Trick to prevent 100% virus infection from USB, memory card, phone to computer

Here are 3 extremely useful tips to help you prevent 100% virus infection from USB, memory card, phone to computer.

Computers infected with viruses from peripheral devices are a very common problem and are difficult to control. So how to prevent 100% of viruses from spreading to your computer?

Equipping basic knowledge and "learning" a few tricks for preventing and preventing the threat of viruses on Windows is something that any user needs to do immediately, even if you are a person If you have experience or not, you should know. Because, if the computer is infected, performance can be reduced and important software or document applications can be destroyed by viruses. So it is not too late for you to learn some tricks to prevent viruses from spreading from peripherals to computers, this article will share with you how to block viruses from USB, memory cards, and phones into your computer. results that anyone can do.

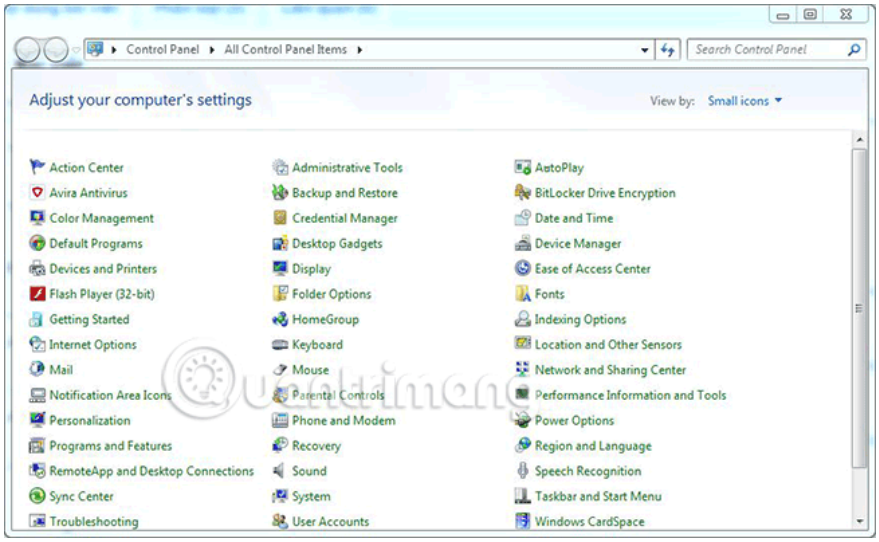
1. Learn about the safe anti-virus mechanism on the Vietnamese military

1. Turn off Auto Play on the system

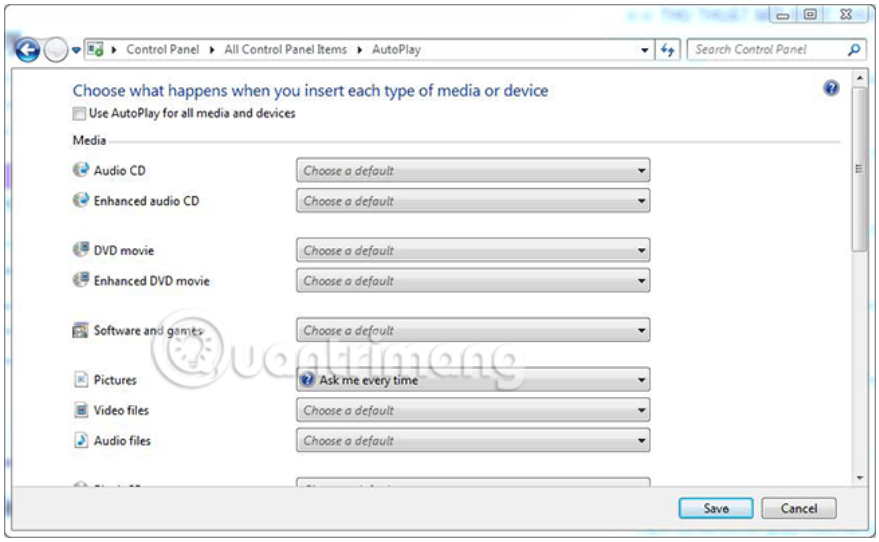
When you connect peripheral devices such as USB, memory card, phone, CD / DVD, . to the computer via USB port, the computer will automatically open the device or run the files automatically in the device. suffering from that malicious code is the virus will quickly spread to the computer. This is one of the very dangerous virus links and you need to turn this feature off so as not to affect the operation of the system.

To turn off Auto Play on Windows, do the following:

Step 1: Access the *Control Panel* via the search bar and select Auto Play.



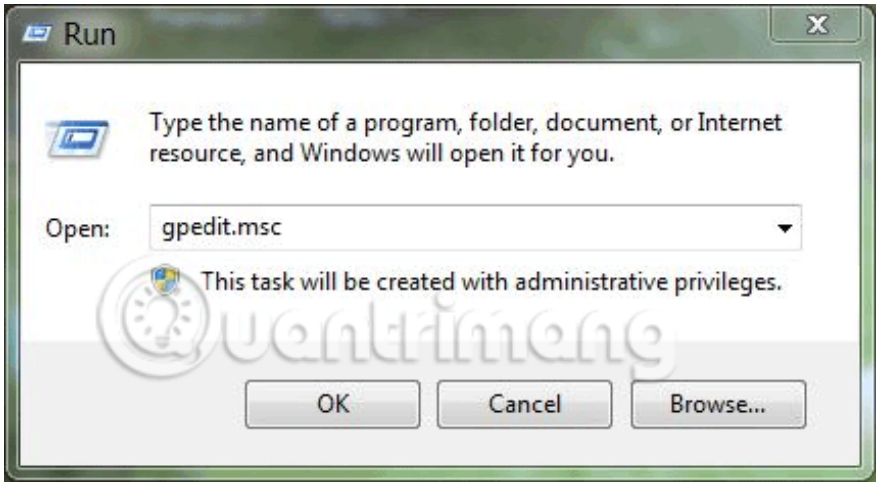
Step 2: Uncheck the box " *Use Autoplay for all media and devices* ".



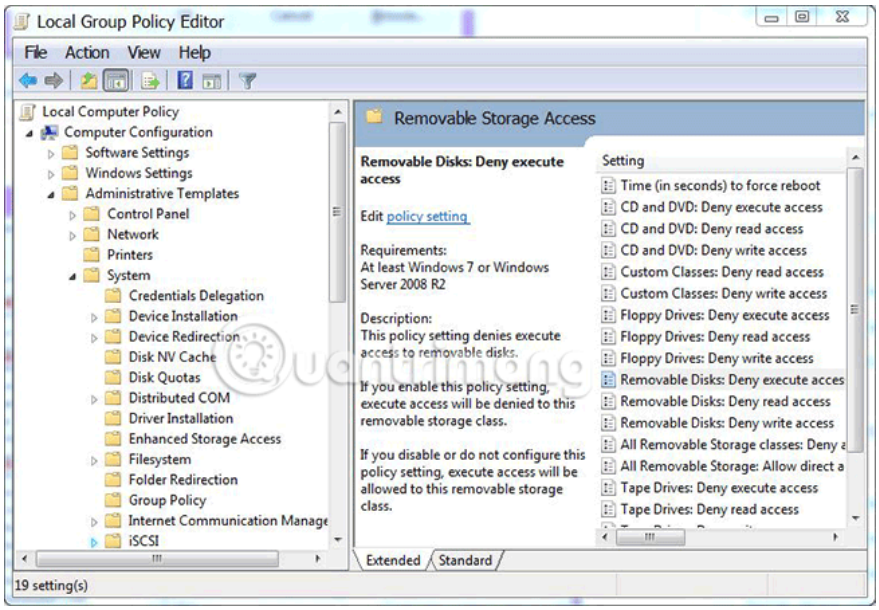
2. Prevent running virus files directly from USB

This trick is a great way to prevent all '.exe' files, usually to run applications and activate the virus. Since we only use USB to store documents, documents and images as the main reason, turning off this option makes your computer quite safe from USB virus infection. To do the following:

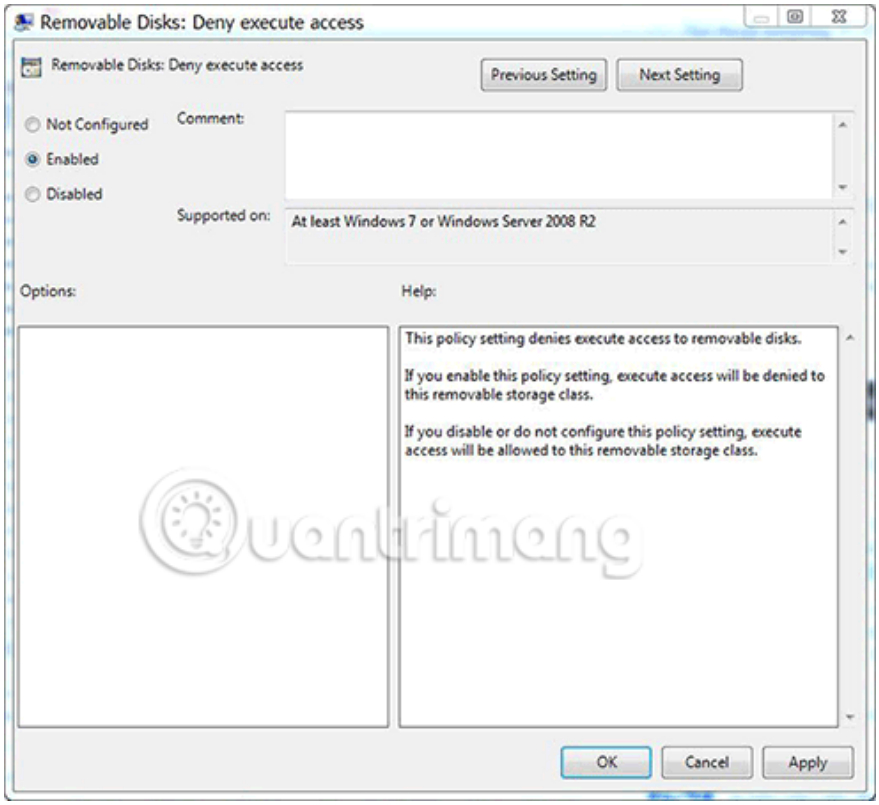
Step 1: Open the Run dialog box and enter the command *gpedit.msc* and click *OK*.



Step 2: Next, go to the following link: *Computer Configuration> select Administrative Templates> select System> select Removable Storage Access> find on the right of the item named Removable Disks: Deny Execute Access* .



Step 3: Double-click the *Removable Disks: Deny Execute Access file* you just found and turn on *Enabled* , then click *OK* to apply the change.



After successfully setting up the above, all the files in * .exe format will not be able to run directly on the USB, this also means that even if you accidentally hit the wrong file, it is okay. because it cannot run.

In many cases, many people will feel inconvenient if they cannot run the * .exe file, to solve this problem, you should use Winrar to compress the file in .rar or zip format. The way it works is as follows: When you double click to run the executable file in the compressed file, the application will be unzipped to the system temporary folder so it can run normally and is not afraid of virus infection if Unfortunately the application has a virus attached.

Note: To be more secure, you should compress important files before copying to USB, because documents to weight compressed files will be very safe.

3. Install antivirus software

In addition to the above two ways, you should install an antivirus program strong enough to protect your computer from the dangers of malicious programs and prying eyes. If conditions permit you to use anti-virus software for a fee, no free software still provides good protection for users, after all, a home with a port will be more secure, right. Have you seen the Top 10 most effective anti-virus software for Windows that TipsMake.com shared before? One thing to keep in mind when plugging in external storage devices is to scan them once to make sure the device is not infected.

So above, we showed you how to prevent USB, memory card, and phone from infecting your computer with three simple tips, thus helping you to protect your computer from viruses and spyware. Malicious messages, . This is really useful for all users, especially those who often have to work with USB or use memory cards, phones to connect to computers.

Hope you enjoy this article.

Maybe you are interested:

1. 4 great USB utilities that you may not know yet
2. 4 virus fake troll friends extremely happy
3. How to fix when Facebook is infected with virus

You finished reading the article "**Trick to prevent 100% virus infection from USB, memory card, phone to computer**" 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.

© 2019 TipsMake.com