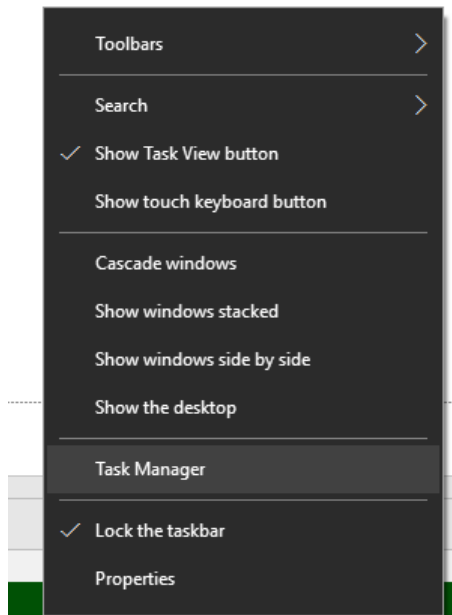


Look for this process wscript.exe



If have
wscript.exe, it's
mean you are
shortcut virus
bot. Then you
cannot follow
this LDP.

Right Click on your computer task
bar and open Task Manager.

A screenshot of the Windows Task Manager Performance tab. The tab is green with a white header. It shows the 'Performance' tab selected. Below the header, there are four columns: 'Name', 'CPU', 'Memory', 'Disk', and 'Network'. The 'CPU' column shows 2%, 'Memory' shows 31%, 'Disk' shows 0%, and 'Network' shows 0%. The 'Name' column lists four applications: 'AVG User Interface (32 bit)', 'Firefox (32 bit)', 'Microsoft PowerPoint', and 'Task Manager'. The 'CPU' column shows 0%, 0%, 0.3%, and 0.3% respectively. The 'Memory' column shows 5.7 MB, 261.7 MB, 47.7 MB, and 10.1 MB respectively. The 'Disk' column shows 0 MB/s for all. The 'Network' column shows 0 Mbps for all.

Name	2% CPU	31% Memory	0% Disk	0% Network
Apps (4)				
> AVG User Interface (32 bit)	0%	5.7 MB	0 MB/s	0 Mbps
> Firefox (32 bit)	0%	261.7 MB	0 MB/s	0 Mbps
> Microsoft PowerPoint	0.3%	47.7 MB	0 MB/s	0 Mbps
> Task Manager	0.3%	10.1 MB	0 MB/s	0 Mbps

A screenshot of the Windows Task Manager Performance tab showing system resources. The table lists various system components and their resource usage.

Services and Controller app	0%	2.2 MB	0 MB/s	0 Mbps
Shell Infrastructure Host	0%	3.8 MB	0 MB/s	0 Mbps
System and compressed memory	0%	123.3 MB	0 MB/s	0 Mbps
System interrupts	0%	0 MB	0 MB/s	0 Mbps
Windows Explorer	0.8%	37.1 MB	0 MB/s	0 Mbps
Windows Logon Application	0%	0.9 MB	0 MB/s	0 Mbps
Windows Session Manager	0%	0.2 MB	0 MB/s	0 Mbps
Windows Start-Up Application	0%	0.6 MB	0 MB/s	0 Mbps

How to Secure Your USB Drive and Prevent It from Spreading Virus

By : SIAT

How to Secure Your USB Drive and Prevent It from Spreading Virus



You must prepare a brand new USB 8GB pen drive to learn this !!!!

Here, we will discuss the preventions in common two situations:

- Stop your USB flash drive from being infected
- Secure your USB drive from various virus attacks

1. Secure the USB Flash Drive

- This method utilizes the security permission of the **NTFS file format** to safeguard your USB drive.
- **Note:** Fat32 is a default file system for many USB drives and it is excellent if you use it on different operating systems like Windows, Mac OS and Linux but if you are using Windows primarily, you can convert the file system to NTFS in a safe manner. Additionally you should not try converting the USB drive to NTFS if the size is lesser than 2GB as that may reduce the performance of the USB drive.

Step 1



Device Manager

- Go to the **Device Manager** after inserting the USB drive.



Step 2

- Right-click on the USB drive found under the Disk drives section and select **Properties**.



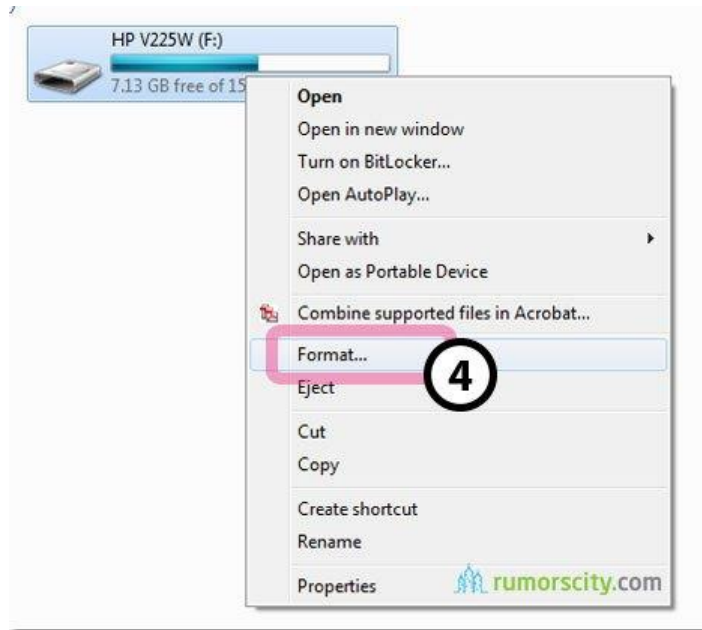
Step 3

- Under the Policies tab, go ahead to the **Removal Policy** tab and select the **Better Performance** option.



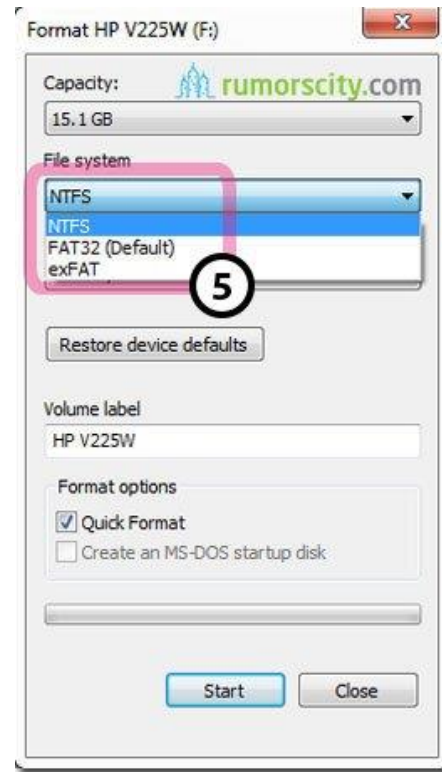
Step 4

- Now right-click on the USB flash drive icon and choose **Format** by going to **My Computer**.



Step 5

- You have to make sure that the **NTFS** is selected from the File system menu.

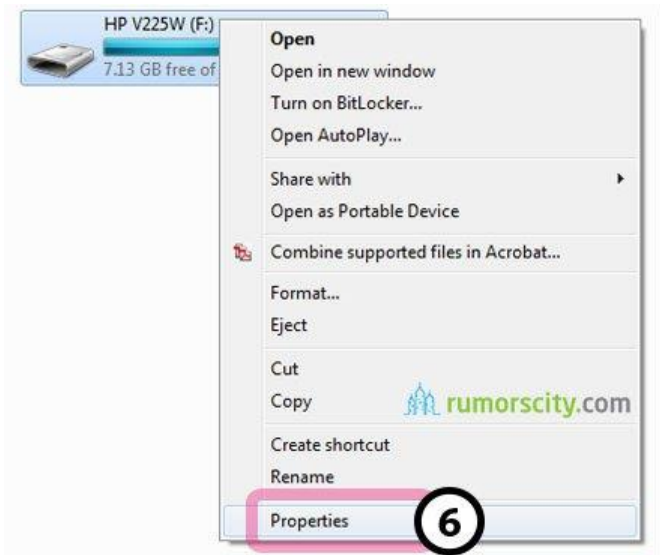


Step 6

- Click the **Start** button to format the flash drive utilizing the NTFS file system.
- Now that the process for the flash drive format complete, configure the root of the USB flash drive so that it is in the **read-only** option.

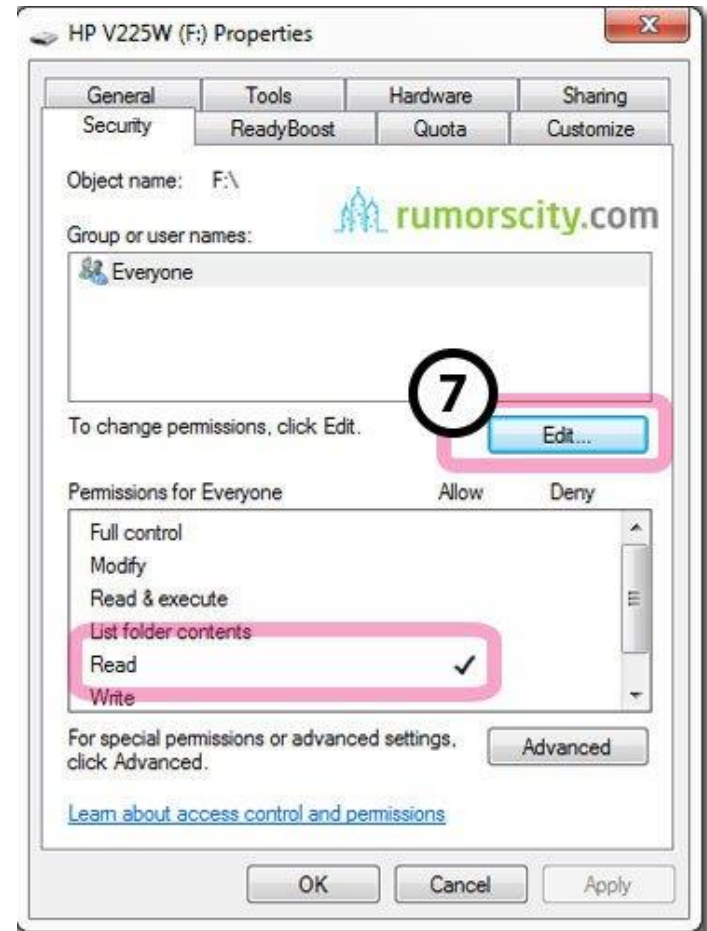
Step 1

- Go to **My Computer**, right-click on the USB flash drive and after that, select the **Properties** option.



Step 2

- Now go on to the **Security** tab and select **Everyone** access only **Read-only rights** to the root folder.



Step 3

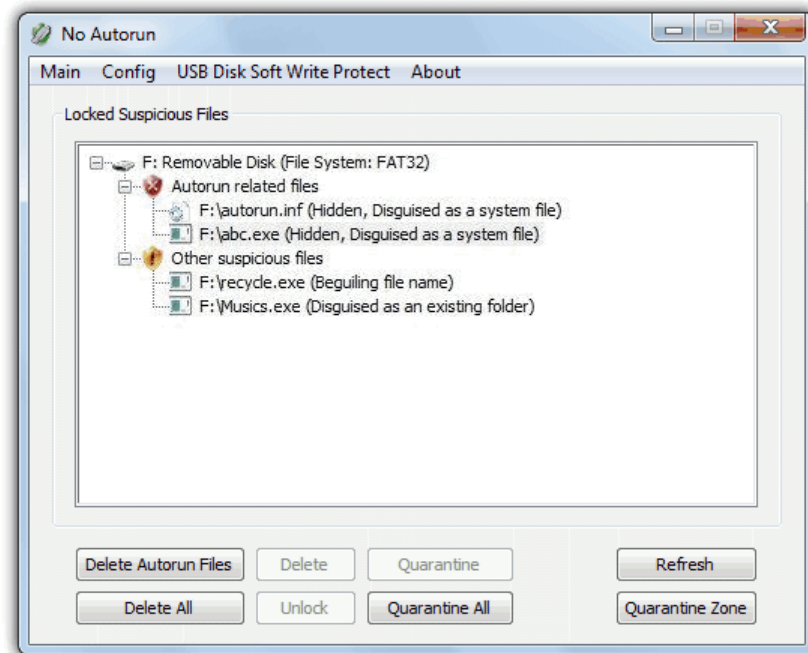
- As a final step, you can create a folder named **Write** and allow it to read or write. If you follow the steps mentioned above, viruses and malware cannot write in the root of the USB flash drive. Additionally, You can always save your data in the **Write** folder/ My File / etc names that you like.

2. Keep your Windows safe from USB Drive attacks

- Disable the **Autorun** feature in your USB drive, to prevent viruses in the USB from attacking your computer. This way, the drive won't start automatically as soon as you plug it in your computer. (Usually your **autorun** file would be infected by the virus and the virus is hidden in that file in the USB drive).

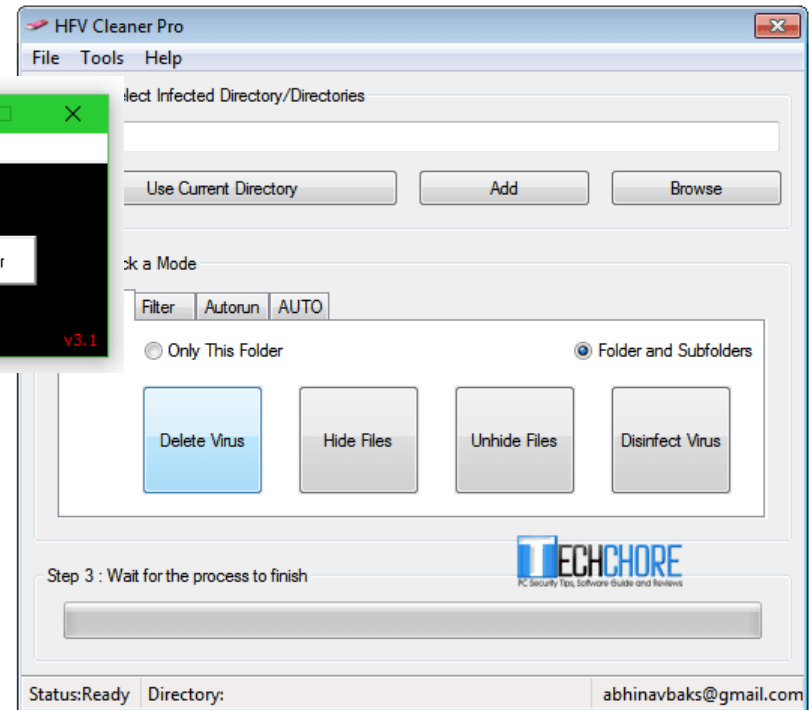
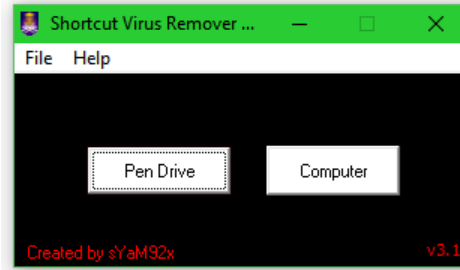
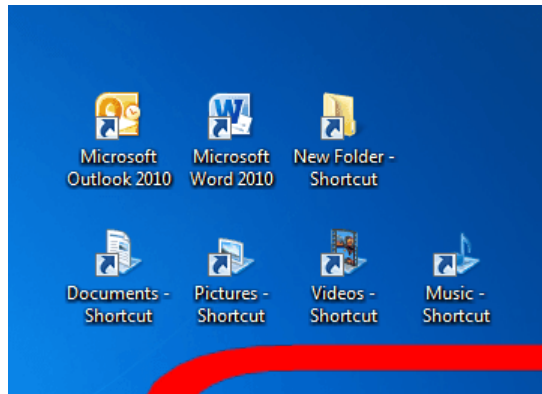
In order to disable the autorun feature of your USB drive, use this registry fix:

- We use software



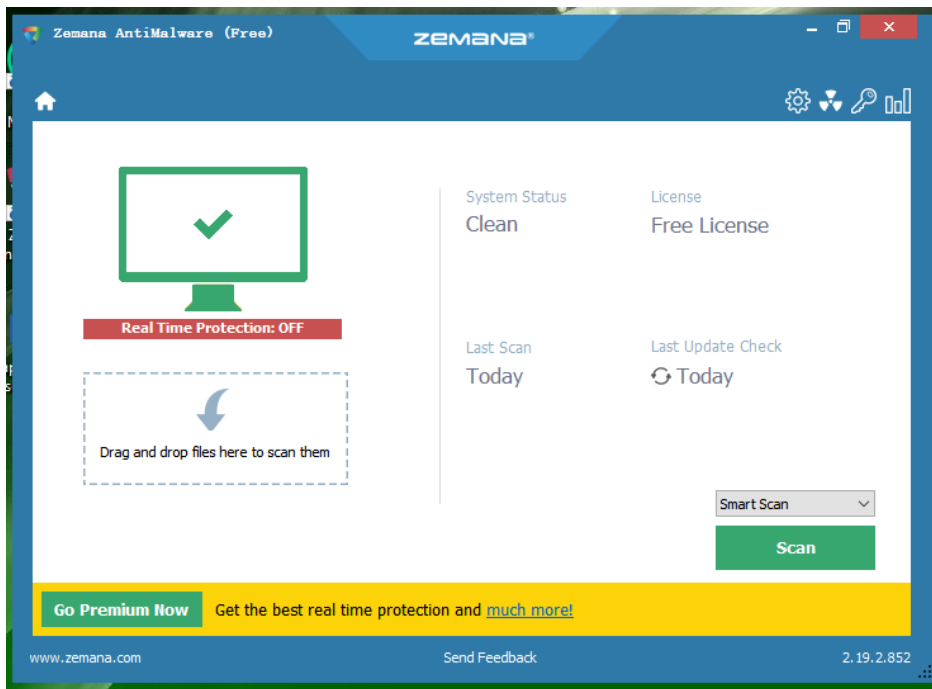
For those which infected pen drive

- We use software







Good Free Software 1

Zemana AntiMalware Free is an on demand malware scanner designed to clean your PC from all the infections that have taken place on your PC. Its unique cloud capability scanning technology will remove all types of malware infections, viruses, trojans, worms, rootkits, bootkits, unwanted apps, browsers add ons, adware and even those annoying toolbars!



Good Free Software 2

Free Download Manager

Download Accelerator	Smart Video Grabber	Multi-Talented Manager	Safe and Absolutely Free
			
Accelerate downloads by up to 6 times, resume broken download. EagleGet saves your time, nerves and money.	Download video from any website. Specially optimized for 1080p, 720p HD and HTML5 online videos.	Task Scheduler, Malware Checker, MD5/SHA1 Verifier... Rich features to help you get everything done.	EagleGet is absolutely free, designed without any feature or time limitations. No spyware or malware!
Quick Download	Quick Download	Quick Download	Quick Download

Download EagleGet v2.0.4.9 (MAR 12, 2016)

Good Free Software 3

“Best & Free” uninstaller for Windows

The advertisement features a background image of a smiling woman with blonde hair and blue eyes, looking at a laptop. The laptop screen displays a Windows taskbar and a list of installed programs. Overlaid on the image is the text 'IObit Uninstaller 5' in a large, white, sans-serif font. Below this, in a smaller white font, is the text 'Improved Powerful Uninstall to Remove Stubborn Programs & Plug-ins' and 'Enjoy Cleaner, Faster PC & More Secure Online Browsing'. A prominent green button with the text 'Free Download' is centered below the text. At the bottom, in a small white font, it says 'V 5.3.0 | 12.5 MB' and 'Supports Windows XP/Vista/7/8/8.1/10'.

IObit Uninstaller 5

Improved Powerful Uninstall to Remove Stubborn Programs & Plug-ins
Enjoy Cleaner, Faster PC & More Secure Online Browsing

Free Download

V 5.3.0 | 12.5 MB
Supports Windows XP/Vista/7/8/8.1/10

Good Free Software 4

Pls install and use free version and you will found a lot of unwanted things in your computer



SUPERAntiSpyware®
Remove spyware, NOT just the easy ones!

Home | Download | Purchase | Press Releases/News | Support | Forums | Blog | Company | Contact Us

New Version 6.0 Available Now!

Over **50 MILLION** downloads worldwide!

Free Edition
Download

Portable Version
Download

Professional Edition
Download Free Trial

Educational/Enterprise
Licensing

Featured on...

NEW! SUPERAntiSpyware Version 6.0

The banner features a background of binary code (0s and 1s). On the left, there are three overlapping screenshots of the SUPERAntiSpyware software interface. On the right, there are four large, rounded rectangular buttons in red, blue, green, and orange. Below these buttons, there are several logos for media outlets and partners, including CNET, Download.com, NBC, Clark Howard, Computer America, and SnapFiles.