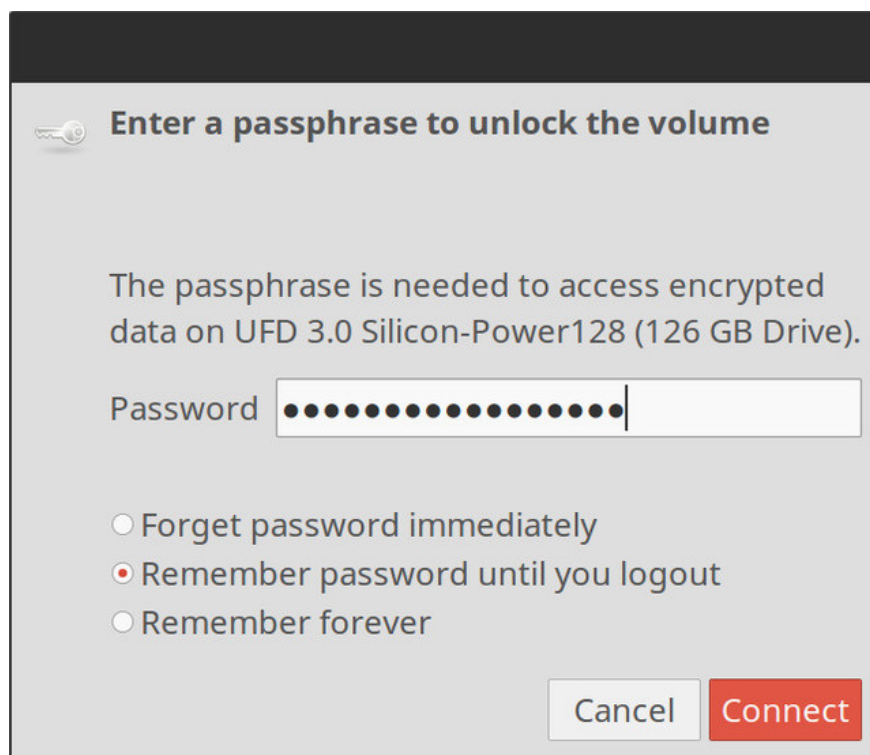


# 4 small tips to help secure data on USB drive better

Most users often store their valuable data on a USB drive to avoid a system failure or virus attack. However, the biggest drawback is that users are not interested in encrypting their USB drive to prevent bad cases from happening. Even on devices that have Encrypted Partition integrated, adding passwords to use encryption is also considered inconvenient.

Most users often store their valuable **data** on a USB drive to avoid a system failure or **virus** attack. However, the biggest drawback is that users are not interested in encrypting their USB drive to prevent bad cases from happening. Even on devices that have Encrypted Partition integrated, adding passwords to use encryption is also considered inconvenient.

## 1. Use Encrypted Partition (encrypted partition)



Most users often store their valuable data on a USB drive to avoid a system failure or virus attack. However, the biggest drawback is that users are not interested in encrypting their USB drive to prevent bad cases from happening. Even on devices that have **Encrypted Partition** integrated, adding passwords to use encryption is also considered inconvenient.

The advice for you is **to use Encrypted Partition** to protect important data, your personal data is safest.

Some tools can help you do this. On Windows operating systems you can use some tools like Rohos Mini Drive or USB Safeguard. Or if you're using Mac or Linux, you can use encryption tools designed to replace TrueCrypt like AxCrypt (Windows), DiskCryptor (Windows), and AESCrypt (Windows, Mac, Linux). You can also use the Linux Unified Key Setup tool.

## 2. Save 'sensitive' data on cloud storage service



Another solution to improve data security on USB drives is that you should save these data on cloud storage services. Of course sharing data on cloud storage services, email or instant messaging (or instant messaging, online chat, chat - from chat in English, IM short for Instant Messaging, is translation The service allows two or more people to talk online via a computer network) quite simply and conveniently.

In addition, you can refer to some of the best cloud storage services available here.

## 3. Regularly perform backups

The advice for you is **to back up your data regularly** to avoid losing data. Of course, you also need to make sure that the disk space can store the amount of data you want to back up. In addition, you should also **consider the security** and importance of data. Does the data need to be encrypted?

If you need encryption, you can refer to opening the Encrypted Partition section above.

## 4. Use a USB drive to unlock the computer



Every time you want to unlock your computer, you must enter the password into it. If you have to enter your password multiple times in a day, it makes you feel uncomfortable and spend your time. And moreover, if other people know your password, they can gain unauthorized access and steal your important information and data.

If you want to find another solution to unlock your computer more easily, **USB Raptor** is the first choice for you.

USB Raptor is a free tool that helps users to lock and unlock the computer using a USB drive as a key (without the user having to enter a password).

Refer to how to use USB Raptor here.

### **Refer to some of the following articles:**

1. 4 ways to fix USB errors without formatting: 'Windows was unable to complete the format'
1. Protect your Google account with USB "security key"
1. Summary of some ways to fix USB Device Not Recognized on Windows 7, 8 and 10

### **Good luck!**

You finished reading the article "**4 small tips to help secure data on USB drive better**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.