



TJMicro Tech Tips

Encrypting Your Data on a USB Drive

With the introduction of Cloud services, many of us are saving our important documents onto the Cloud for safekeeping. However, for some, saving important documents for sharing or backups of our hard drive to a USB drive is the more economical or convenient option. As mentioned in our [previous post on backing up your data](#), USB drives might be a cost friendly option for back ups, but can be easily lost. To prevent unauthorized access to your private data, it is highly recommended that you encrypt any hard drive or USB that you own, giving access to only those who you decide should have access.

When we talk about encrypting your data on a USB drive, there are two main options to consider:

- 1) Encrypting the entire USB drive; or
- 2) Encrypting the files on the USB drive.

There are pros and cons to both, and they require different software and steps to be taken. Here, we will discuss both options to help inform your choice of which option is better for you.

Encrypting the Entire USB Drive

Just as it sounds, when you encrypt the USB drive, everything on the drive is covered under the encryption. The main advantage of this is that the chance of accidentally revealing sensitive information is minimized. However, on the other side of the coin, if there becomes an issue with the encryption, likely the entire USB will become unreadable, making it very difficult to access or recover any of your files. If you are using a computer outfitted with Windows or Linux, you will need to download encryption software, such as [McAfee Endpoint Encryption](#).

Encrypting Files on the USB Drive

Instead of encrypting the entire drive, there might be only specific files that you want securely protected. In this case, you only need to focus on encrypting those particular files. The most common method is using **partition encryption**. This means that groups of files can be encrypted together, and that you can have different groupings of files that are separately encrypted on the same drive. This allows you to give access to certain secure files without giving away access to all of the sensitive information. Software like [Rohos Mini Drive](#) allows you to set up partition encryption on your drive.

And what if these don't meet your needs?

In some cases, you might not be interested in encrypting more than one file – or you only need a couple of files encrypted, and access given to different people. If the file is a Microsoft Office document, such as an Excel or Word file, or Adobe PDF, these programs allow you to password protect files without needing third party software.

With any form of encryption, it's important that you remember the password or key to allow you to access the documents in the future. Keep the password/key stored in a safe place, and make sure it's only given to those who you plan on giving access to your sensitive information.

Please note, the abovementioned software programs are just one of many options available, and are only provided to serve as an example. TJMicro Ltd has not received any financial compensation for mentioning these particular programs, and does not endorse these particular programs over any other. TJMicro promotes using the program that best suits your needs.



Kyle Hacker is the CEO of TJMicro Ltd – your complete source for professional IT services. Kyle has diverse experience in managing professional IT services and strives to meet the needs of all his clients. TJMicro Ltd provides tailored services to organizations of all sizes and across the private and public sector. To find out more about what TJMicro can do to help support your business, contact Kyle at kyle@tjmicro.com.

If you have any questions about encrypting your external drive or USB, please contact TJMicro Ltd by phone at 416-317-6000 or email at info@tjmicro.com.

To find out more about services offered by TJMicro Ltd, visit us at www.tjmicro.com.



Your complete source for professional IT services