Encrypt a USB Drive in Windows 10

A USB drive is a portable device that offers a convenient way of storing and/or transferring your data, though this can come with several security risks. Thankfully, you can encrypt a USB drive and protect your confidential/sensitive files and data whenever they're transferred between different locations.

You should note that encryption doesn't protect your data and files from password prying methods and password-collecting malware. It's simply a way of preventing your sensitive and confidential files and data from landing in the wrong hands or being accessed by unauthorized persons via security incidents and data breaches.

In order to encrypt your USB drive using BitLocker, take the steps below:

1. Insert your USB flash drive into your Windows PC.
2. Open **File Explorer**.
3. Right click on flash drive and select **Turn on BitLocker**.
4. Wait a few seconds for BitLocker to initialize.
5. Next, check the **Use a password to unlock the drive** box.
6. Type in a unique, strong password you can remember in the **Enter your password box**, and do it again in the **Re-enter your password** box.

   You'll get a prompt to back up a recovery key. This key allows you to access the USB drive in the event that you lose the encryption password you entered in the previous step. You can save this key or print it out and store it someplace safe instead of storing it in the cloud.
   Suggestion: *Save this file to a folder on your Home drive. (U:\)*

7. Next, select how much of your USB drive you'd like encrypted. Here, you have two options: **select the entire drive or the used space only.**
8. Select the **New encryption mode (XTS-AES)** (with an improved algorithm, it also offers integrity support).
9. The next step is to encrypt the USB drive. The speed by which it encrypts your drive may move fast or slow depending on the size of your USB drive, the amount of data you have stored on it, and the system specs of your machine. Click **Start Encrypting** when ready.