How to encrypt your files in Windows (Part 1)

Encryption is the process of encoding data so it can't be read or copied, unless you have the proper key to decode it. The process is much more complex, but you get the idea. The important thing is that we encrypt our data as soon as possible to prevent it from being accessed by someone else.

Windows 7 Ultimate includes BitLocker to allow file encryption. If you're using Windows 7 Home Premium you're out of luck, but there are third-party tools to safeguard your files. I'll mention a couple of them in my next blog post.

Encryption on Windows 7 Ultimate

To enable BitLocker on Windows 7 Ultimate go through the following steps:

1. Click **Start**, click **Control Panel**, click **System and Security**, and then click **BitLocker Drive Encryption**.
2. Click **Turn On BitLocker** for the operating system drive. BitLocker will scan your computer to make sure that it meets the BitLocker system requirements. If your computer meets the requirements, BitLocker will inform you of the next steps that need to be taken, such as drive preparation, turning on the Trusted Platform Manager (TPM), and encrypting the drive.

3. After the TPM is initialized, the BitLocker setup wizard prompts you to choose how to store the recovery key. You can choose from the following options:
    a. **Save the recovery key to a USB flash drive**. Saves the recovery key to a USB flash drive.
    b. **Save the recovery key to a file**. Saves the recovery key to a network drive or other location.

c. **Print the recovery key**. Prints the recovery key.
d. The BitLocker setup wizard asks if you are ready to encrypt the drive. Confirm that the **Run BitLocker system check** check box is selected, and then click **Continue**.
e. Confirm that you want to restart the computer by clicking **Restart now**. The computer restarts, and BitLocker checks if the computer meets the necessary requirements and is ready for encryption. If it is not, you will see an error message alerting you to the problem after you have logged on.
f. If it is ready for encryption, the **Encrypting** status bar is displayed, which shows the progress of the drive encryption. You can monitor the ongoing completion status of the disk drive encryption by moving the mouse pointer over the **BitLocker Drive Encryption** icon in the notification area, at the far right of the taskbar. Encrypting the drive will probably take a couple of hours. You can use your computer during encryption, but performance may be slower. A completion message is displayed when encryption is finished.

Notes: If your hardware doesn't support TPM you can still use BitLocker but you will be using the **Startup key only** authentication method. This means that the required encryption key information will need to be stored on a USB flash drive, which you'll connect to the PC during startup if the hard drive gets locked by BitLocker for some reason. This can be somewhat of a hassle, so you may prefer to use a third-party tool to encrypt your files instead of BitLocker.

It is important that you store the recovery key in a safe place. You will need it to access your data if you move the drive to another PC, or if BitLocker enters a locked state for some reason. A good idea would be to store the key on a USB flash drive and also print it out and store it in a safe place.

In my next article I'll discuss how to encrypt files in Windows XP Professional.