DEVICE ENCRYPTION IN WINDOWS 11

Windows 11 includes a device encryption feature that helps protect the documents and other data that you store on your PC from being stolen or otherwise accessed by others.

Device encryption is what's known as a full-disk encryption solution because it is applied to an entire disk and not just to certain folders or files. It's also automatic: device encryption is enabled on the PC when you sign in to Windows 11 using a Microsoft account for the first time.

Technically speaking, Windows 11 does not encrypt your entire system disk, which is divided into different logical volumes. Instead, it encrypts the C: drive, which is the volume that contains Windows and other system files. (This drive is often referred to as the system disk.) Any other volumes on this disk will not be encrypted (nor visible while using Windows 11).

If you sign in to Windows 11 with a local account, encryption will not be enabled automatically. This is only one of many reasons why using a Microsoft account is more secure.

Oddly, there are two versions of device encryption, and which you get is determined by which Windows 11 product edition you are using:

If you have Windows 11 Home, you have a basic, streamlined version of device encryption. But if you have Windows 11 Pro, you get a more configurable and manageable version called **BitLocker** drive encryption. Both share the same underpinnings, but BitLocker includes additional features.

For the most part, using device encryption is seamless and not something you will notice. But it is important to understand that any files that you copy or move to an encrypted disk are encrypted during the copy or move process. Likewise, any files that you copy or move from an encrypted disk are decrypted during that process as well. Decrypted files can be read or used by anyone, on any PC.

When enabled, device encryption also provides some additional functionality to the system disk on which Windows is installed. For example, when the PC boots, it will examine the integrity of the system to ensure that nothing suspicious has happened to the PC's firmware or startup files. If an issue is found, you'll be prompted to

provide the recovery key, which was saved to your Microsoft Device account and is like a very lengthy password.

Device encryption doesn't offer much in the way of management: this feature is enabled for you automatically when you sign into Windows 11 using a Microsoft account. However, you can ensure that device encryption is enabled and even disable this feature–which is not recommended–using the Settings app.

To do so, open Settings (WINKEY + I) and navigate to Privacy & security > Device encryption.

Here, you will find a toggle for device encryption and links to "BitLocker drive encryption" and "Find your BitLocker recovery key," the latter of which launches your default web browser and displays an informational website.

If you are using Windows 11 Pro, the "BitLocker drive encryption" link will open the BitLocker Drive Encryption control panel. But if you are using Windows 11 Home, the Microsoft Store app will launch and try to sell you a $99 upgrade to Windows 11 Pro.

The only actionable option here is "Device encryption." If you toggle that to "Off," Windows 11 will decrypt the system drive, which could leave the files it contains open to being compromised. Do not disable "Device encryption."

However, if you are using Windows 11 Home, it is possible that device encryption is disabled, even if you have signed in with a Microsoft account.