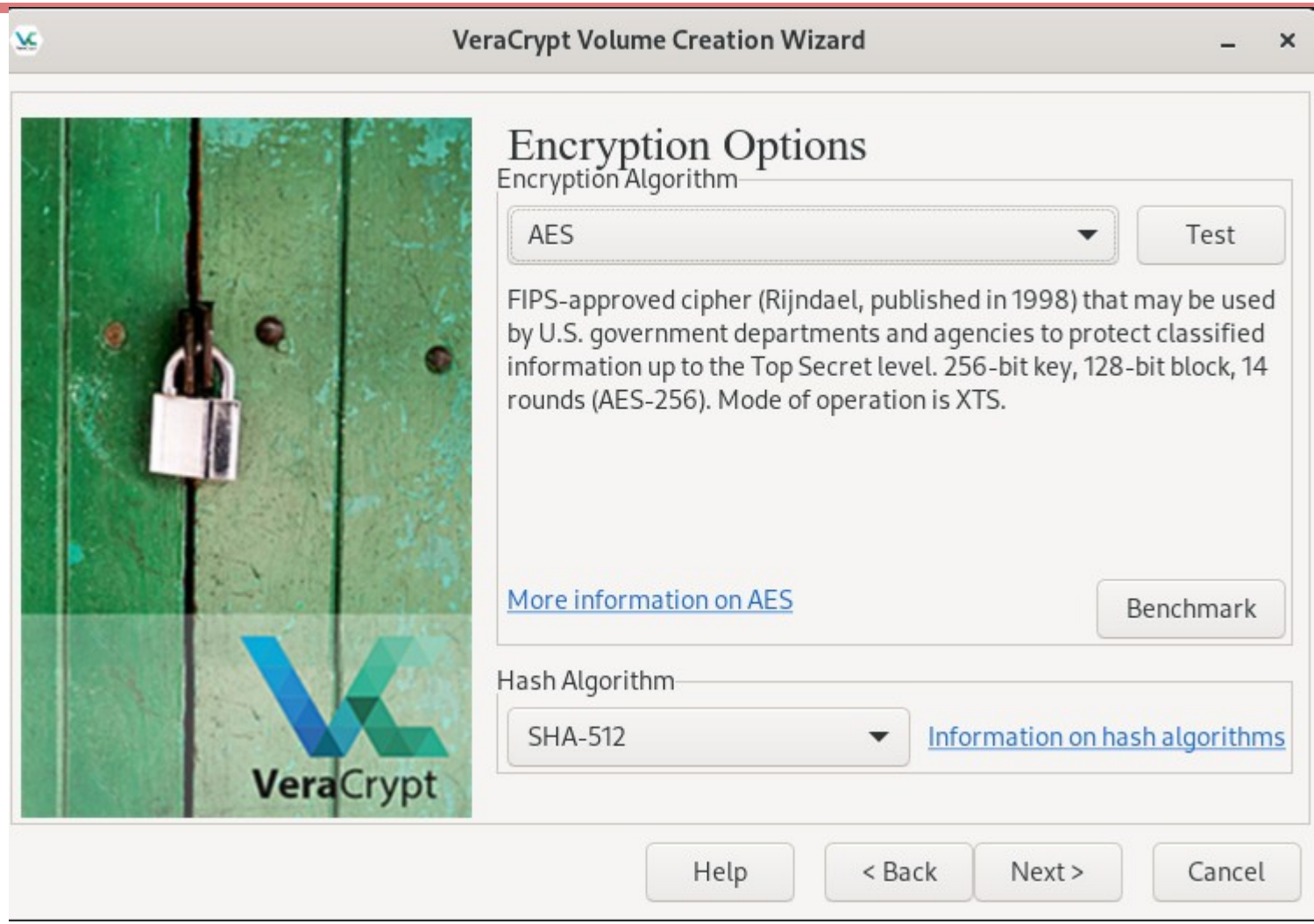
Veracrypt

- Then let’s create a volume



Veracrypt

- Then let’s create a volume



Veracrypt

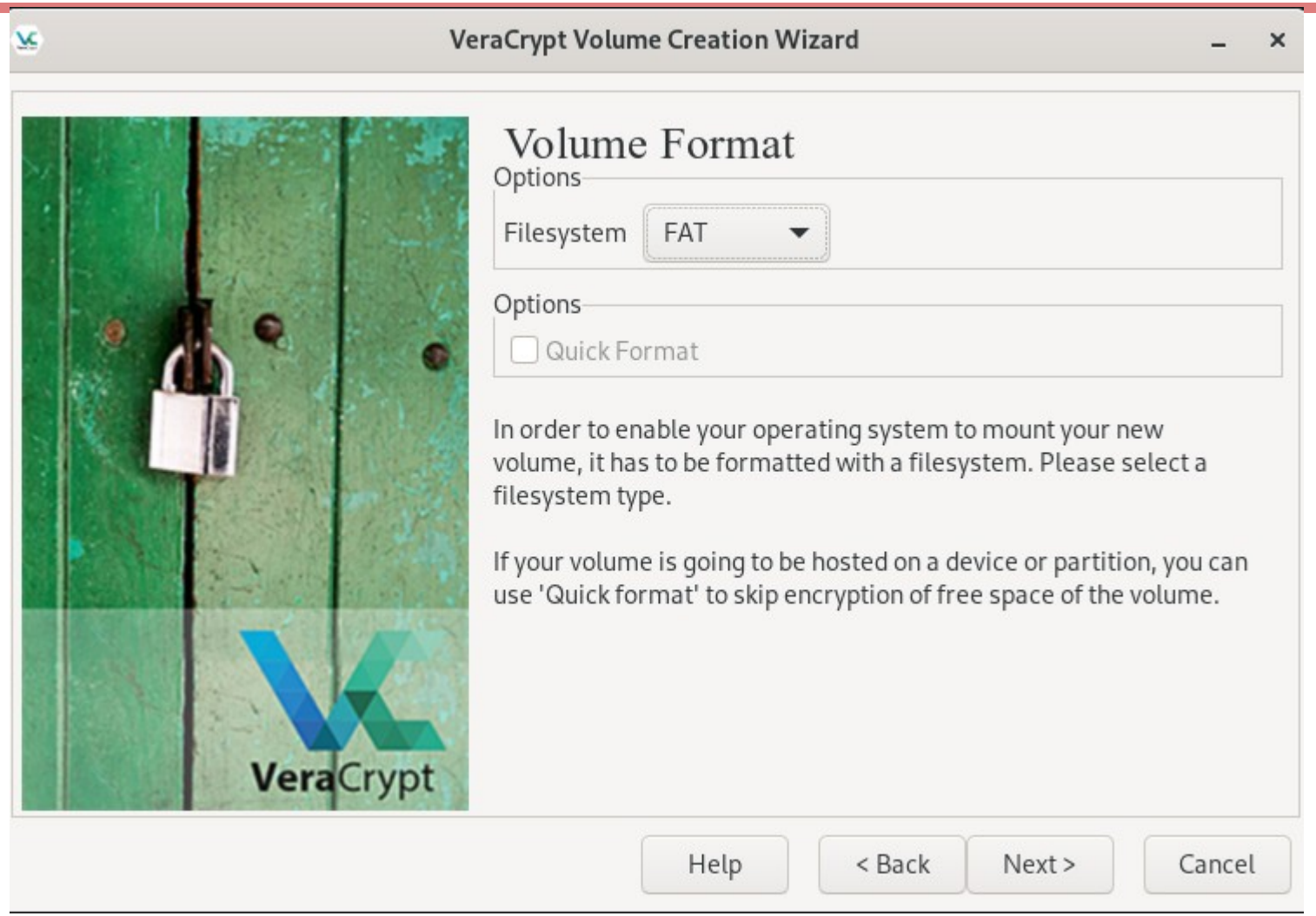
- Then let’s create a volume

Veracrypt

- Here you enter your strong passphrase (or a randomly generated password from a password manager)

Veracrypt

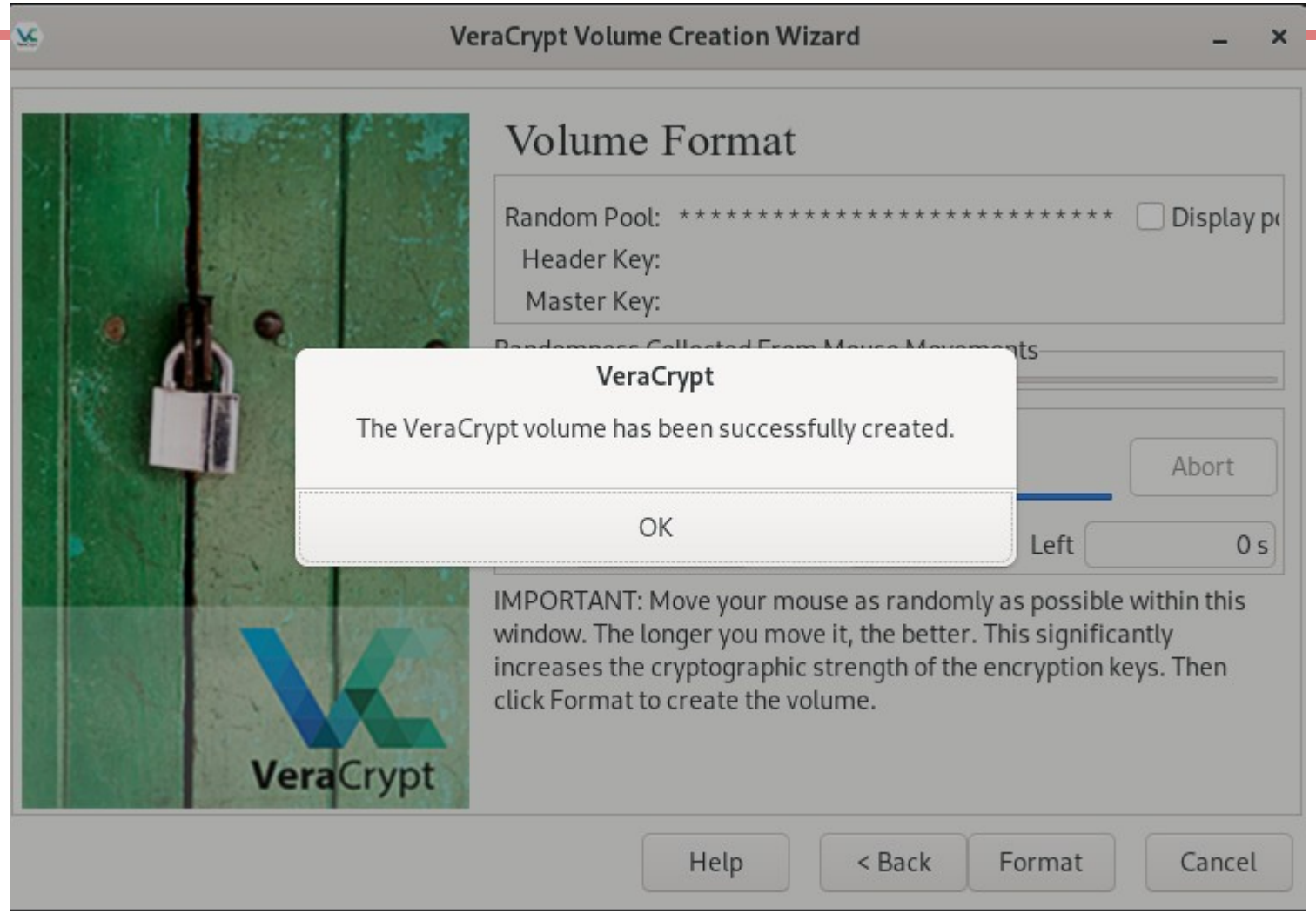

digital SAFETY
IS
SPELLED
WITHOUT
AN
R


VeraCrypt Volume Creation Wizard
Volume Format
Options
Filesystem
FAT
Options
Quick Format
In order to enable your operating system to mount your new volume, it has to be formatted with a filesystem. Please select a filesystem type.
If your volume is going to be hosted on a device or partition, you can use 'Quick format' to skip encryption of free space of the volume.
VeraCrypt
Help
< Back
Next >
Cancel

Veracrypt

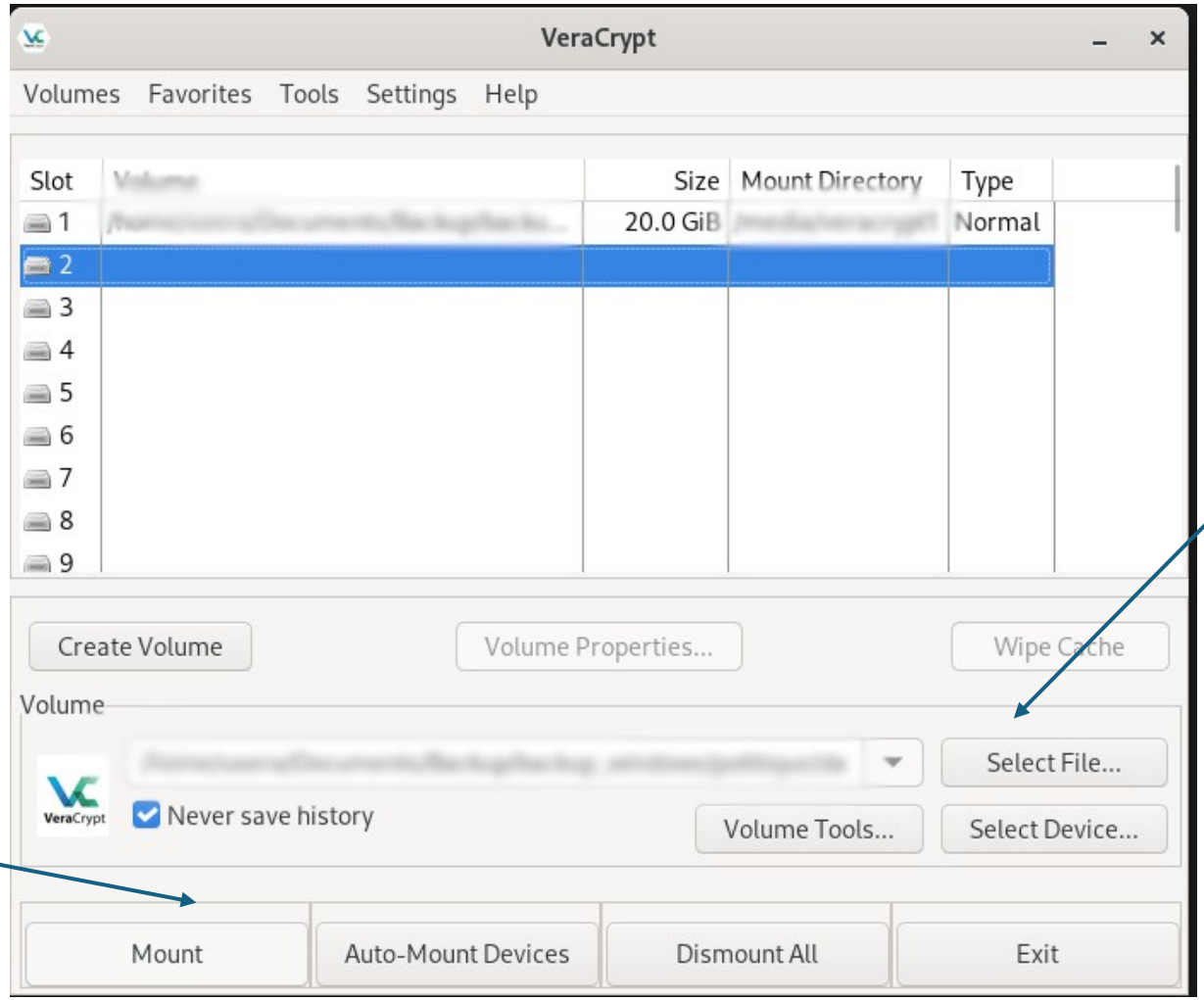
- Here you just move your mouse randomly until you have a lot of “randomness”

Veracrypt


VeraCrypt Volume Creation Wizard
Volume Format
Random Pool:
Header Key:
Master Key:
Display p
VeraCrypt
The VeraCrypt volume has been successfully created.
OK
Abort
Left
0 s
IMPORTANT: Move your mouse as randomly as possible within this window. The longer you move it, the better. This significantly increases the cryptographic strength of the encryption keys. Then click Format to create the volume.
VeraCrypt
Help
< Back
Format
Cancel

Veracrypt

1) Select a slot here



2) Find the encrypted file you just created

3) Mount it

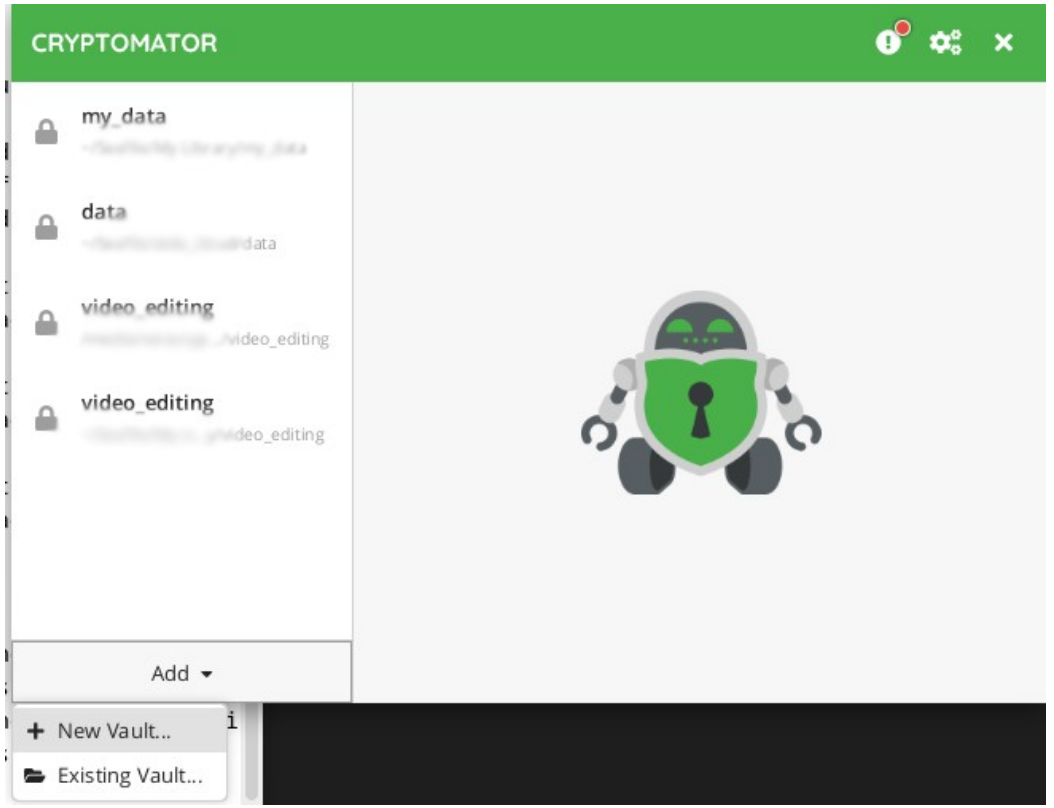
Veracrypt

- That’s it ! Your encrypted folder is now decrypted and you can add things inside, then click on unmount and you can share it safely

Cryptomator

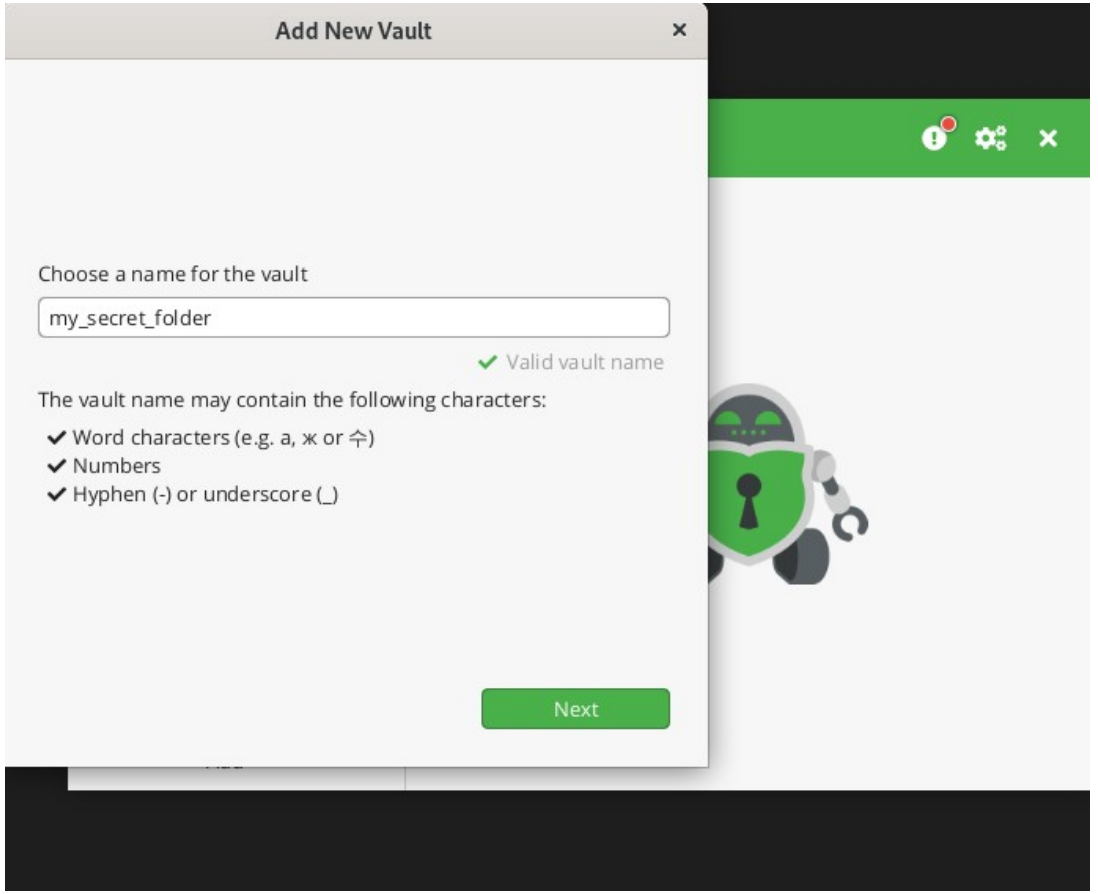
- First you download and install it: https://cryptomator.org/downloads
- Then let's create a container,

or "vault"



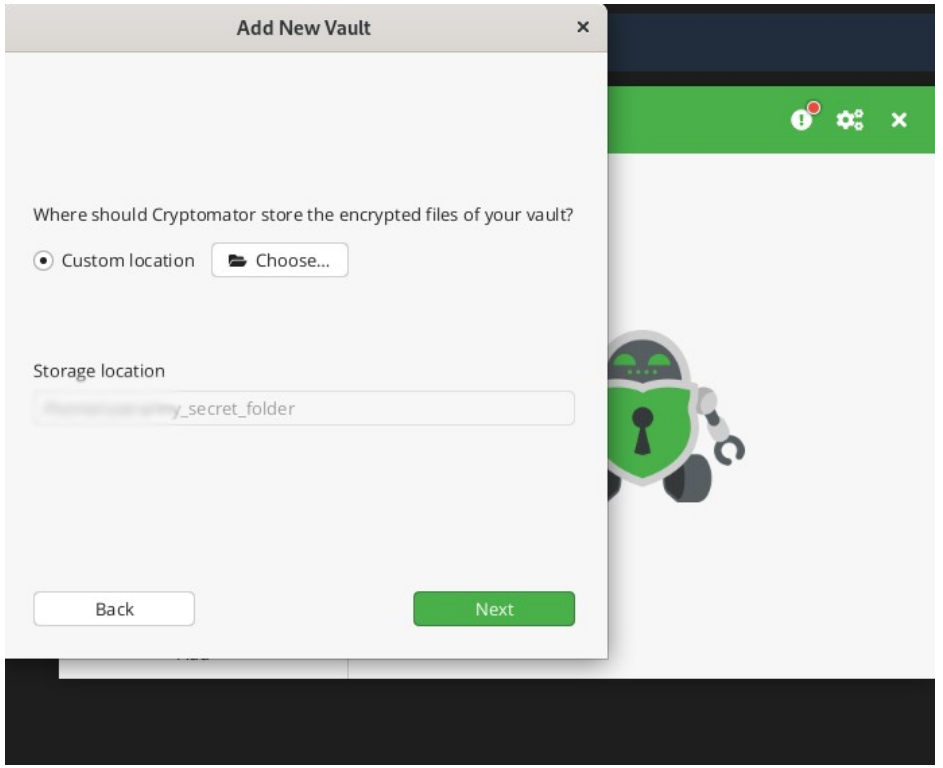
Cryptomator

- Then let’s create a container, or “vault”

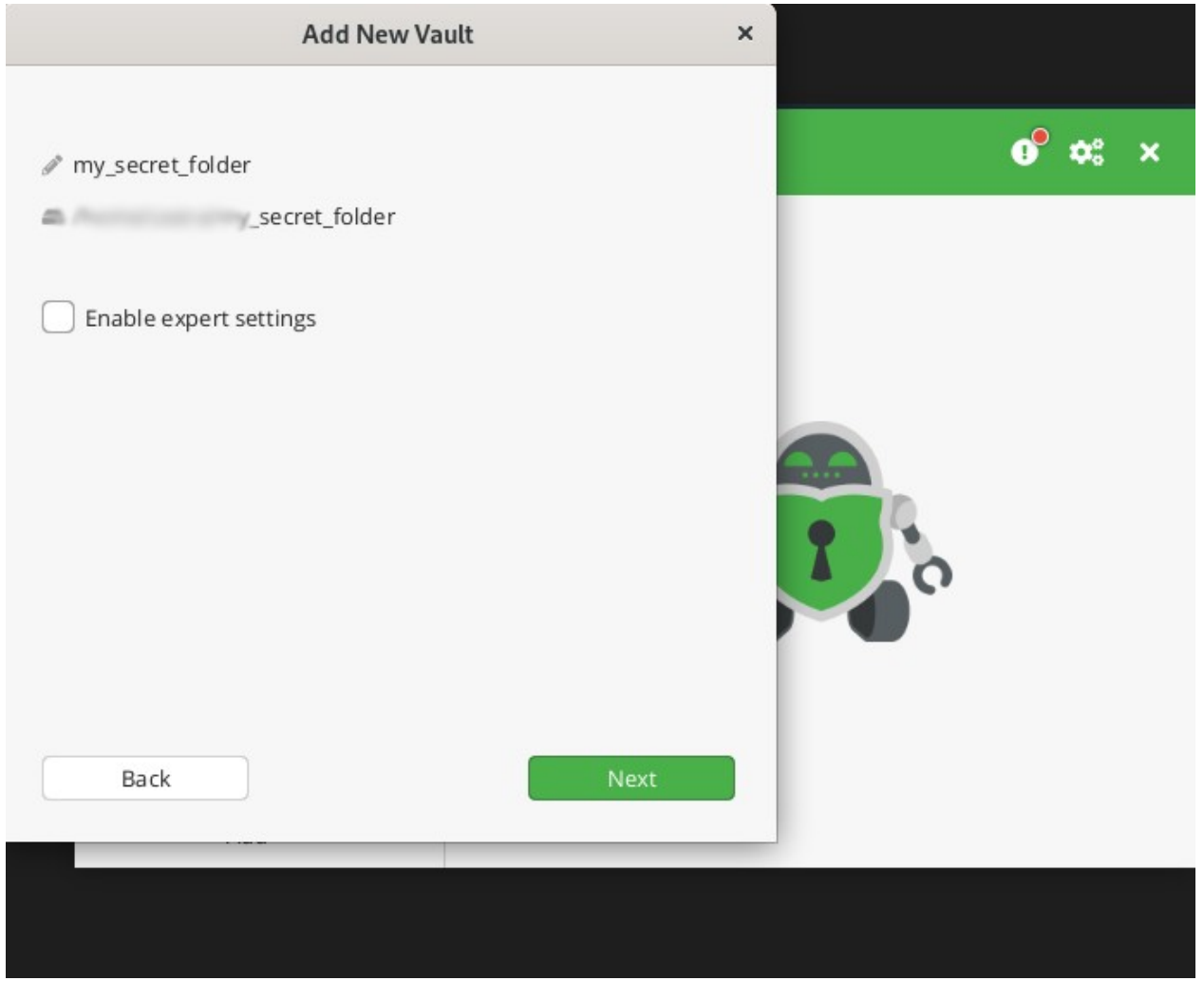


Cryptomator

- Choose the location of the Encrypted folder

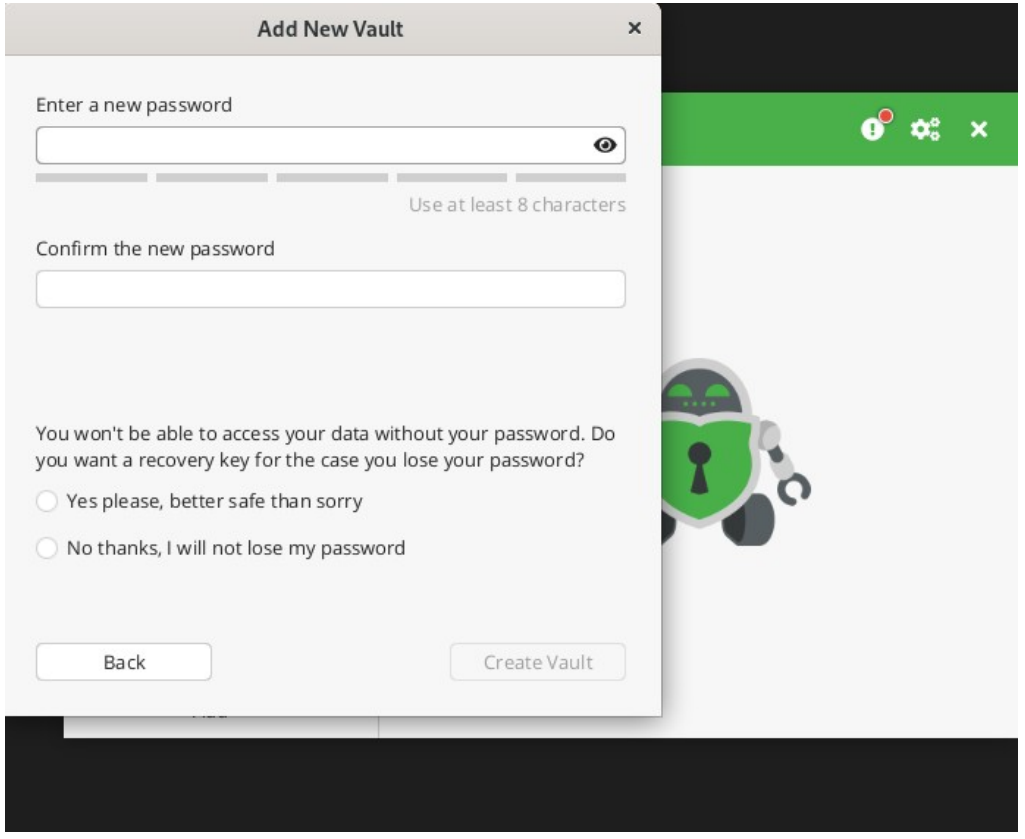


Cryptomator

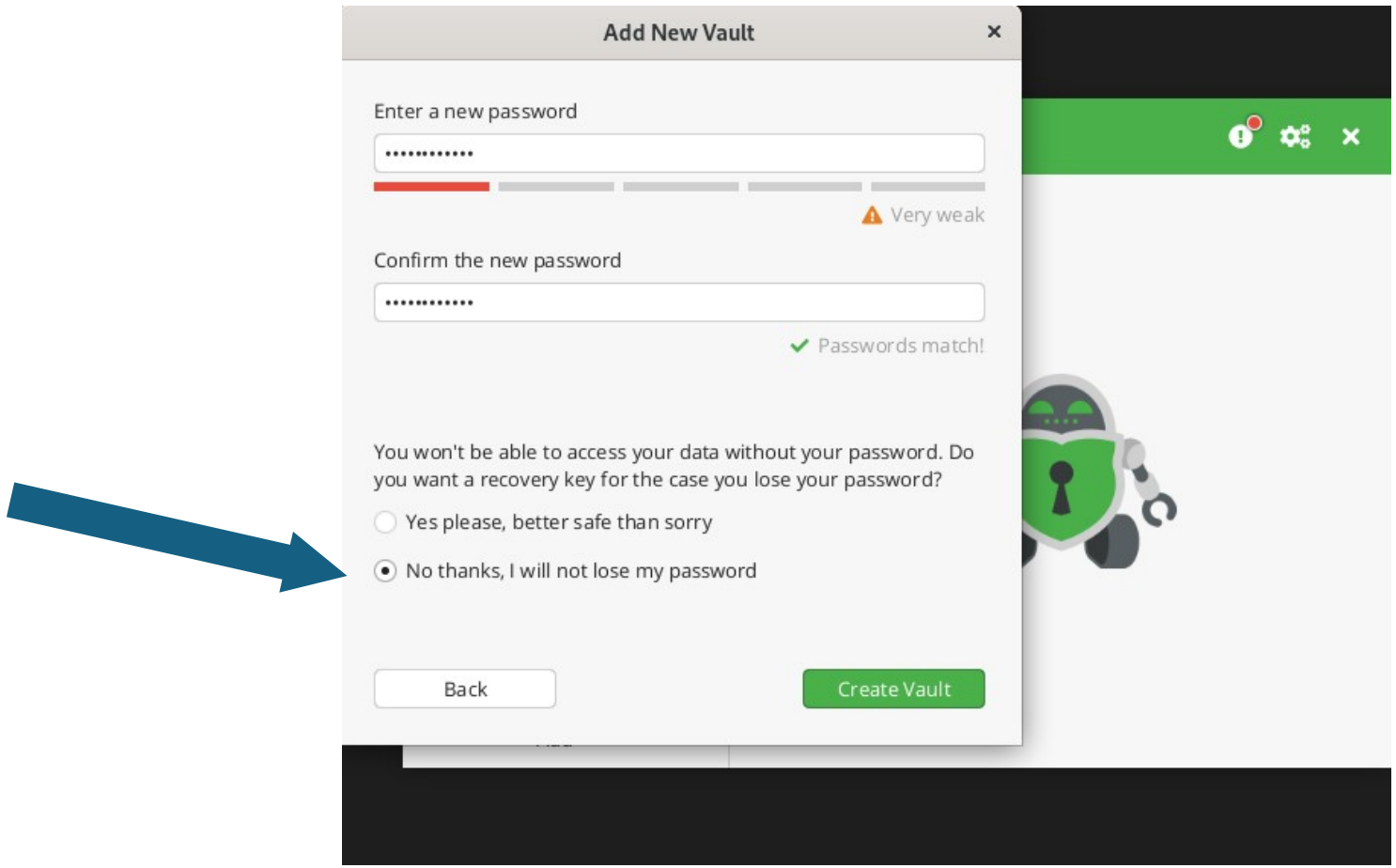


Cryptomator

Here goes your 6 words strong
Passphrase or a randomly generated
Passphrase in a password manager

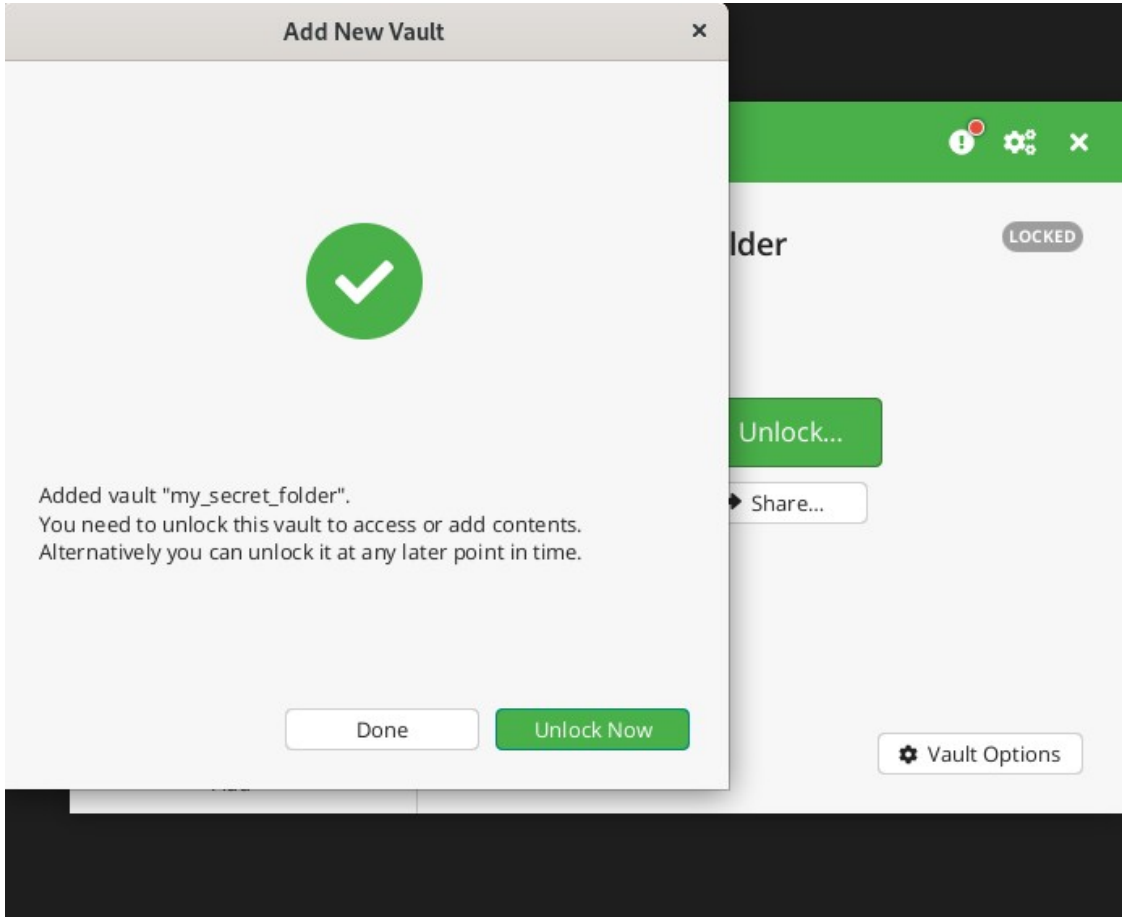


Cryptomator



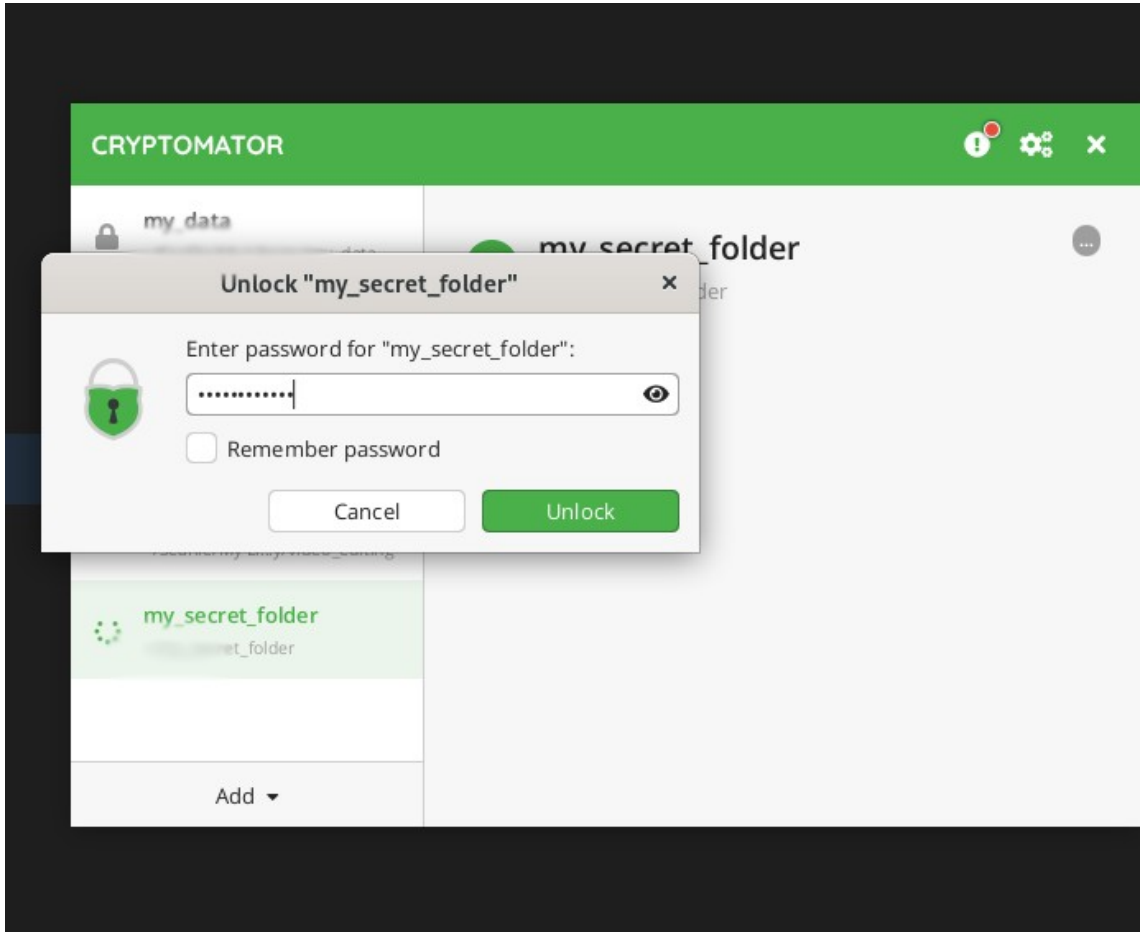
Cryptomator

Click on “Unlock Now”



Cryptomator

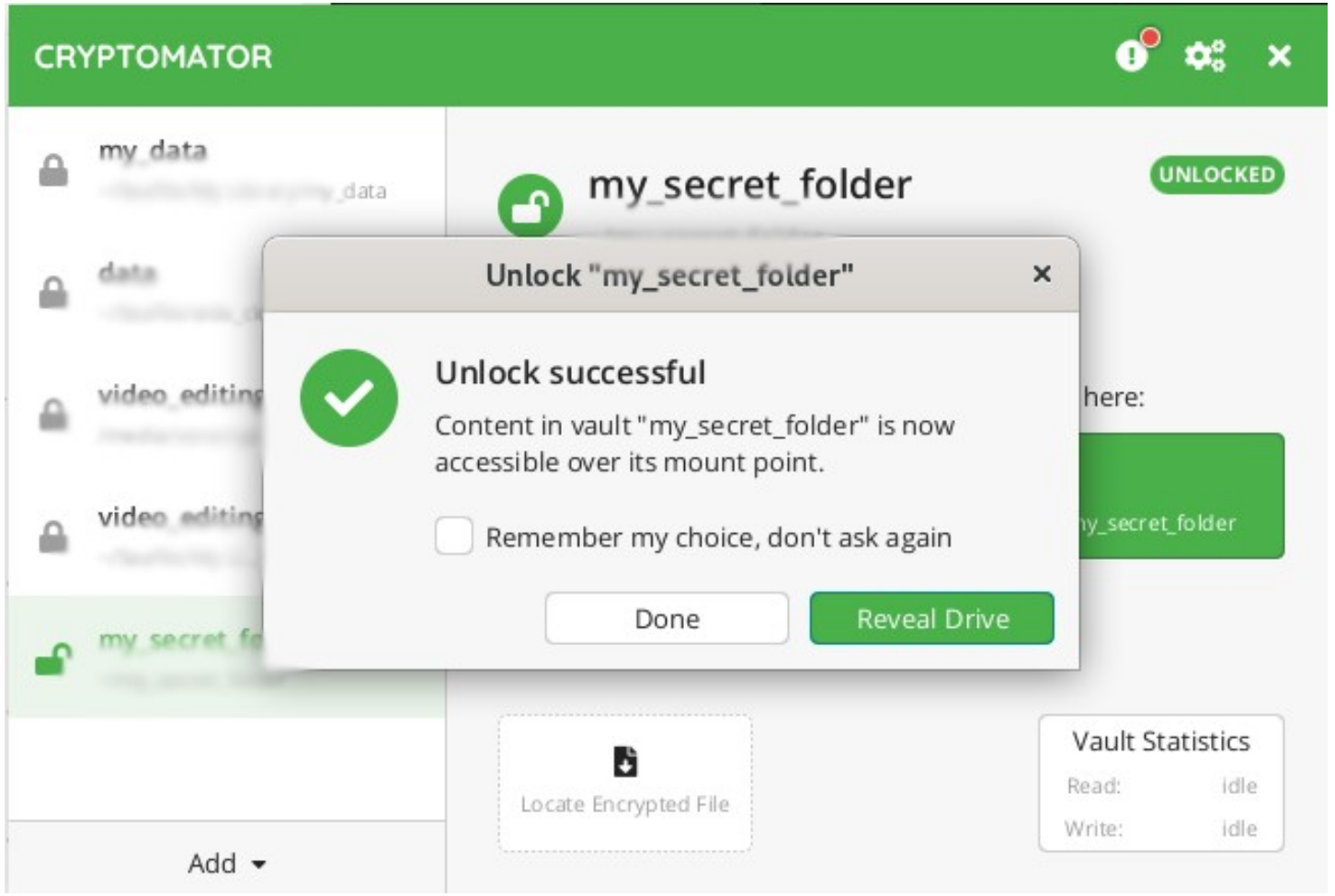
Enter your password and then “Unlock”



Cryptomator

Then “Reveal Drive”.

You are all set, you can put things inside your folder and then lock it and share it, using for example a cloud storage.



Full Disk Encryption

- What about the data on your device? If the Police for example seize it ?
- This is why you ALSO need to implement Full Disk Encryption. When you do that, all the data in your device (computer, phone, USB key, …) are encrypted and cannot be accessed by someone who has a physical access to your device

What is Full Disk Encryption?

- If you do not do anything specific, your hard drive is nothing different from a normal USB key: anyone who gets a physical access to it can access all the datas

contains

don’t think that because you need a password to open your windows session, the data inside are protected. They are protected when you computer is ON, but if you turn if off, you are back to the stage of something as easy to access as a USB key

What is Full Disk Encryption?

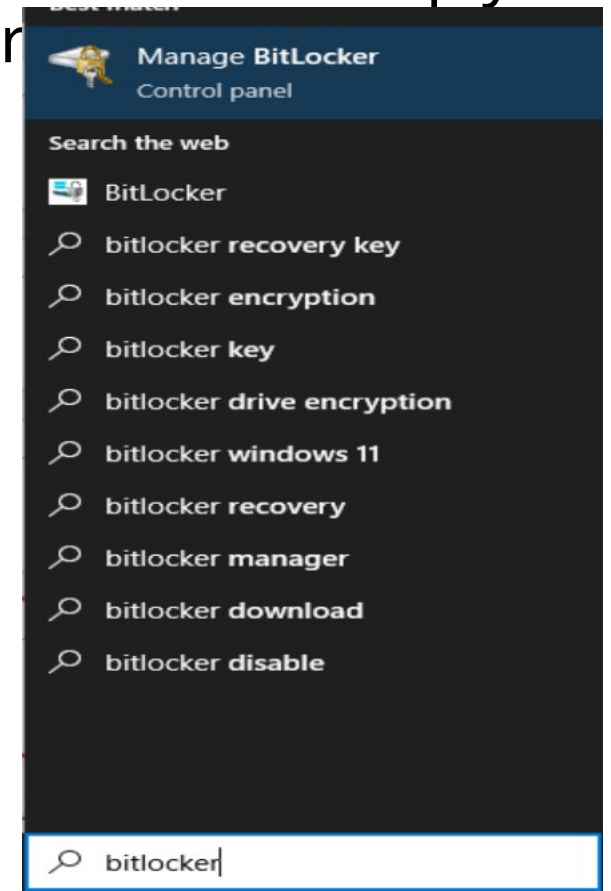
- Full disk encryption means encrypting all the data on your disk, so that without a password, you cannot access them

contains

the key is necessary to recover the data

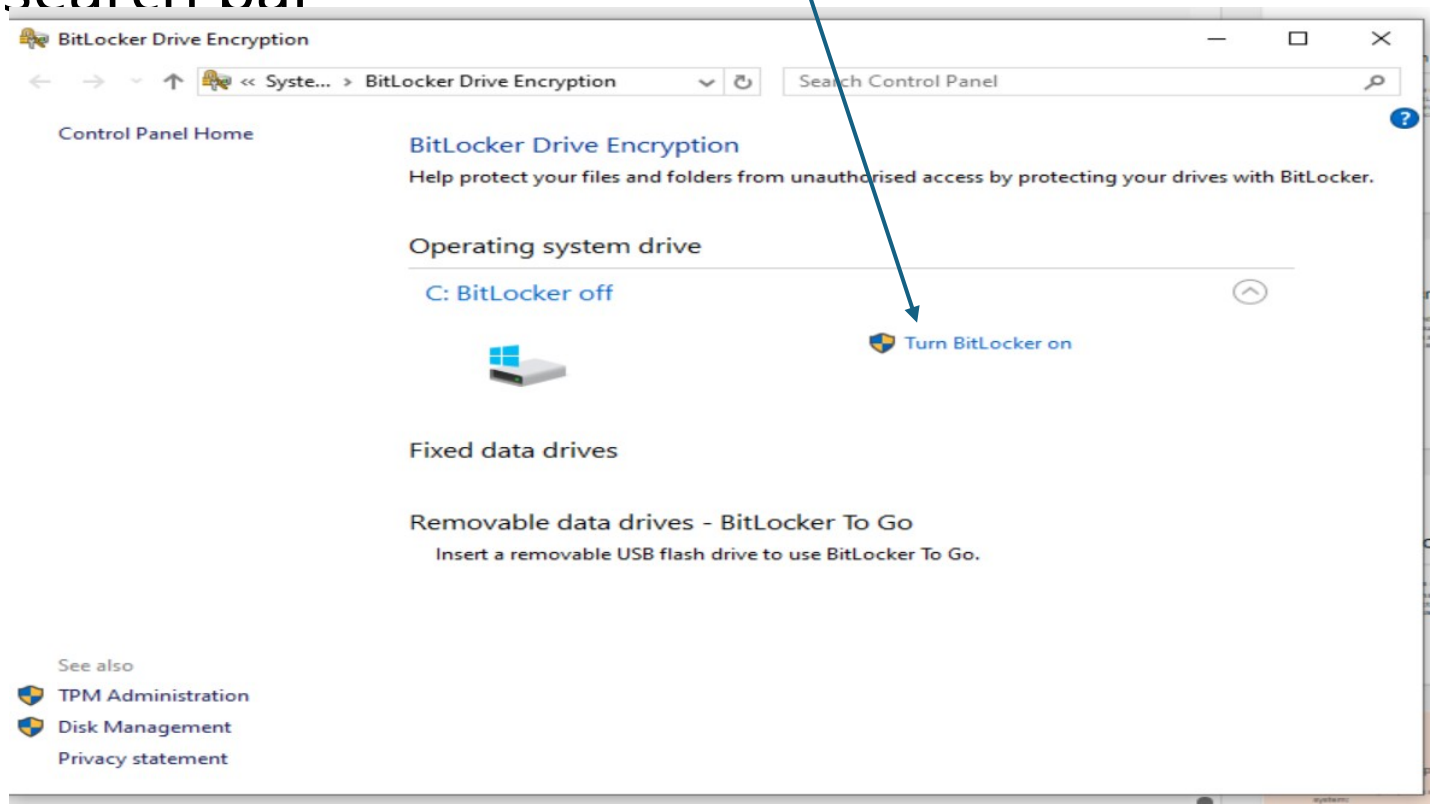
Full Disk Encryption

- How to set it up depends on your system:
  - On Windows, if you have BitLocker, it consists simply in activating it. Type “BitLocker” in the search bar



Full Disk Encryption

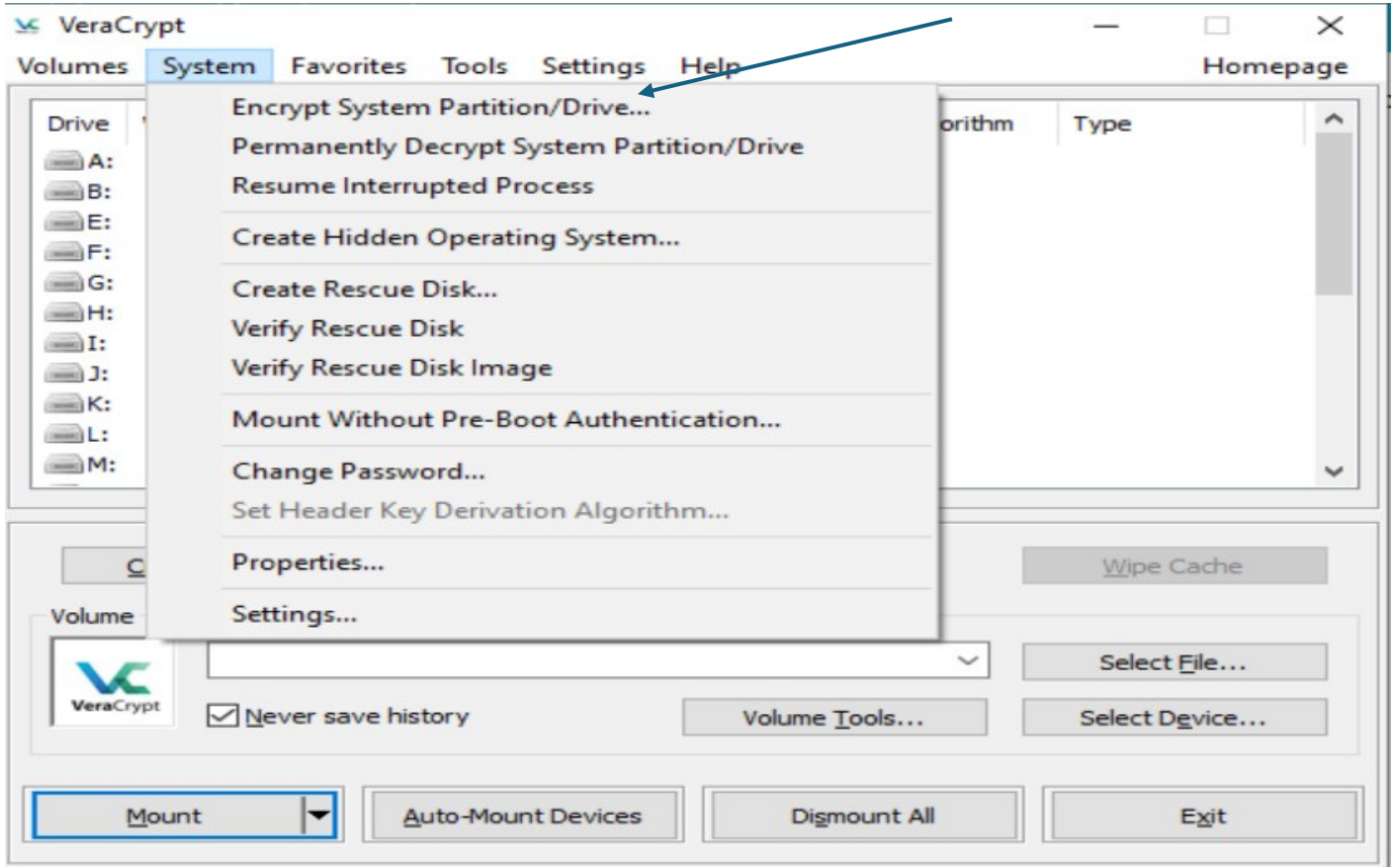
- How to set it up depends on your system:
  - On Windows, if you have BitLocker, it consists simply in activating it. Type “BitLocker” in the search bar



Some versions of Windows have also a system called “Device Encryption”. None is really better, but careful to not login with a Microsoft account when activating it and to select the option to save the recovery key locally.

Full Disk Encryption

- How to set it up depends on your system:
  - On Windows, if you do not have it, you can do it with Veracrypt



Full Disk Encryption

- On MacOS, you can use FileVault

Step 1

In System Settings, click Privacy & Security.

Step 2

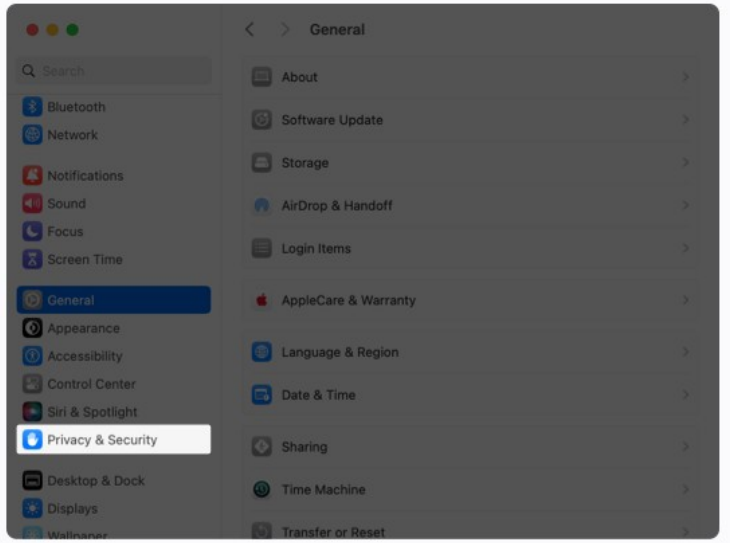
Scroll down to the Security section and click FileVault.

Step 3

Click Turn On.

Step 4

Enter an administrator's name and password,



Full Disk Encryption

- On MacOS, you can use FileVault

Step 2

Scroll down to the Security section and click FileVault.

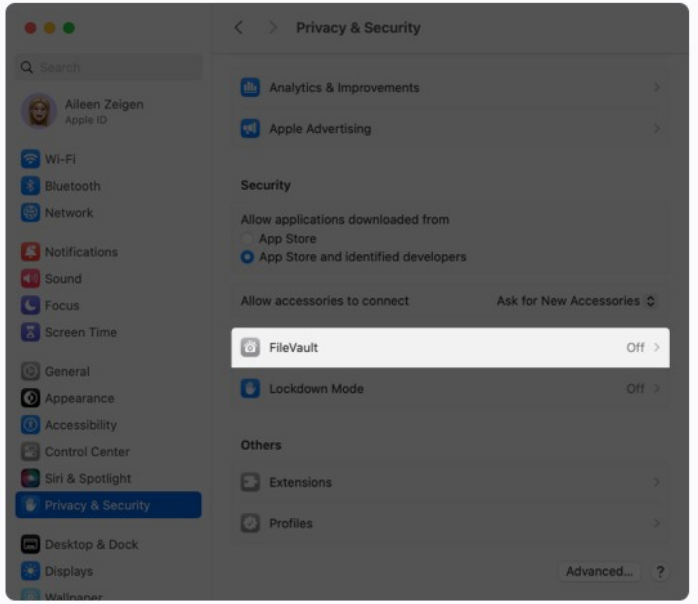
Step 3

Click Turn On.

Step 4

Enter an administrator's name and password, then click Unlock.

When you turn on FileVault, you can choose to use an iCloud account or a recovery key to unlock the disk.



Full Disk Encryption

- On MacOS, you can use FileVault

Step 3

Click Turn On.

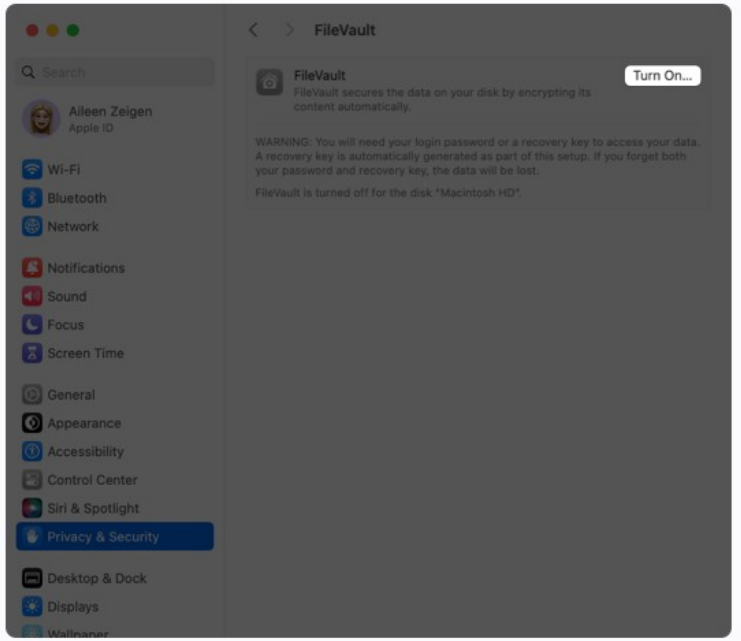
Step 4

Enter an administrator's name and password, then click Unlock.

When you turn on FileVault, you can choose to use an iCloud account or a recovery key to unlock the disk.

Step 5

Select "Create a recovery key and do not use my iCloud account," then click Continue.



Full Disk Encryption

- On MacOS, you can use FileVault

Step 4

Enter an administrator's name and password, then click Unlock.

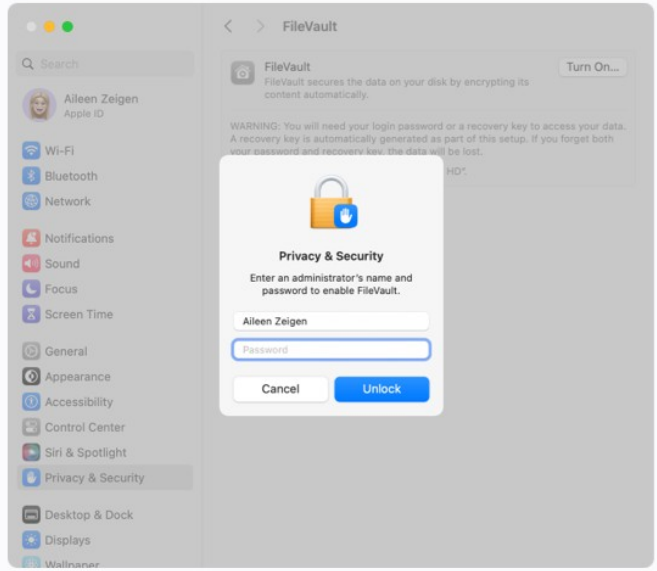
When you turn on FileVault, you can choose to use an iCloud account or a recovery key to unlock the disk.

Step 5

Select "Create a recovery key and do not use my iCloud account," then click Continue.

Note

If you previously set up iCloud on your Mac, the option "Allow my iCloud account to unlock my disk" appears. If you select that option, encryption starts automatically after you click Continue. When iCloud isn't set up, the option "Set up my iCloud account to reset my password" appears instead. If you select that option and then click Continue, you must sign in to your iCloud account to start encryption.



Full Disk Encryption

- On Linux, you can use LUKS. However this usually requires to format your computer. I can make a dedicated workshop about it, please reach out if you are a Linux user (and if you are concerned about safety, you should be one!)

Full Disk Encryption

- On your phone, activate the locked option of Signal to encrypt your Signal related data.

Encrypting a USB key

- Let us start with a simple case: encrypt a usb key
- There are many ways to do it, but here I will tell you a way that is ”cross platform”: you will be able to use the USB key on MacOS, Windows or Linux
- Let us first prepare the usb key partitions. The way to do this depends on your OS.

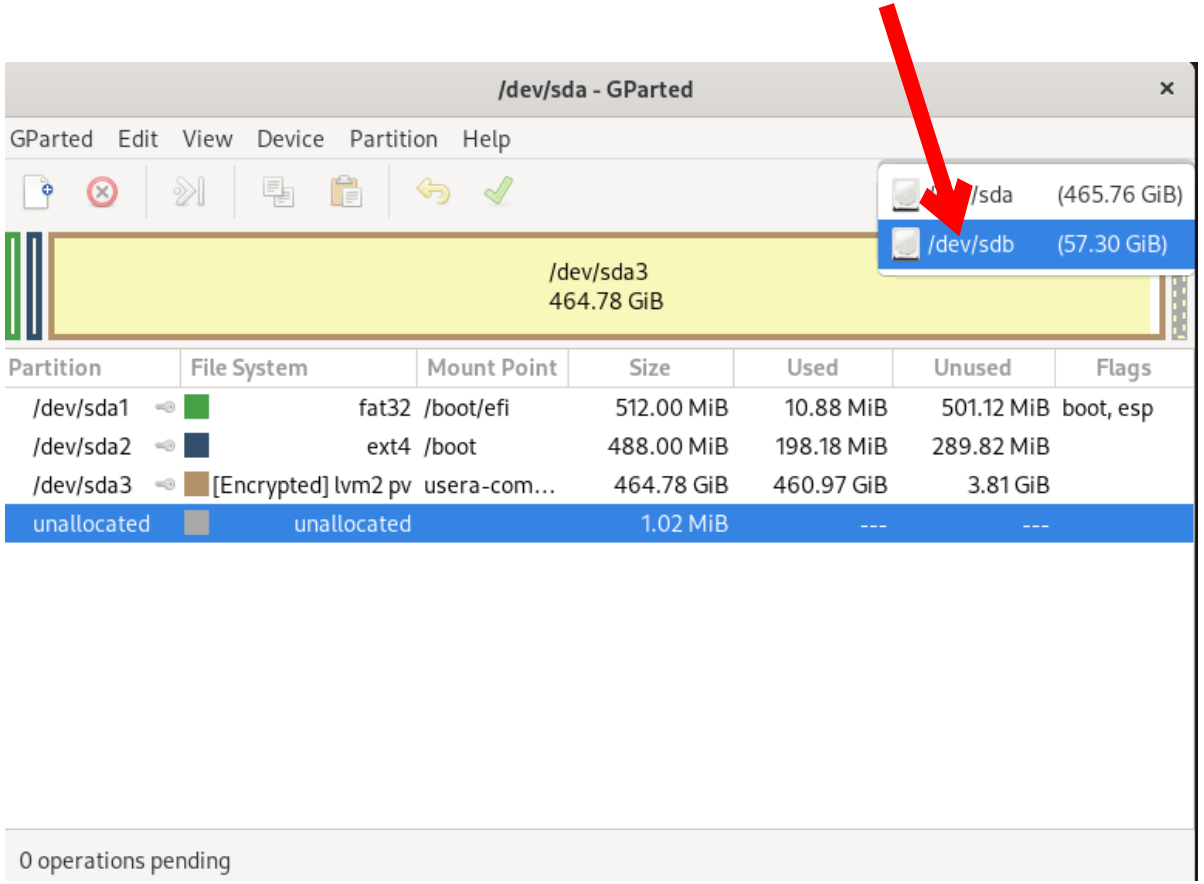
Encrypting a USB key

- Case of linux
- Start by installing the tool gparted:

”sudo apt install gparted”

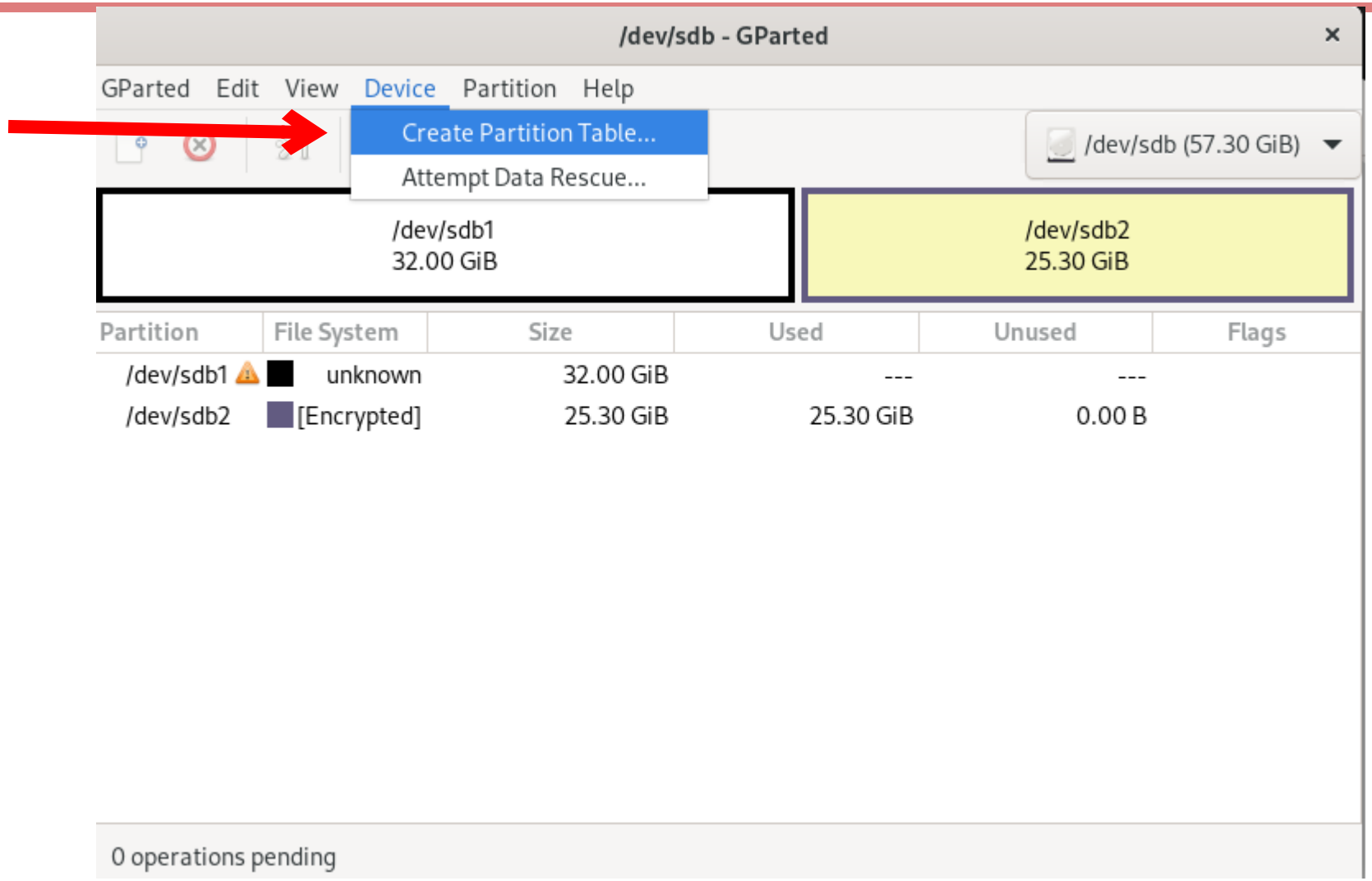
- Then launch it: ”sudo gparted”

choose your USB key (not your hard drive, this would destroy all you data !)



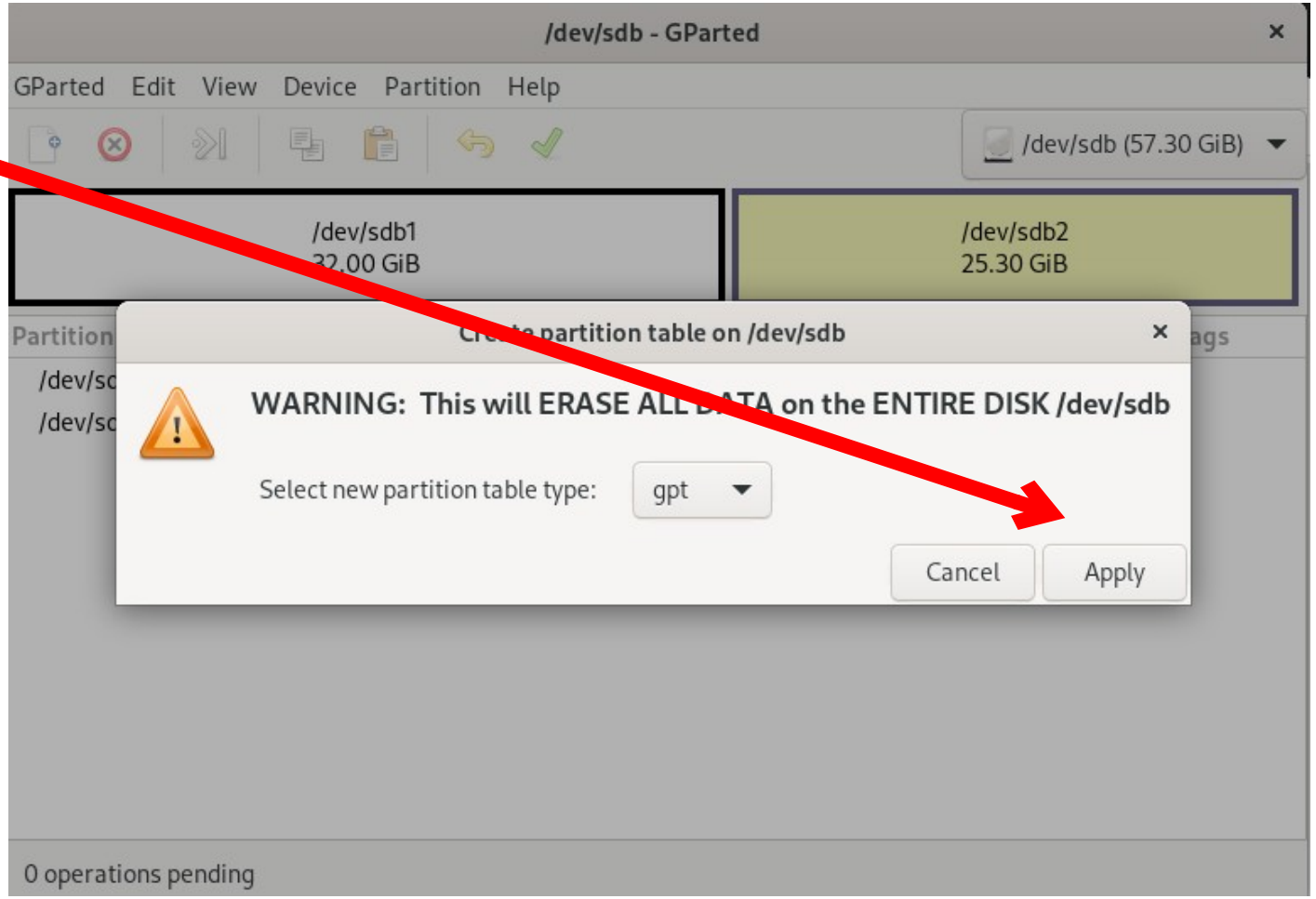
Encrypting a USB key

click here (careful, this will destroy forever all the data on the disk)



Encrypting a USB key

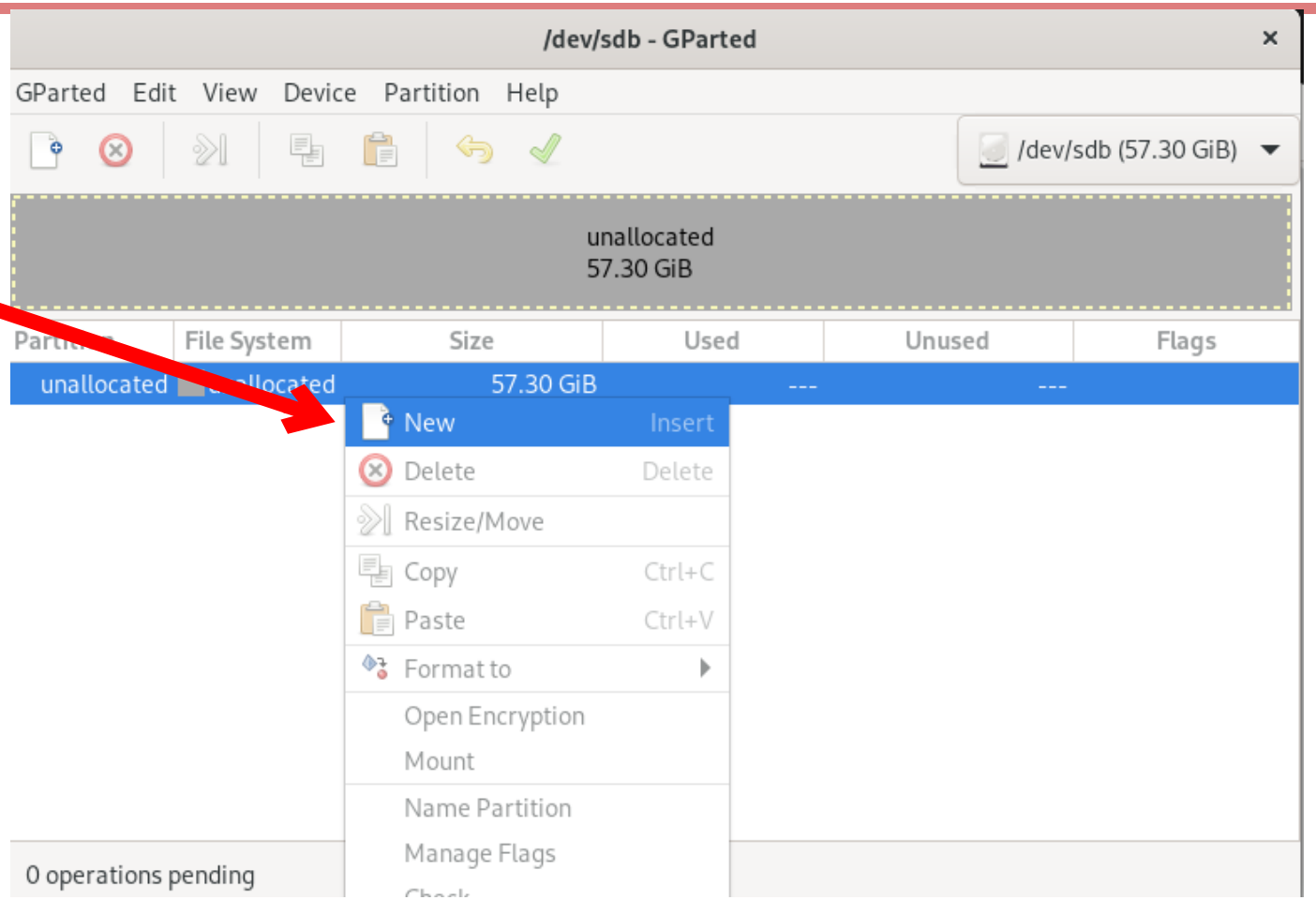
select ”gpt” and click on Apply



Encrypting a USB key

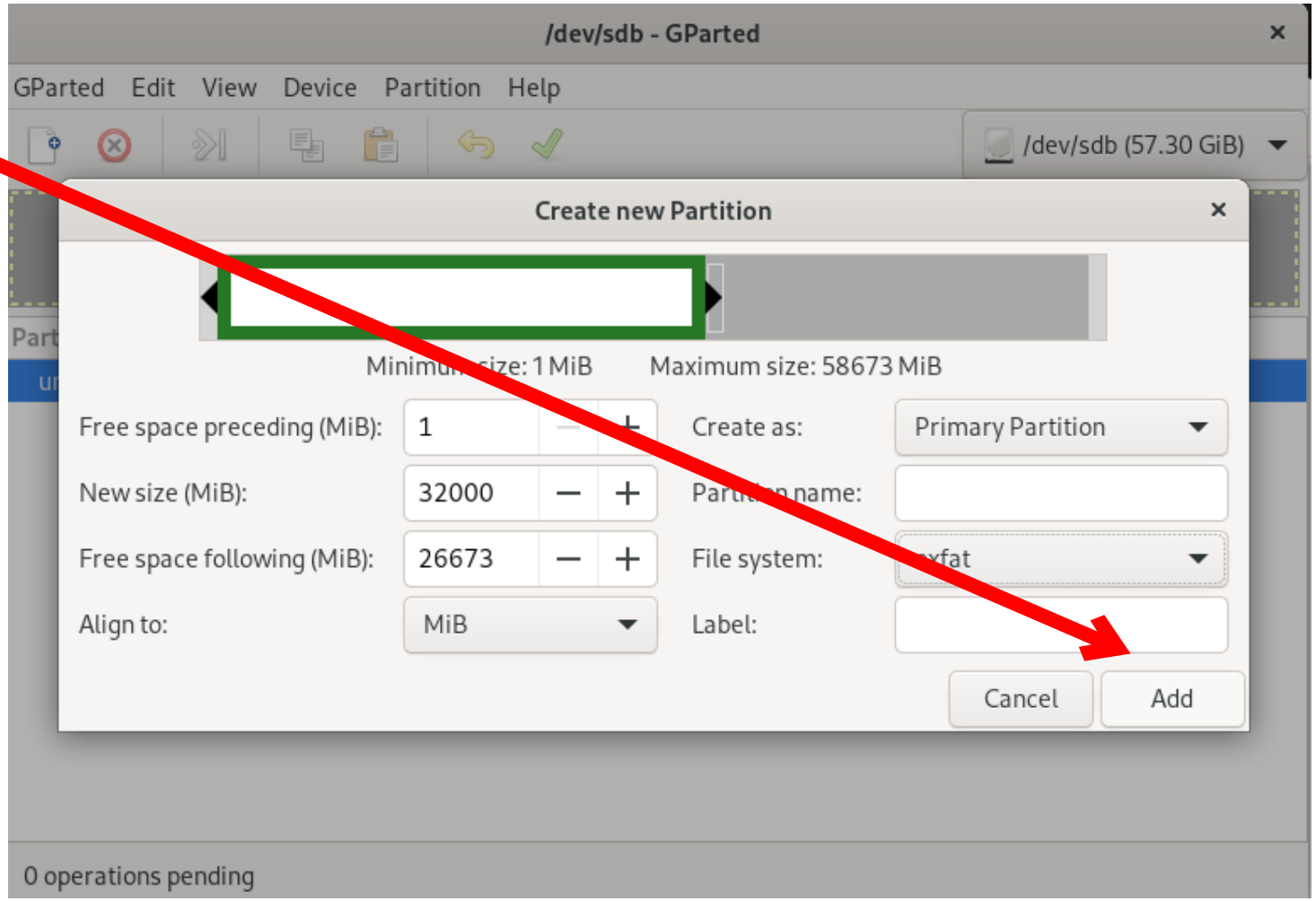
digital SAFETY IS SPELLED WITHOUT AN R

right click on the unallocated space and click on ”New”



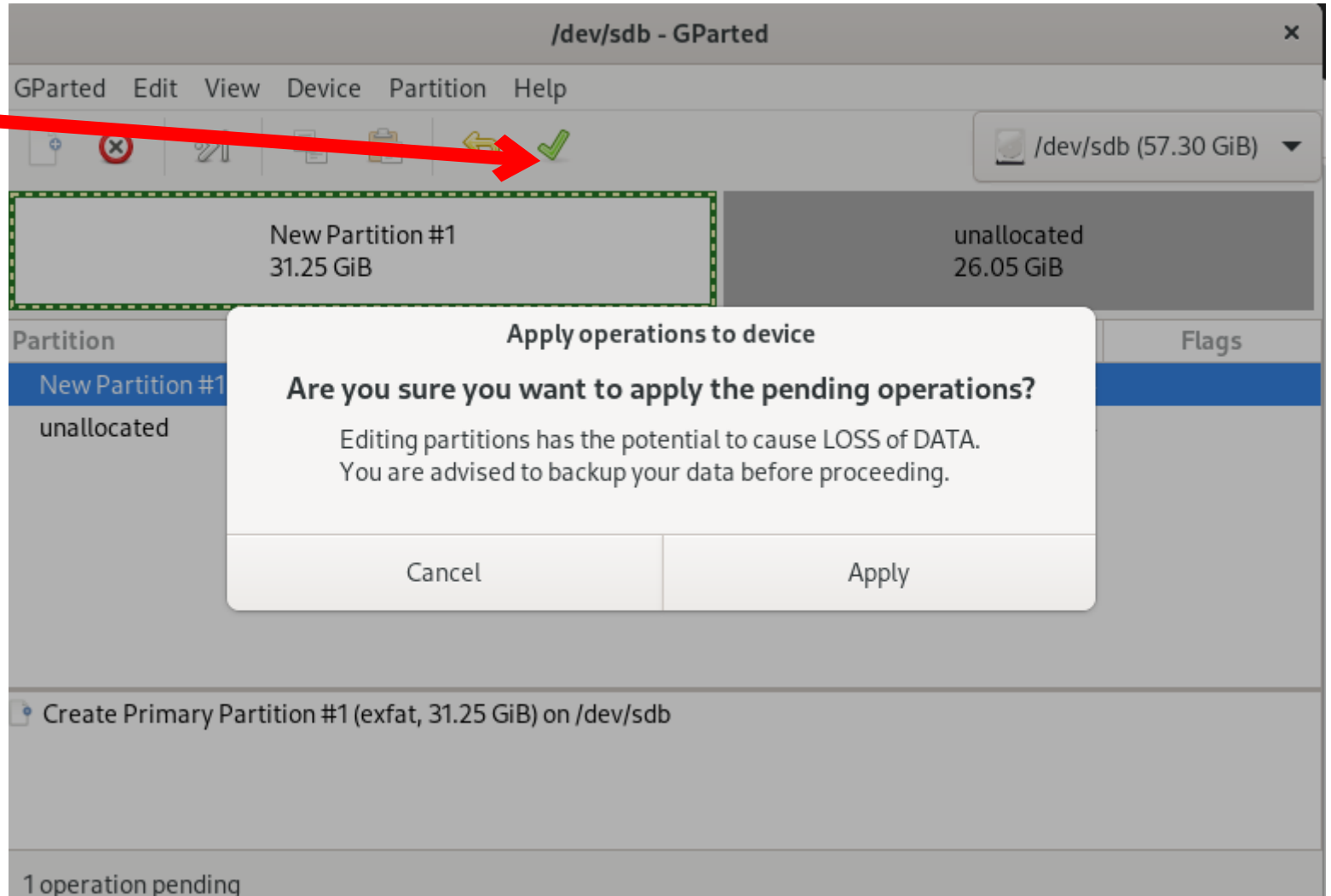
Encrypting a USB key

Fill the New size with all the size available, select ”exfat” for the filesystem, then click on ”Add”



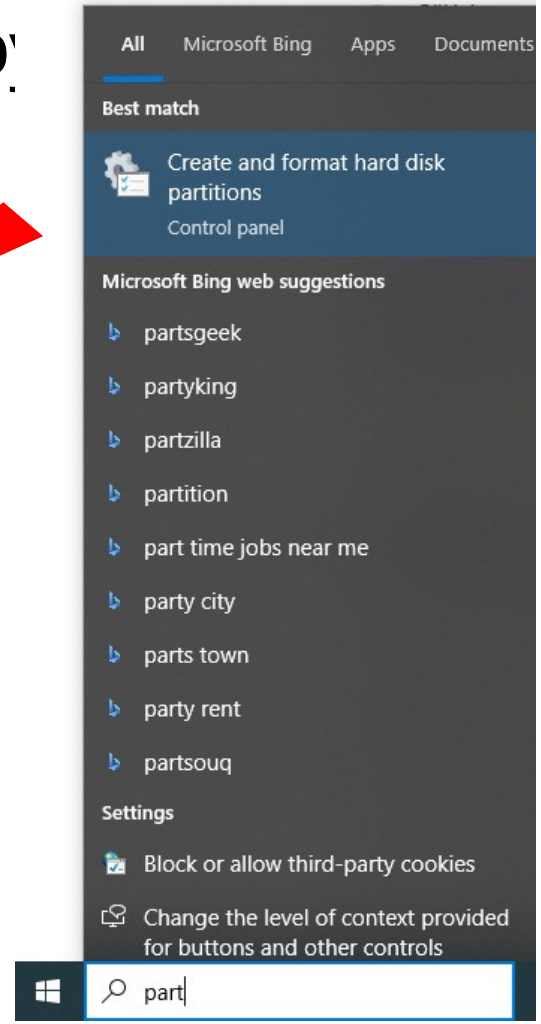
Encrypting a USB key

Click on the ”Apply” logo, then ”Apply”



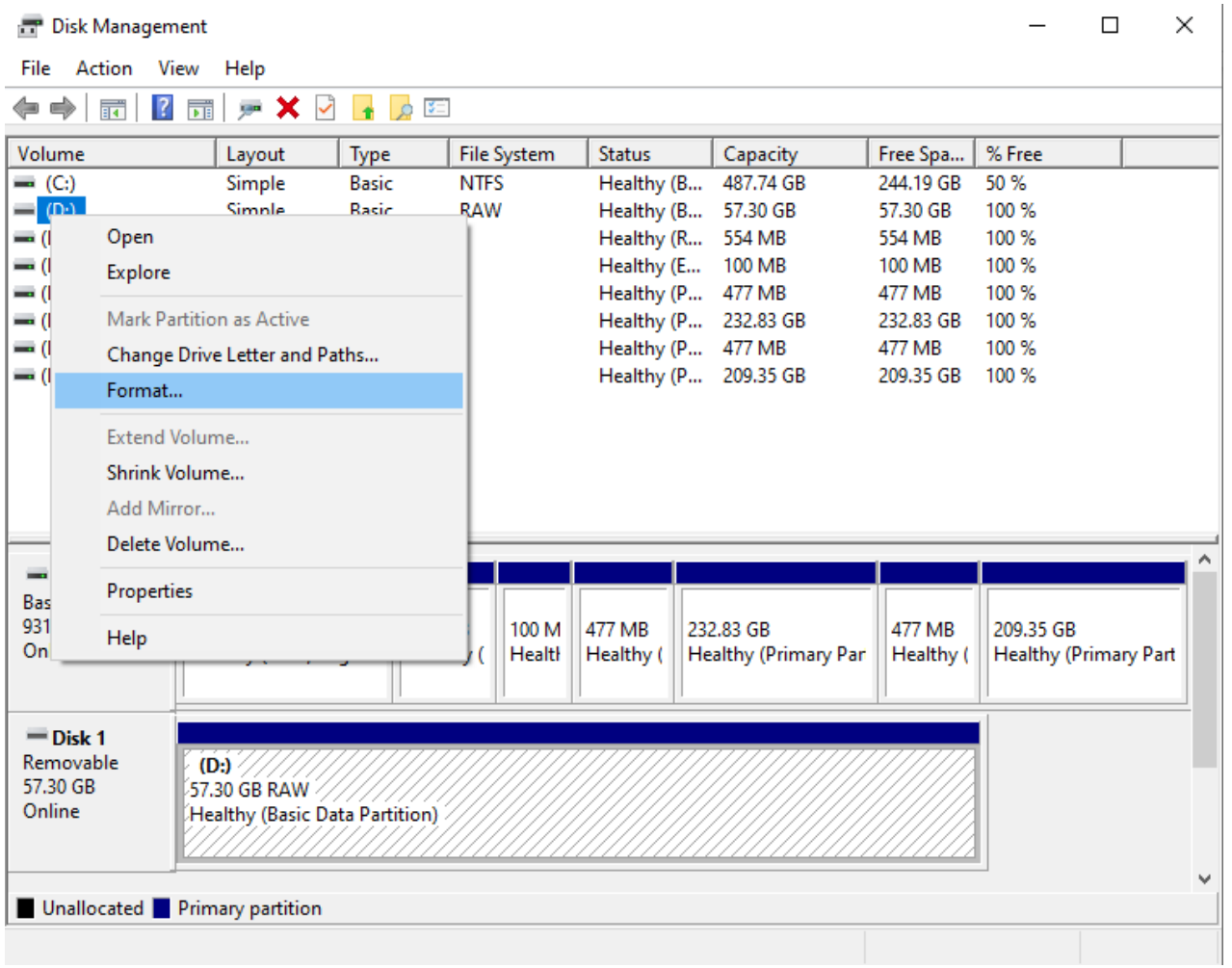
If you are on Windows

- You need to open the disk partitioning system b
  ”part” in the search bar



If you are on Windows

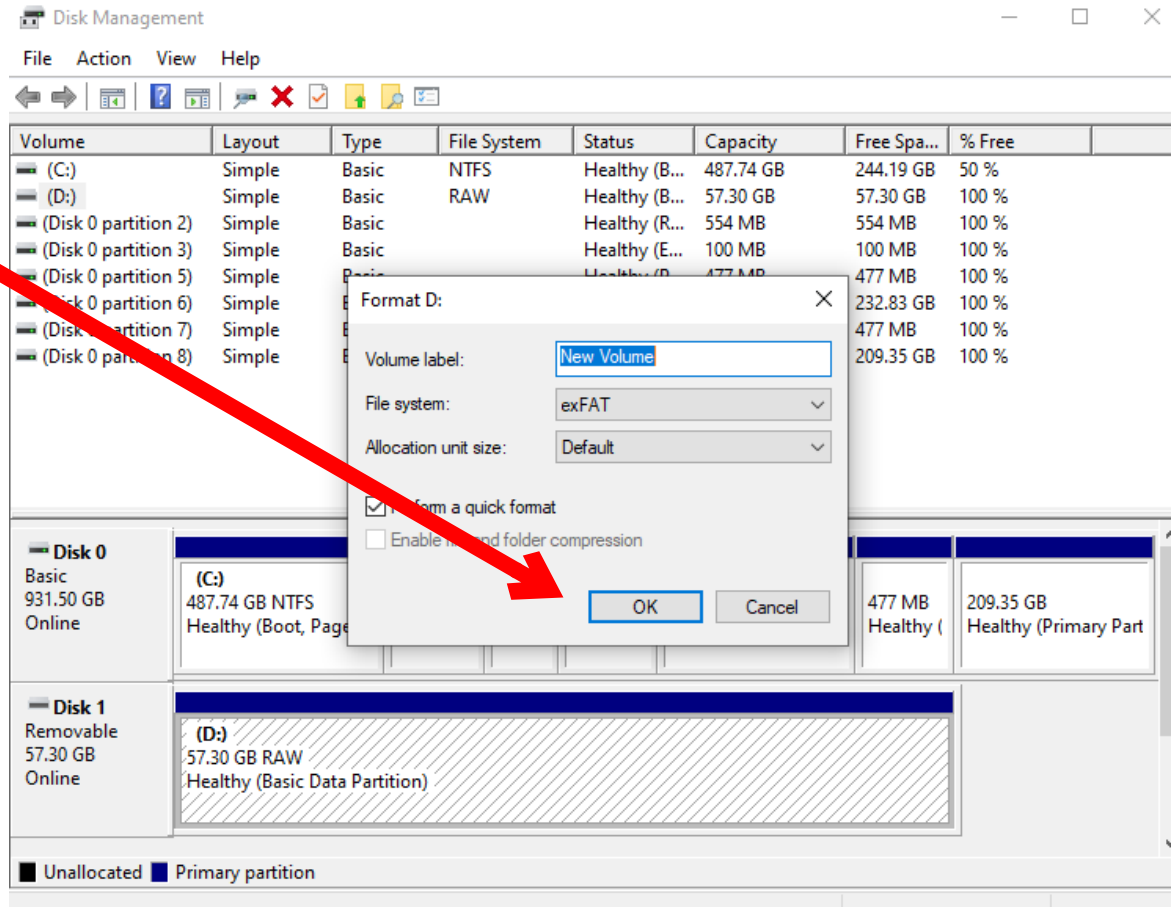
- Right click on your disk and select ”Format”



If you are on Windows

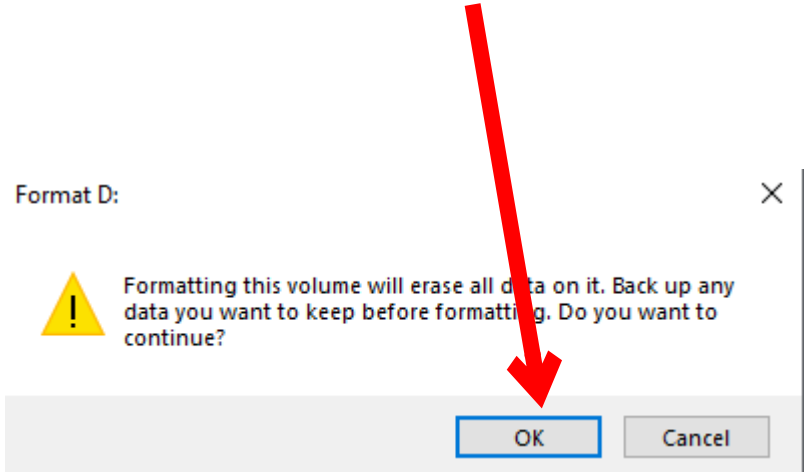
digital SAFETY IS SPELLED WITHOUT AN R

- Select exFat



If you are on Windows

- You can ignore the warning (but we agreed that all data on this USB key will be lost right?)

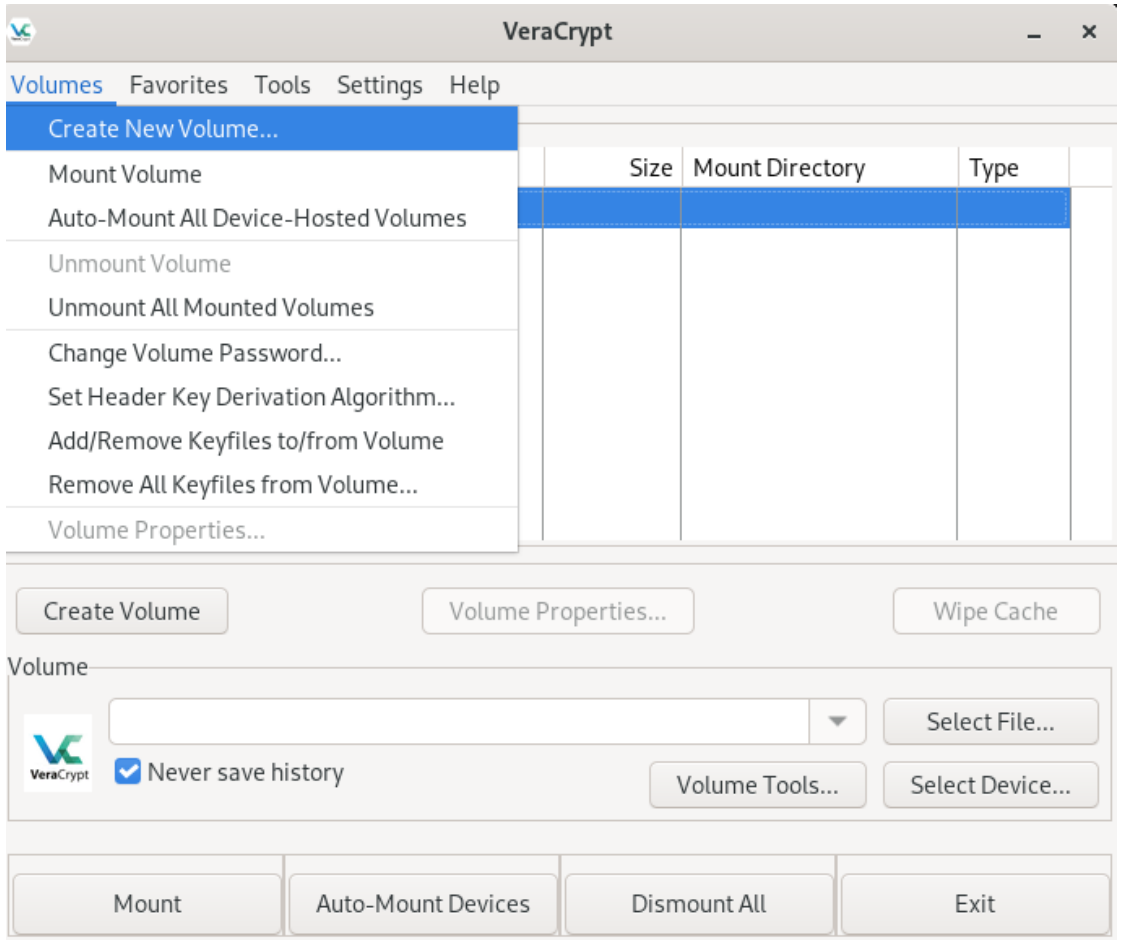


If you are on MacOS

- You need to use the diskutility software
- Select the correct disk, make some free space by removing some partitions or shrinking them
- Create a partition with the exfat filesystem, the size you want
- Click on ”apply”

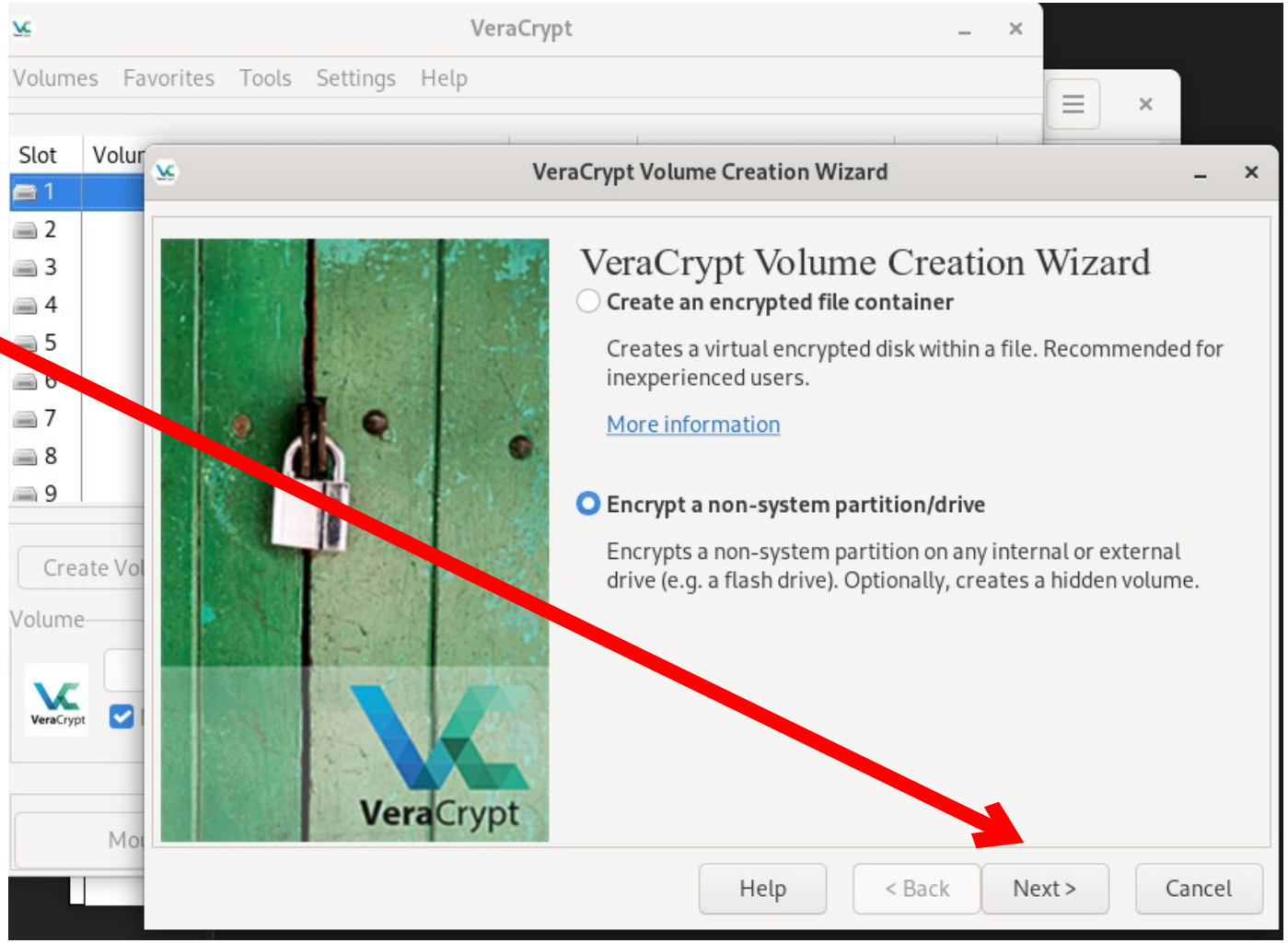
Create the volume on Veracrypt

- Create a new volume



Create the volume on Veracrypt

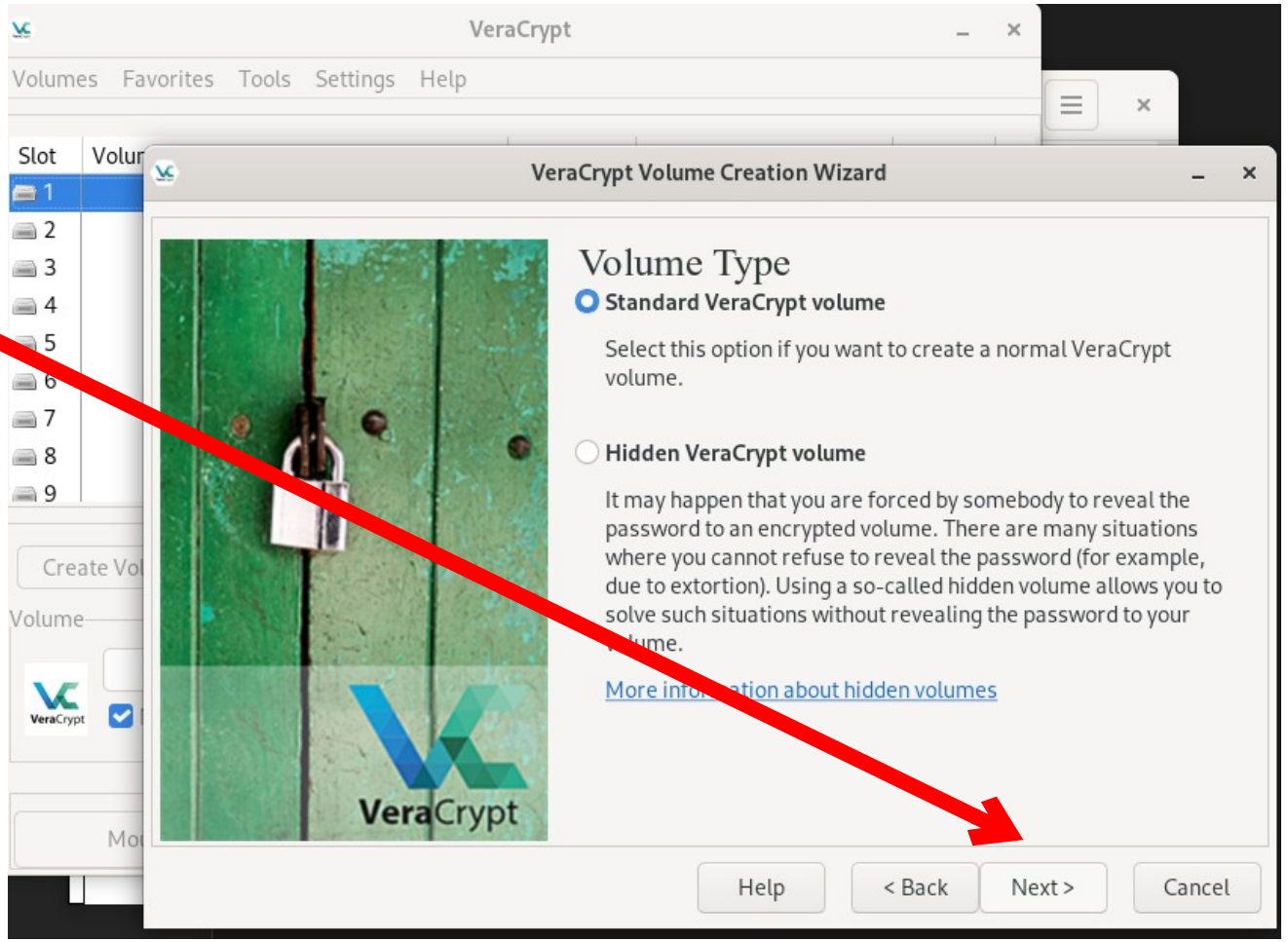
- Create a new volume



Create the volume on Veracrypt

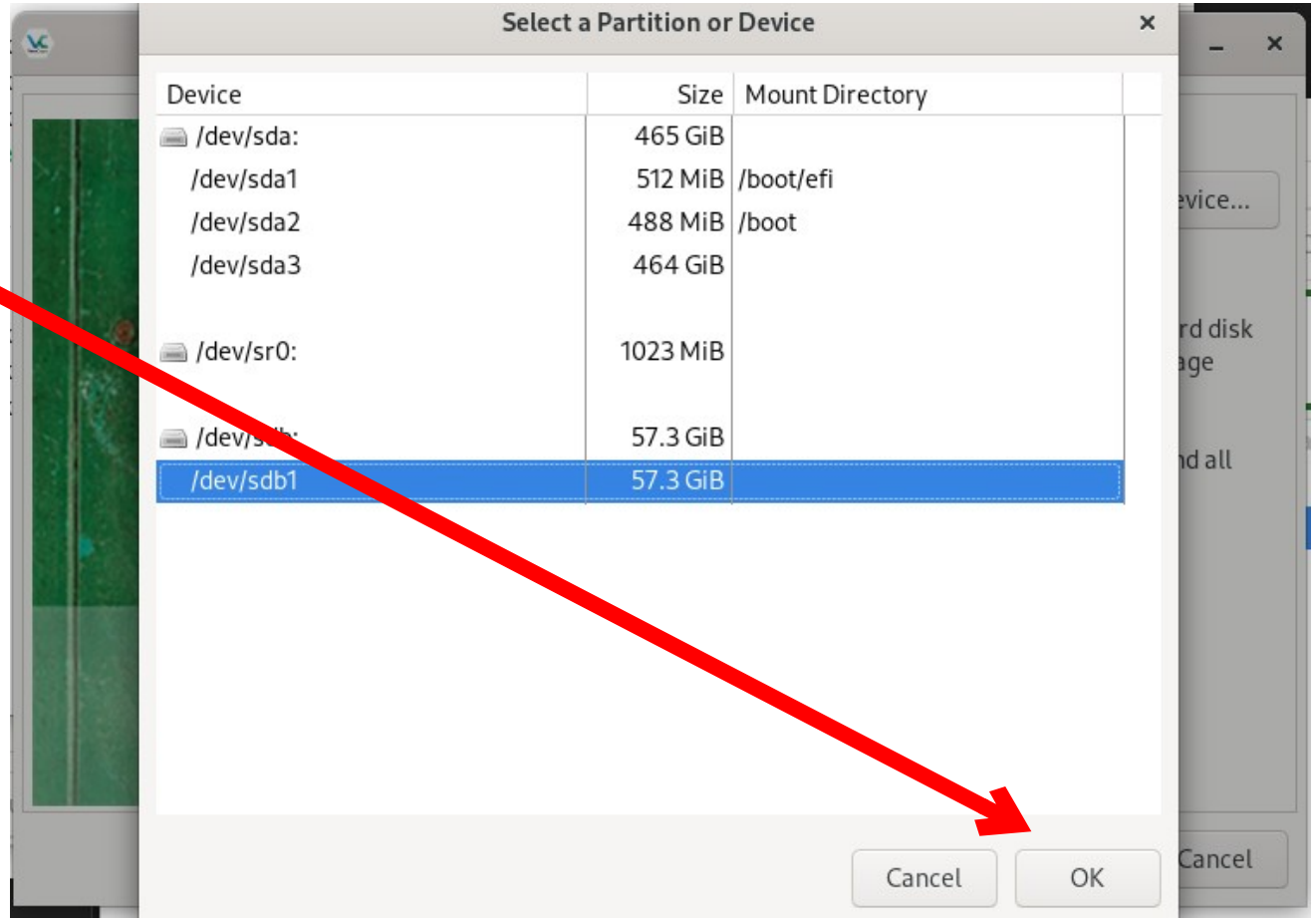
digital SAFETY IS SPELLED WITHOUT AN R

- Create a new volume



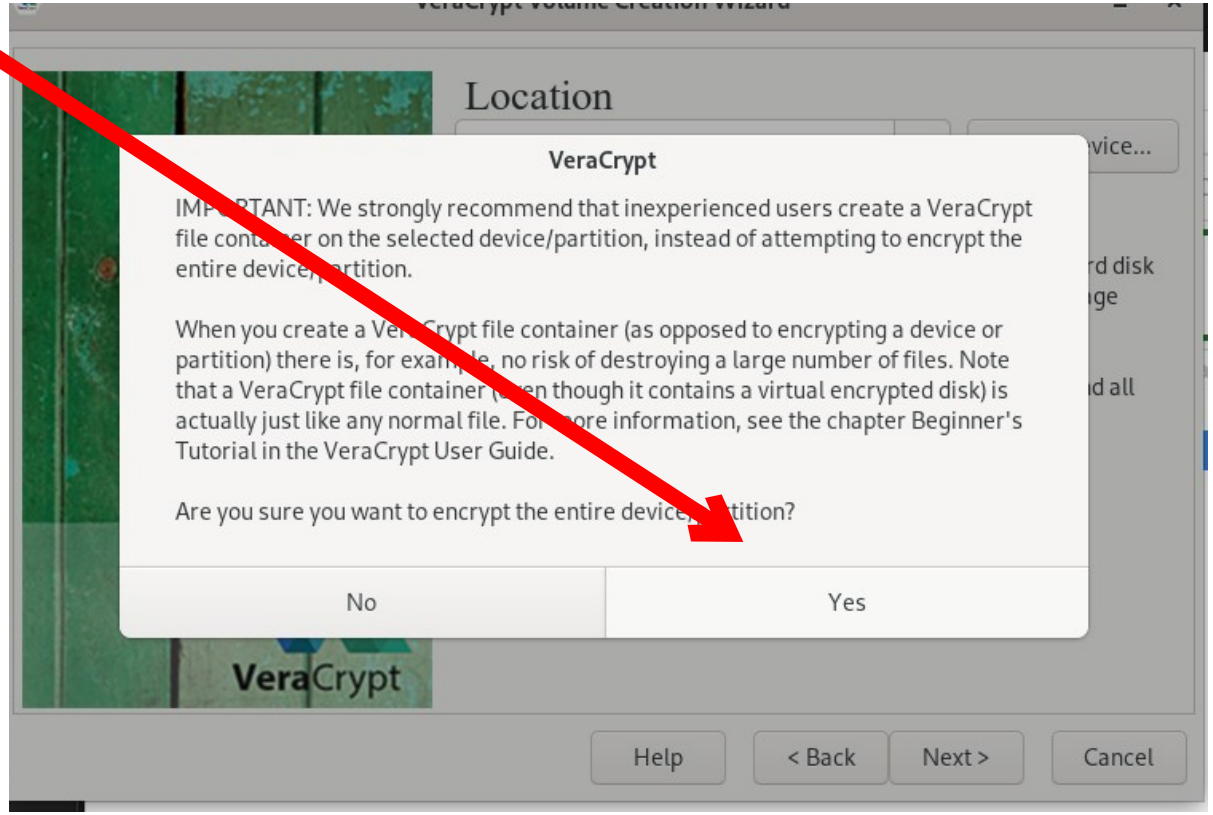
Create the volume on Veracrypt

- Select your partition (do not make a mistake here, or you can once again loose all your data)



Create the volume on Veracrypt

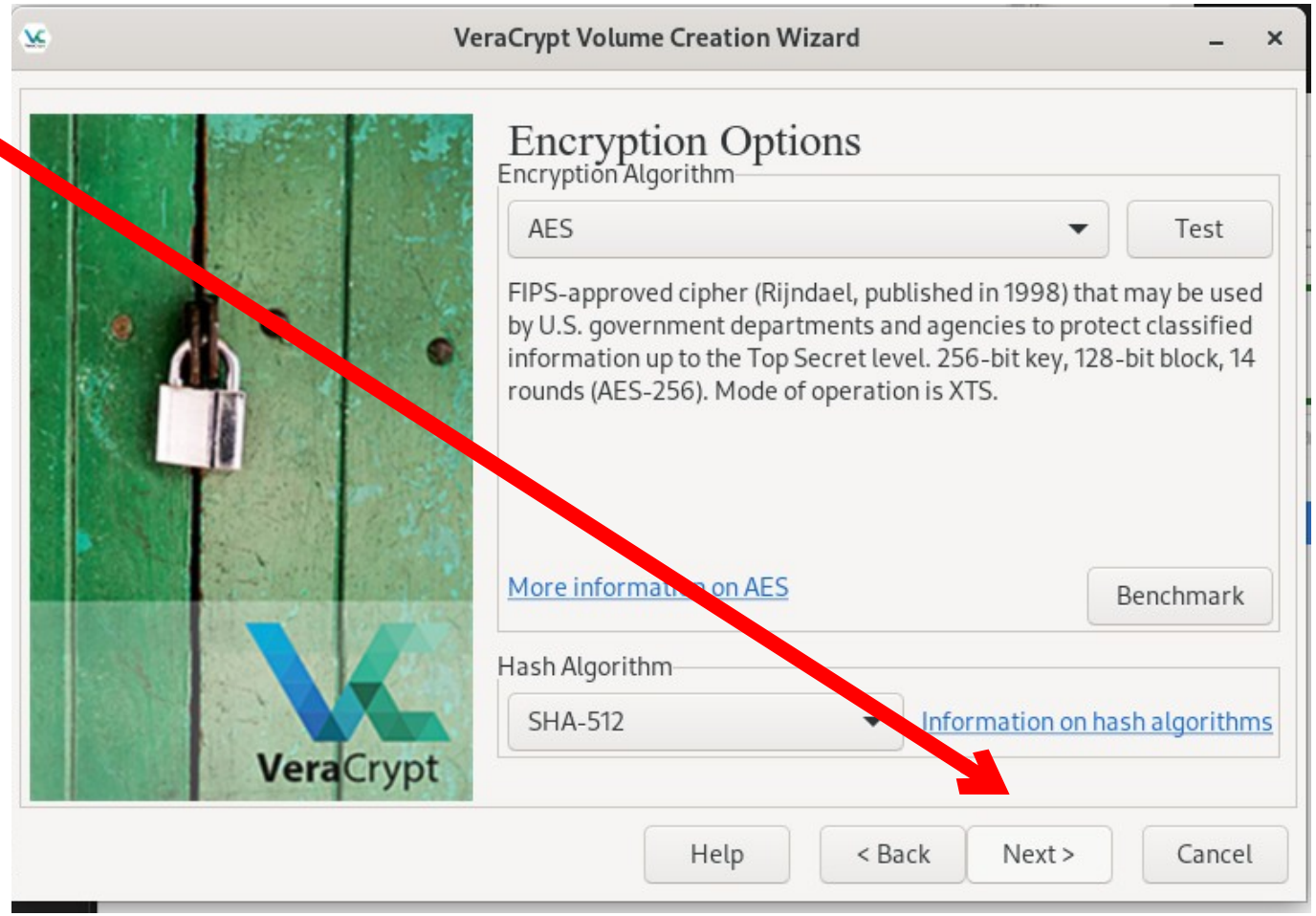
- Ignore this warning



Create the volume on Veracrypt

digital SAFETY IS SPELLED WITHOUT AN R

- Keep the default here

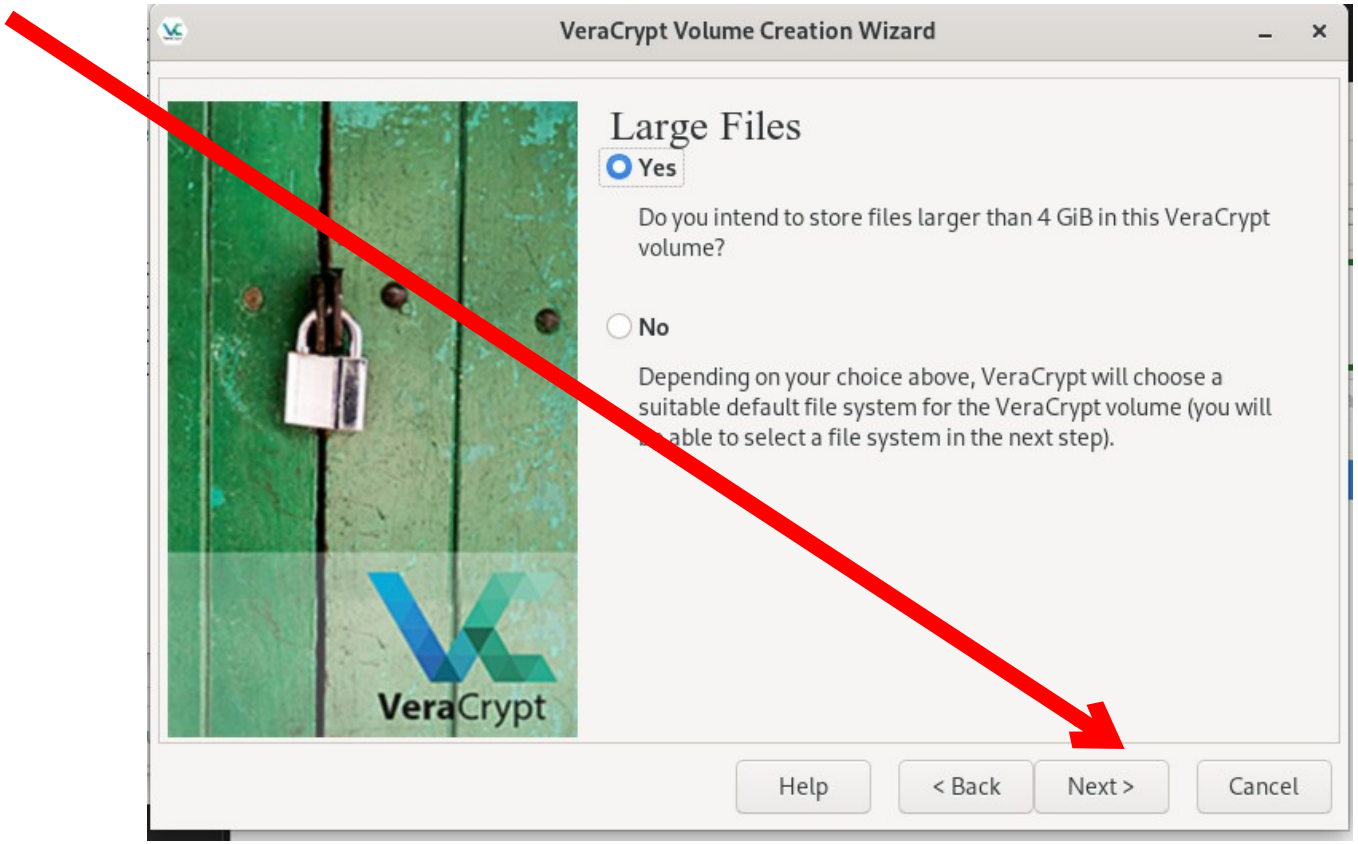


Create the volume on Veracrypt

- Enter a strong passphrase two times and continue

Create the volume on Veracrypt

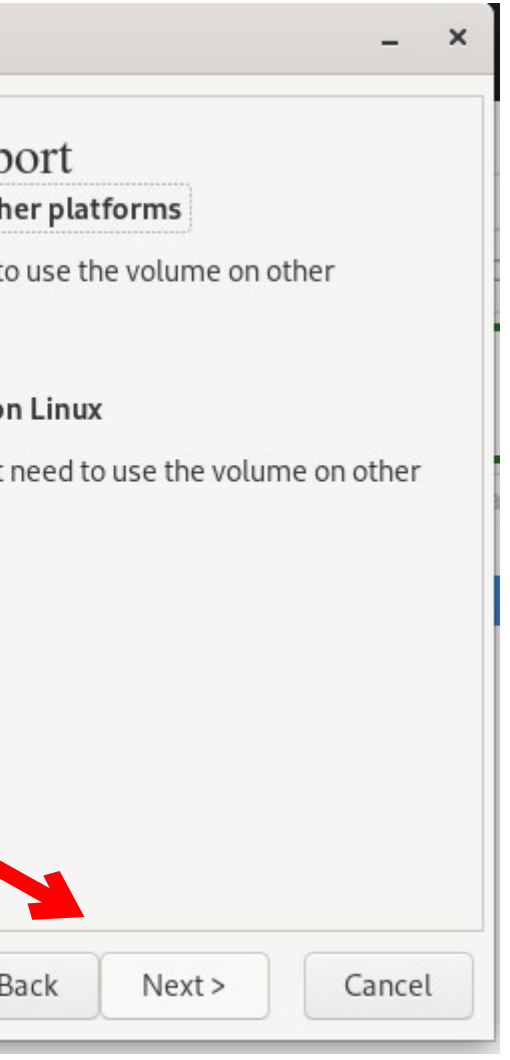
- Say that you might want large files



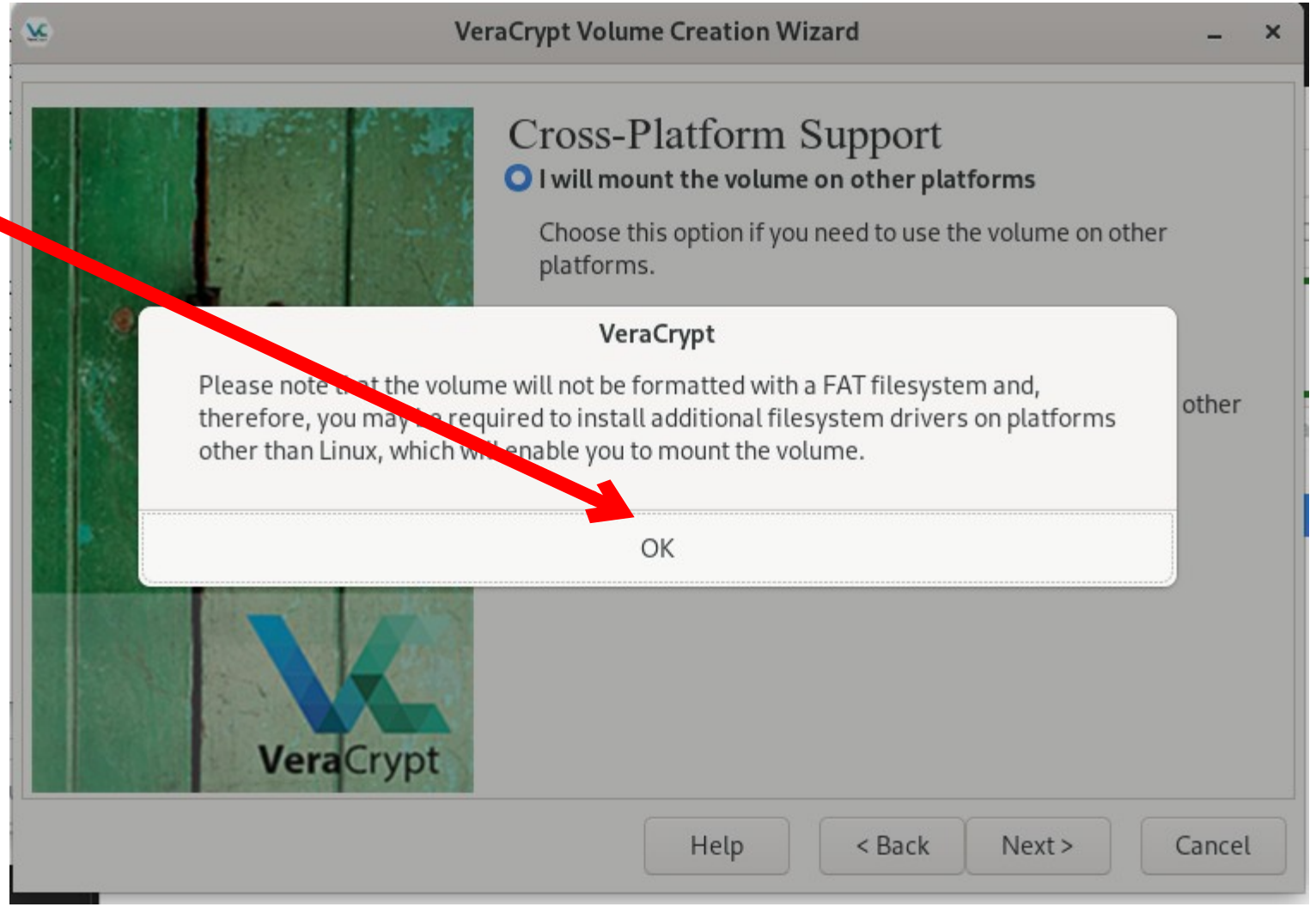
Create the volume on Veracrypt

- Select ”exFAT” and continue

Create the volume on Veracrypt



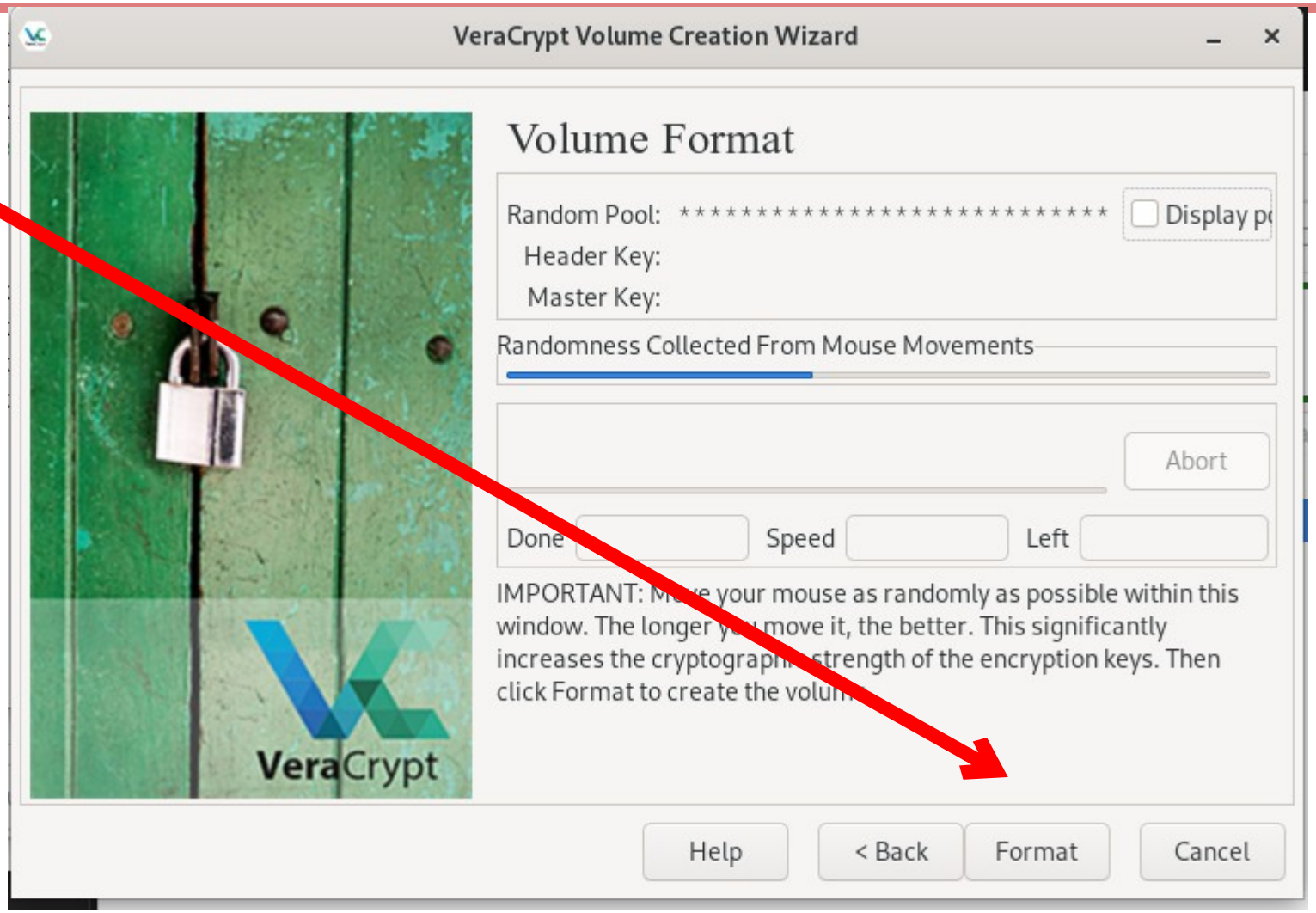
Create the volume on Veracrypt



Create the volume on Veracrypt

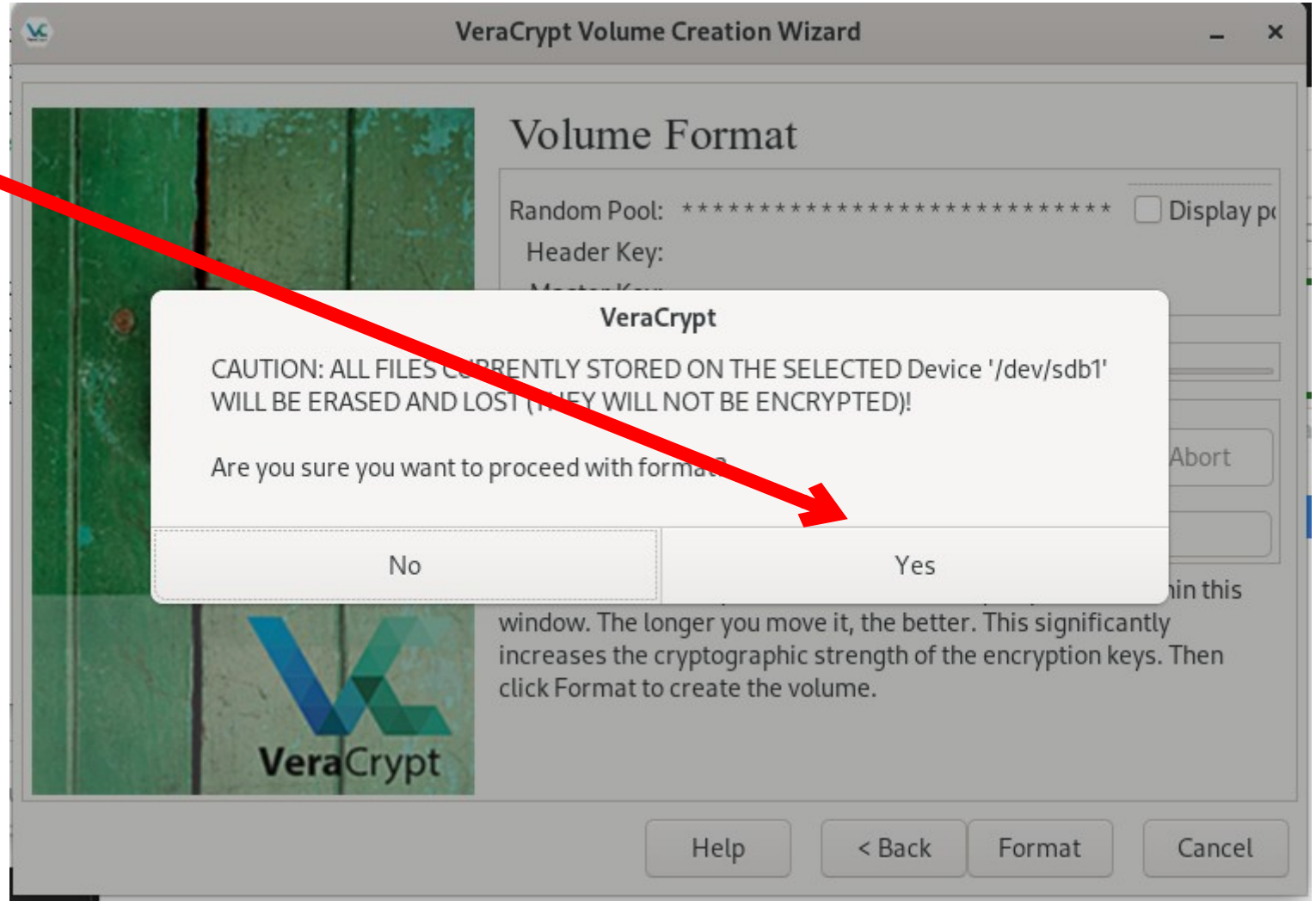
digital SAFETY IS SPELLED WITHOUT AN R

move you mouse to collect some randomness, then format



Create the volume on Veracrypt

last check: all data will be lost on the selected partition



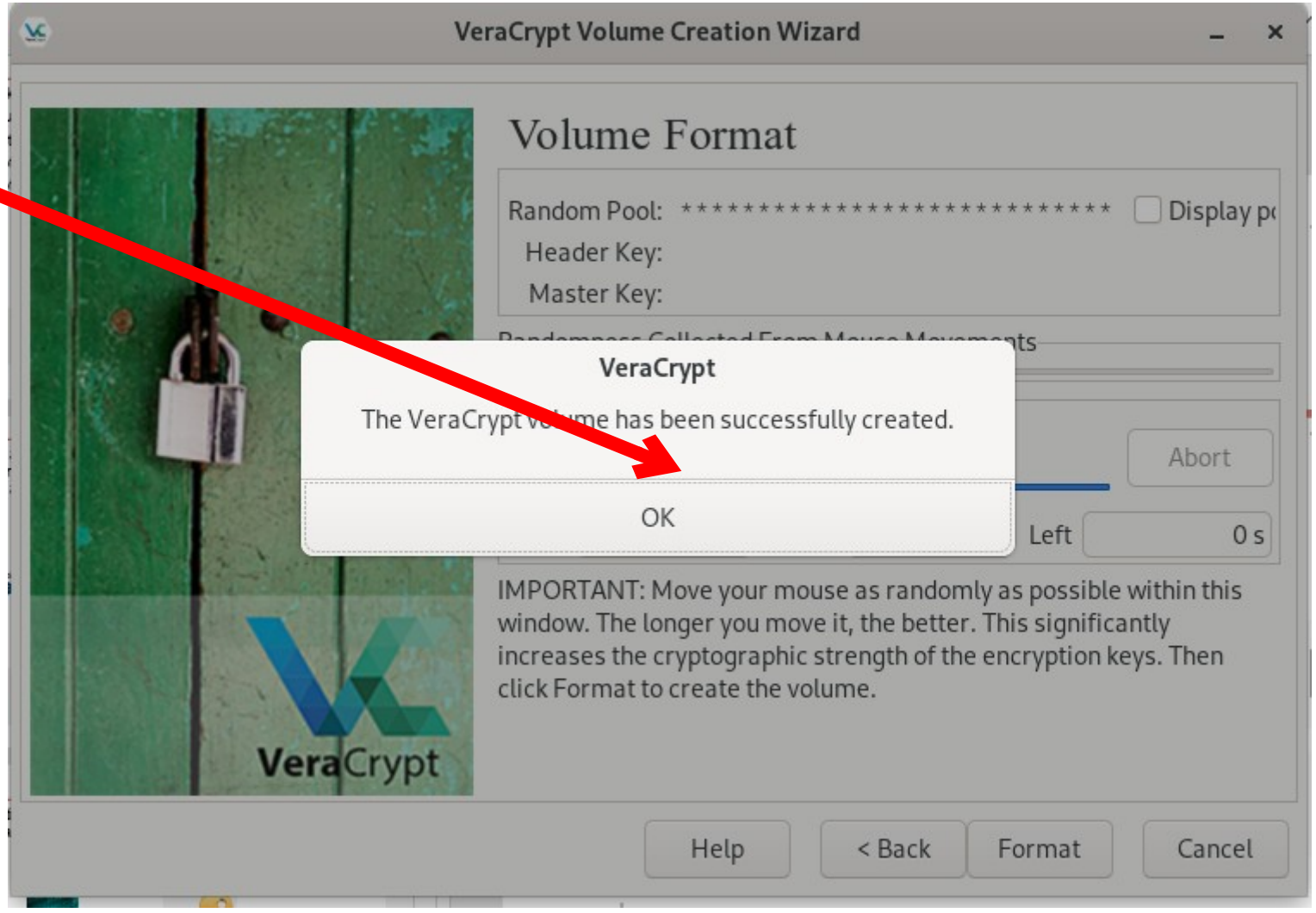
Create the volume on Veracrypt

be patient

Create the volume on Veracrypt

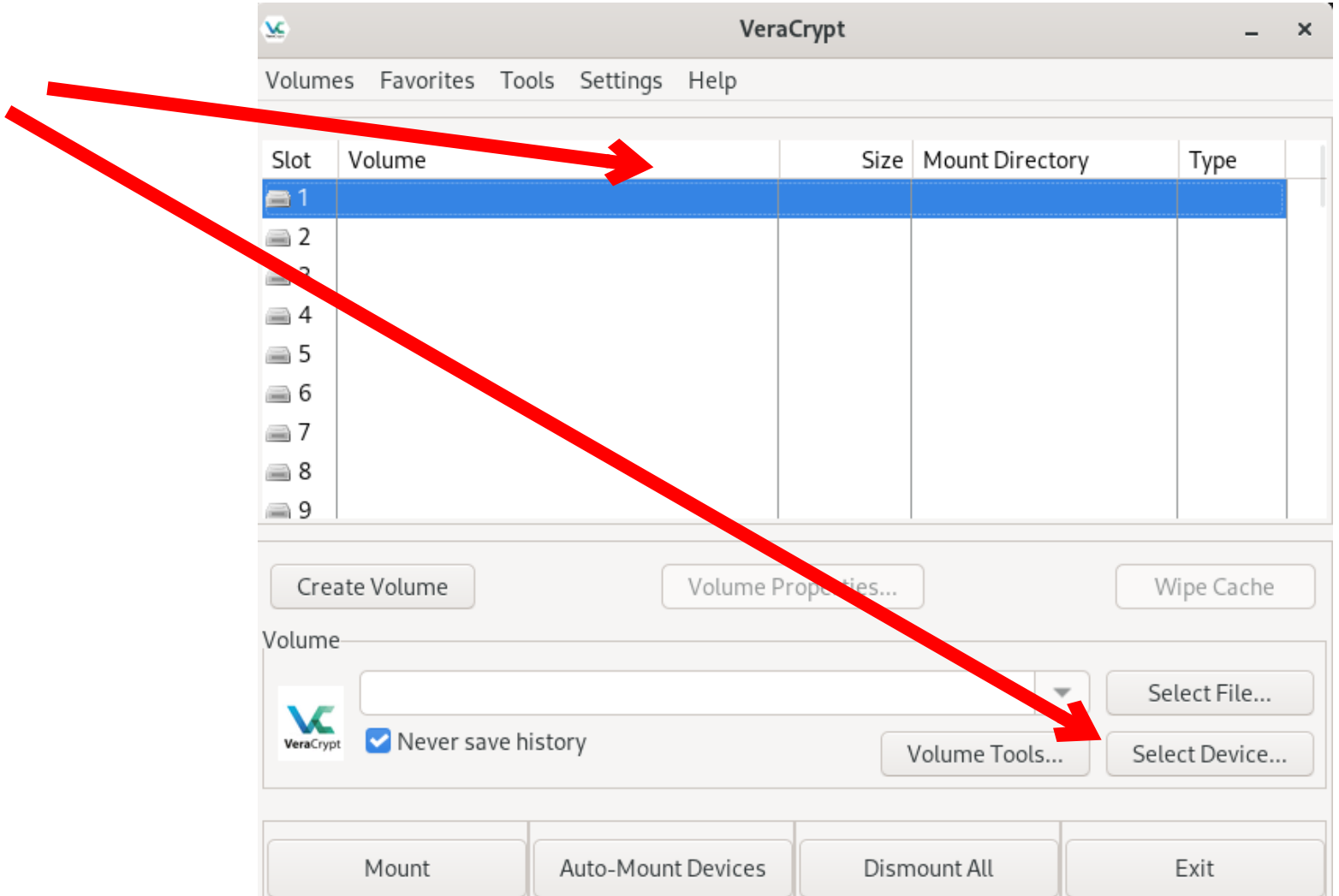
digital SAFETY IS SPELLED WITHOUT AN R

all good



Mount the volume on Veracrypt

Select one slot, then a device



Mount the volume on Veracrypt

digital SAFETY IS SPELLED WITHOUT AN R

Select the correct device, then OK.
You will have to enter your password, then you will be able to access your files.
Congrats !