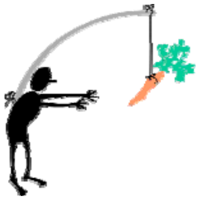
3 Steps to broaden you from Viral Attacks:



1- Motivation:

USB keys are Hot Plug-and-Play devices that are easy to install and use on the move. Not only that but also, USB keys are made of FLASH technologies, that means they can be easily written, erased & re-written again and again. These factors appealed viruses' developers so much as they constitute an easy path to a physical medium allowing them to spread their viruses.

Knowing that a USB Key is considered as a removable hard disk, it might host an "AUTORUN.INF" – an automatically running file that might contain a link to an executable which could be run when double clicking the USB KEY icon on opening.

The Basic idea for prevention is through storing an empty "AUTORUN.INF" file that is READ-ONLY & HIDDEN which cannot be overwritten in order to forbid viruses from copying themselves to your USB & proliferating on each USB usage.

2- Implementation

A. Create an EMPTY text file on your USB KEY called "AUTORUN.INF" with Read-only, and Hidden attributes.

B. Convert the USB KEY to NTFS in order to avoid overwriting of this file by issuing the following command from a Command prompt.

   - **`CONVERT G: /FS:NTFS`**
   - `For Graphical implementation, Cf. Appendix-4-1.`

C. Change the attributes of this file to deny overwriting by issuing the following command from a Command prompt.

   - **`CACLS AUTORUN.INF /D everyone`**
   - `For Graphical implementation, Cf. Appendix-4-2.`

Rule of Thumb:

Never double click the icon of a USB key, always use, Right-Click & Open.
This is also applicable in our case when an empty “Autorun.inf” file is created in order not to fool Windows by asking to run an empty FILE.
Doing so might produce some difficulties when ejecting the USB Key.

3- Conclusion

Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation.

A virus might corrupt or delete data on your computer, use your e-mail program to spread itself to other computers, or even erase everything on your hard disk.

Viruses are most easily spread by attachments in e-mail messages or instant messaging messages or USB Keys. That is why it is essential that you never open e-mail attachments unless you know who it's from and you are expecting it.

Viruses can be disguised as attachments of funny images, greeting cards, or audio and video files.

Viruses also spread through downloads on the Internet. They can be hidden in illicit software or other files or programs you might download.

Prevention is better than cure, so, common sense is needed & all precautions should be taken when handling unsecured files.

Good Luck,

BR,

Nazih SALHAB

****

Applying this procedure means that you agree and consent to GNU GENERAL PUBLIC LICENSE, Sections Disclaimer of Warranty & Limitation of Liability.

This Procedure is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details at http://www.gnu.org/licenses or write to the Free Software Foundation,Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

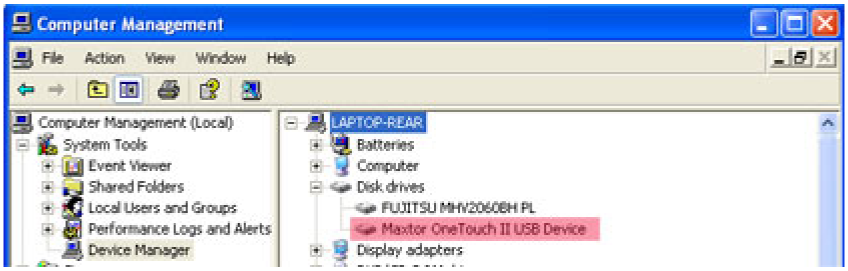
****

4- Appendix:

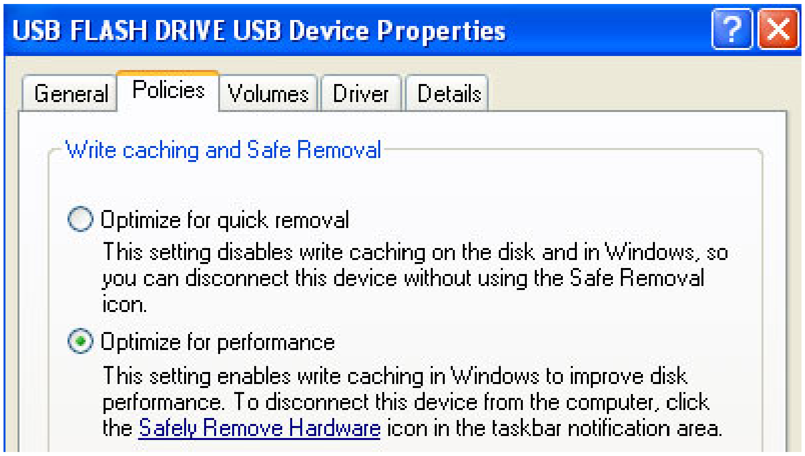
4.1.How to enable USB drive with NTFS?

1. You need to connect your USB device to your computer, that's for sure. Right-click on My Computer from the desktop and choose Manage.

2. Click on "Device Manager" and expand out "Disk Drives". There is maybe couple of drives depending on how many USB drive & hard drive connected to your PC.



3. Right click on USB drive and select "properties". After that, click on the "Policies" tab and choose "Optimize for performance" radio button. Finally click OK and you are done!



Write caching and Safe Removal

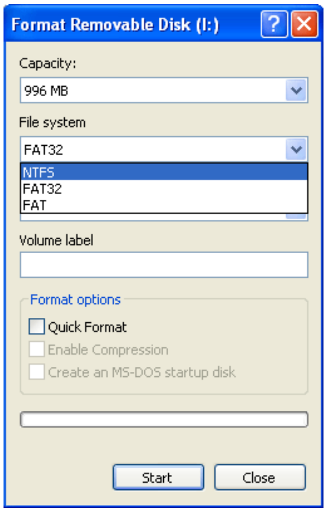
○ Optimize for quick removal

This setting disables write caching on the disk and in Windows, so you can disconnect this device without using the Safe Removal icon.

● Optimize for performance

This setting enables write caching in Windows to improve disk performance. To disconnect this device from the computer, click the Safely Remove Hardware icon in the taskbar notification area.

4. Click OK.
5. Open My Computer.
6. If you right-click on USB drive and select "Format...” you will see NTFS is now available.



Capacity: 996 MB

File system: FAT32

NTFS
FAT32
FAT

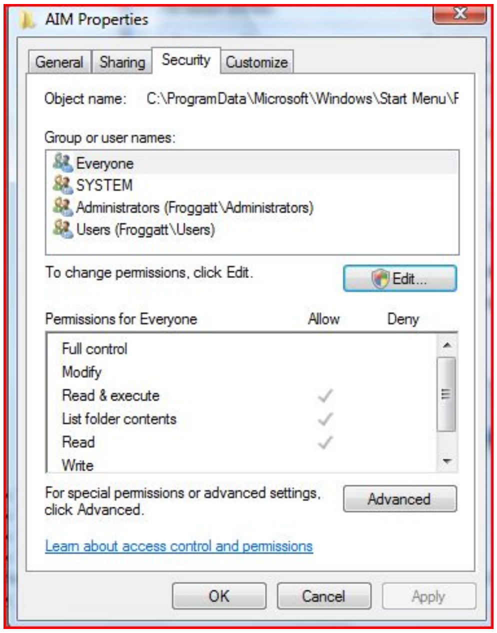
Volume label

Format options

□ Quick Format
□ Enable Compression
□ Create an MS-DOS startup disk

4.2.How to Deny overwriting from Everyone?

1- Right click on the "AUTORUN.INF" file & choose Properties
2- Choose the Security Tab
3- If "Everyone" user doesn't exist, just add
4- Select all the DENY permissions for this user.



Object name: C:\ProgramData\Microsoft\Windows\Start Menu\F

Group or user names:

Everyone
SYSTEM
Administrators (Froggatt\Administrators)
Users (Froggatt\Users)

To change permissions, click Edit.

Permissions for Everyone	Allow	Deny
Full control		
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write		

For special permissions or advanced settings, click Advanced.