

Protect your USB drive from Autorun viruses without using software.

AutoRun viruses are the most common type of virus that infects USB drives. Instead of using specialized software to remove them, do you know how to manually limit their spread?

When your USB drive is infected with a virus, the virus will create a file named **Autorun.inf** to activate the drive's autorun feature. Subsequent uses of the USB drive will inadvertently activate this virus. Even more dangerous is that this virus has a hidden attribute, making it undetectable. In today's article, Taimienphi will guide you on how to **protect your USB drive from the AutoRun virus** without using software, in just a few simple steps.

Protect USB From Autorun Virus

In principle, we want to prevent viruses from creating their own Autorun.inf files on the USB drive. Therefore, we will create an Autorun.inf file on the USB drive ourselves and prevent them from overwriting it. To do this, we must convert all data on the USB drive to NTFS format and grant permissions to prevent overwriting the Autorun.inf file.

Protect your USB drive from Autorun viruses without using software.

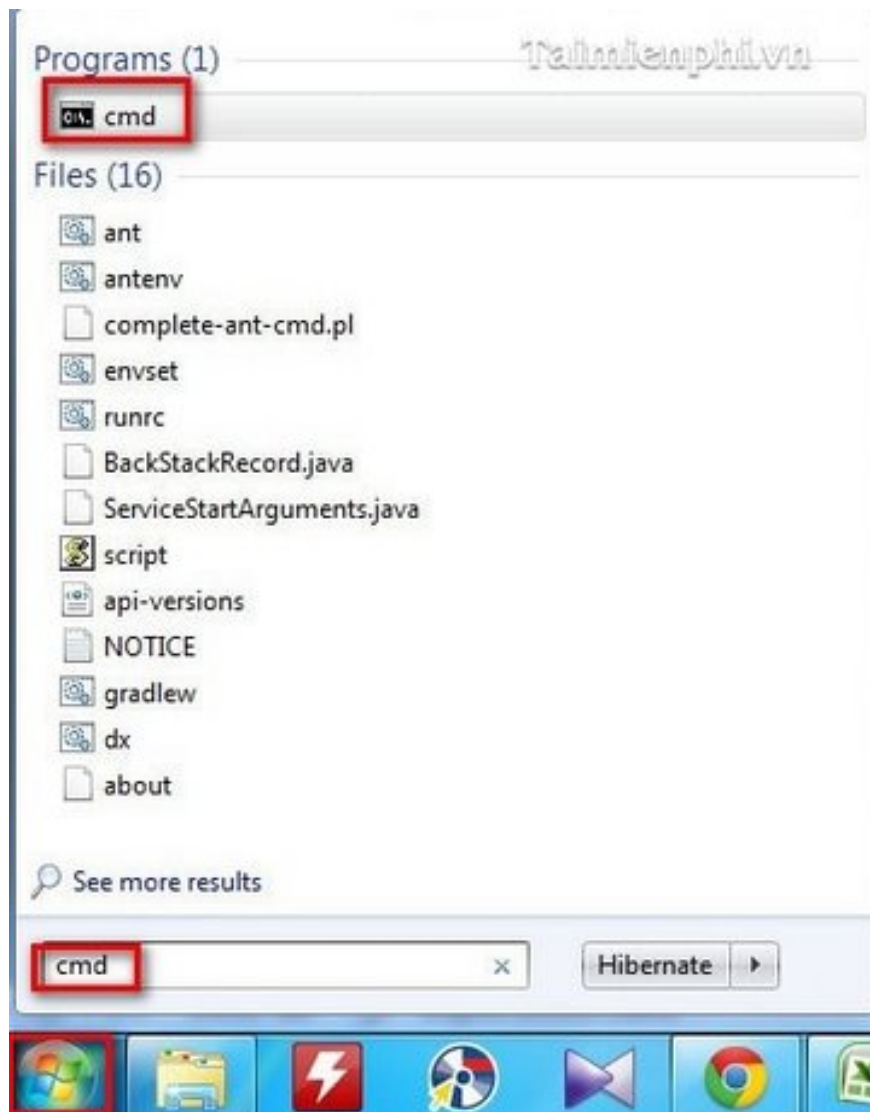
Step 1 : Identify the name of the USB drive.

Go to the USB settings to see what your USB drive is named. In my case, the USB drive is named **T**.

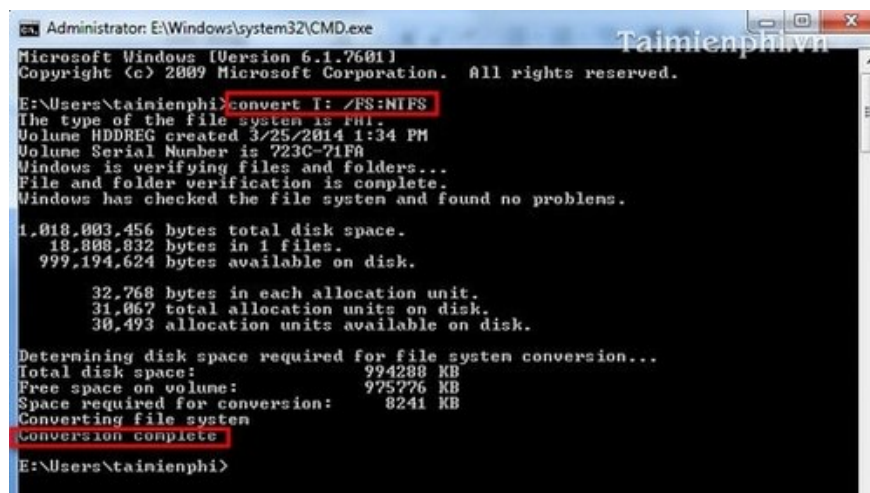


Step 2 : Convert the USB drive to NTFS format.

Click on **Start**, type **CMD** and **press Enter** to open the Command Prompt.

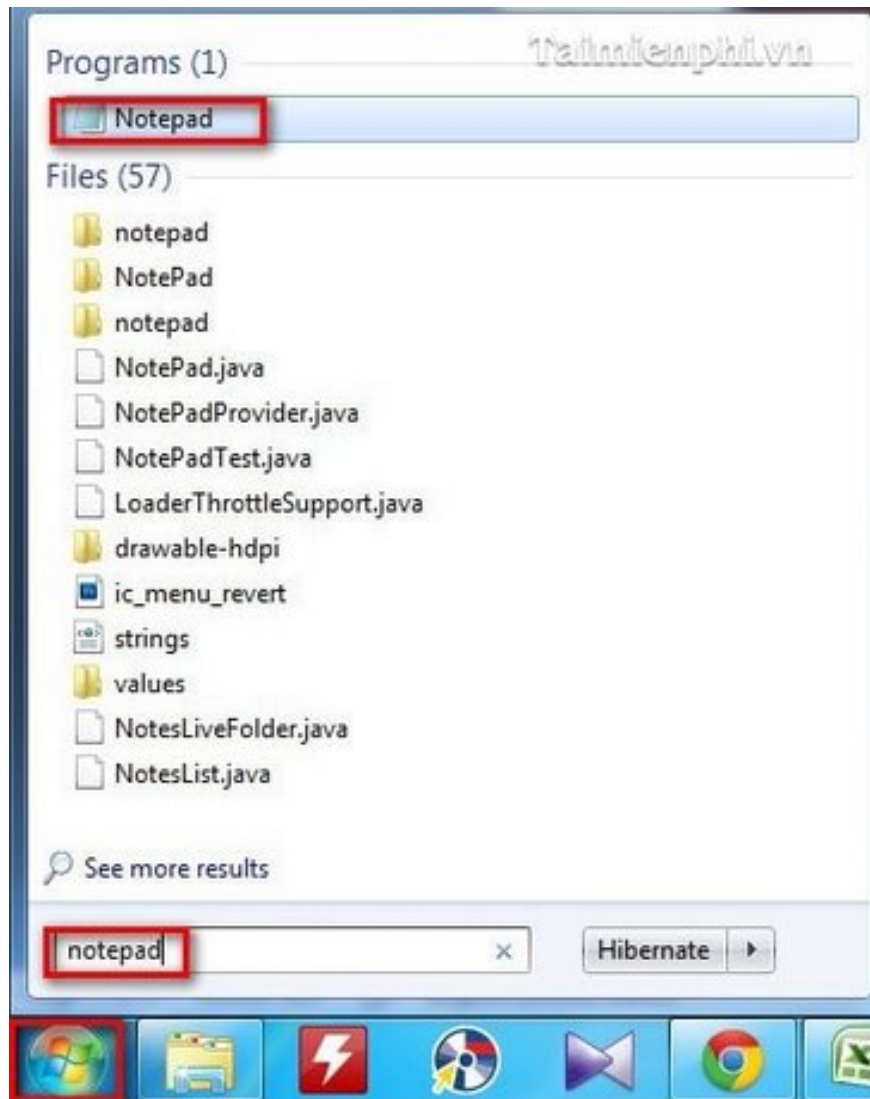


When the Command Prompt window appears, type `convert T: /FS:NTFS` and press **Enter**. (Since my USB drive is named **T**, you can use a different drive letter.) The conversion is complete when the message "**Conversion Complete**" appears .

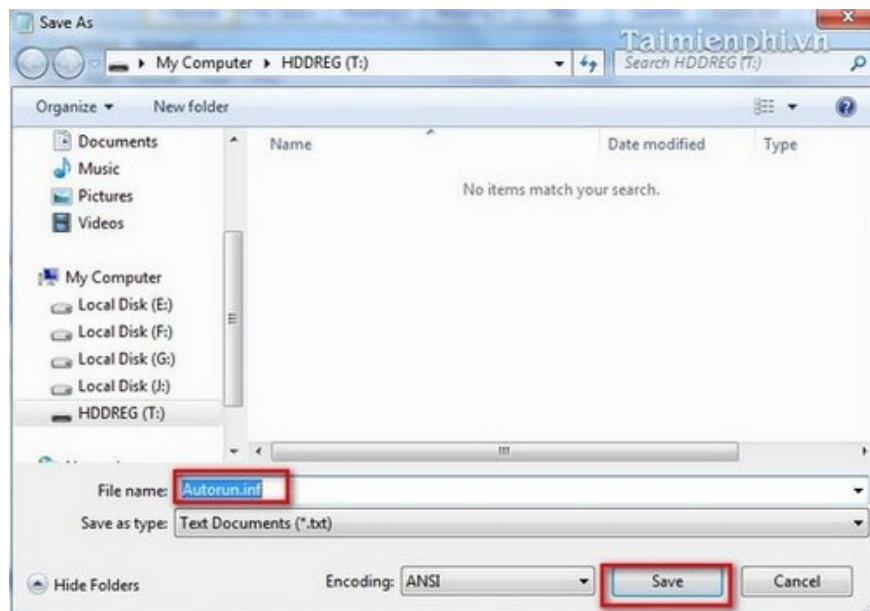


Step 3 : Create the **Autorun.ini** file and transfer it to the USB drive.

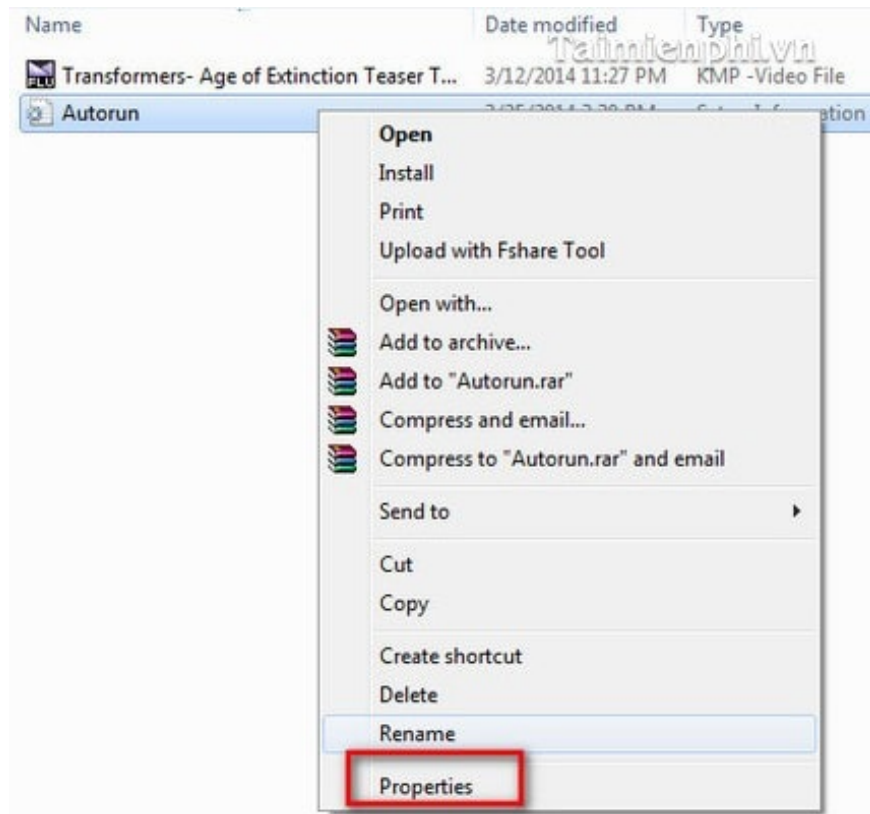
- Press **Start**, type **notepad** , and then press **Enter** to open the Notepad program.



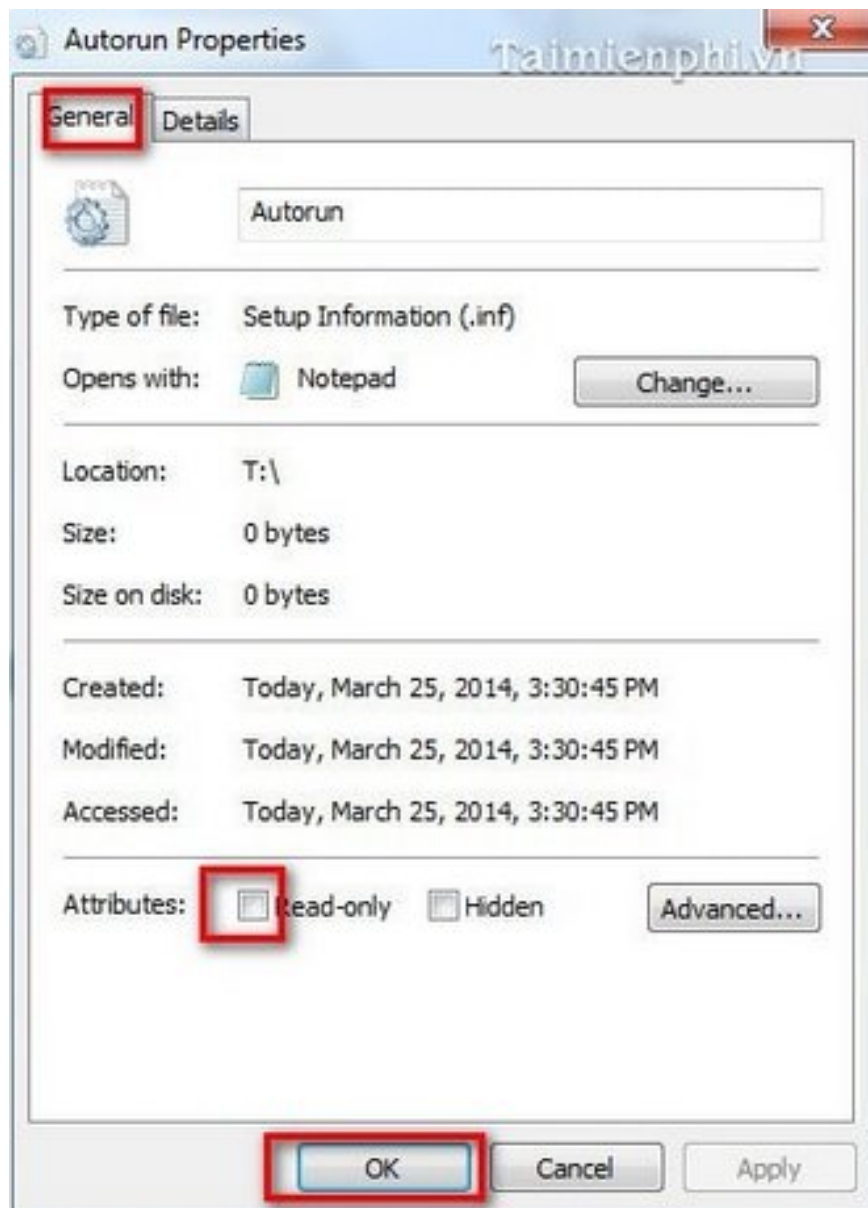
- When the Notepad window appears, you can type anything you want or leave it blank. Then press **Ctrl+S** to save the file, rename it to **autorun.inf** , and save it to a USB drive.



- Next, go to the USB drive, right-click on the **Autorun.inf** file you just created, and select **Properties**.

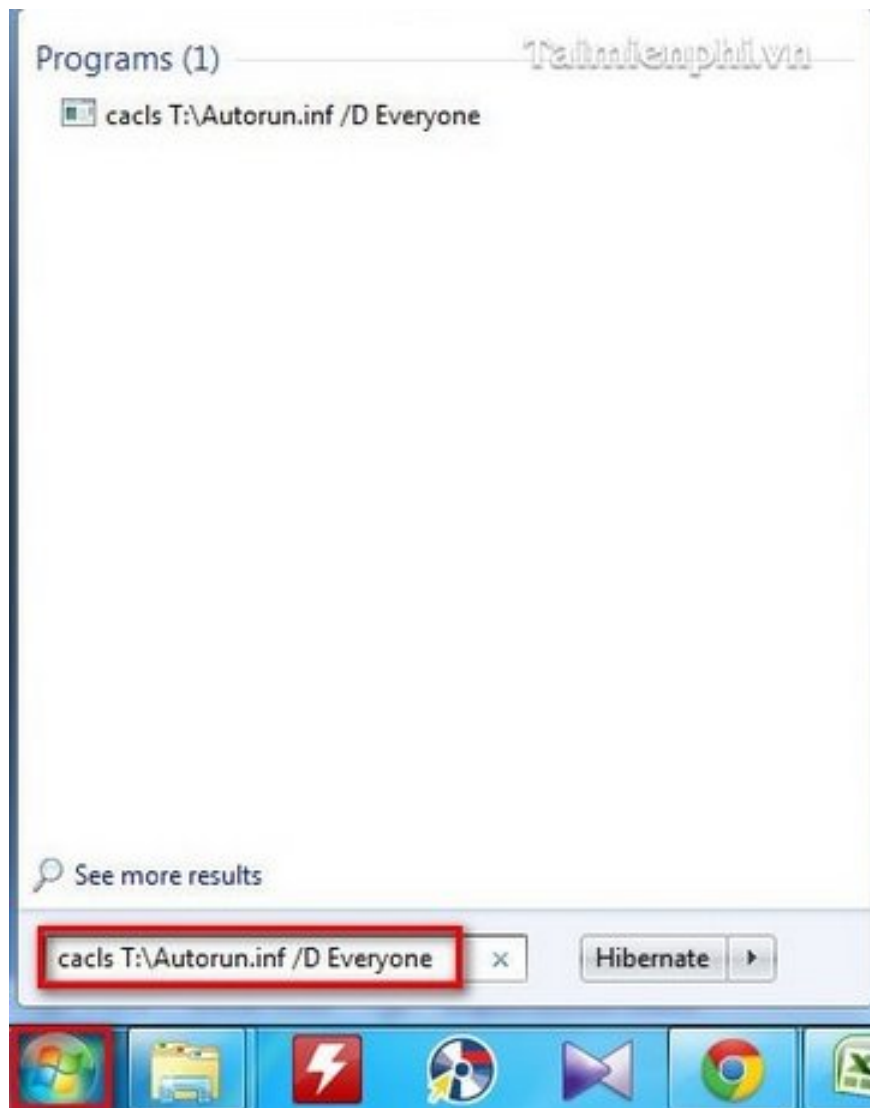


- In the **General** section, click on the **Read-only** box and then press **OK**.

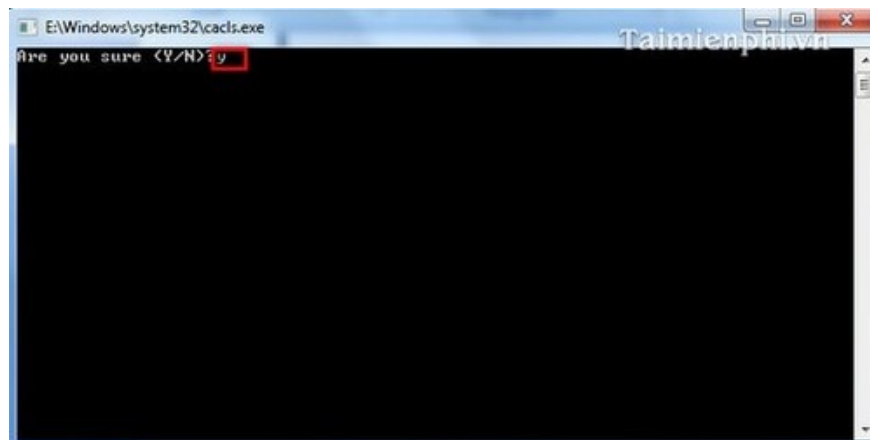


Step 4 : Restrict all access to the Autorun.inf file you just created.

- Click **Start** , type **cacls [USB drive name]:Autorun.inf /D Everyone** and press **Enter**. In my case, I would type **cacls T:Autorun.inf /D Everyone**



- A window will appear; press **Y** , then press **Enter** , and you're done.



Hopefully, with our sharing, you now know how to prevent the Autorun.inf virus with just a few simple manual steps without using any software. Additionally, you can refer to and use the USB protection software available in TipsMake to absolutely secure the data on your USB drive.

There are many ways to remove Autorun viruses nowadays. In addition to the method above, you can remove Autorun using commands in CMD. Refer to the guide on how to remove Autorun viruses using commands on your computer/PC for more information.

You finished reading the article "**Protect your USB drive from Autorun viruses without using software.**" 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.