Create Your Own Google Search Page..

//////////*1000+ HACKING TRICKS & TUTORIALS - ebook By Mukesh Bhardwaj Blogger - Paid Version - only @ TekGyd | itechhacks | Mukeshtricks4u*///////

Step 1: Open Your Browser.

Step 2: Go To www.goglogo.com.

Step 3: Type Your Name In Search Barr.

Step 4: Click On "Create My Search Page Now".

? Top 5 Security Tips To Protect Your Computer From USB Viruses]]

With increasing anti-virus security in place against email-aware viruses and malware, hackers are turning their attention to less well-defended routes such as USB drives. This is the latest method that's used by hackers to torment innocent users. However, there are ways you can protect your computer from USB and Pen drive viruses.

Invest in an excellent anti-virus program that has built in USB virus scan and remover. These anti-USB virus scan programs not only protect your computer from USB Autorun viruses but can also clean worms, Trojans and viruses in your USB memory sticks.You can try anti-virus programs for USB virus such as USB Virus Scan, USB Drive Antivirus and so on.

1.Block USB Viruses:

==========

2.Disable Your Computer's Autorun Feature
When you plug in a USB drive stick into your system, the Autorun feature initiates automatically. If your USB contains any virus programs, it'll use the Autorun feature to infect your computer. To protect your computer, disable the Autorun feature.You can disable the Autorun feature via the Control Panel.
Alternatively, you can use antivirus software to disable and enable the Autorun feature whenever you want. Additionally, these USB blocking softwares allowsystem administrators to specify which removable storage drives users can access.
Keeping your USB device driver updated is a good way to ensure greater stability for your USB drives. While this won't help eradicate USB viruses, USB device drivers are constantly updated to block viruses and deliver timely warnings. You can update your USB device drive from your Windows Computer Management feature in the Control Panel.

==========

3.Update Your Device Driver:

USB firewalls prevent Windows OS from processing malicious programs when a virus infected portable USB device is opened. USB firewalls monitor only your USB devices, and not your CD and DVD drives. By using USB firewalls, you'll be enabling a basic level of protection from the autorun.inf viruses that spread from portable USB devices.

==========

4.Use USB Firewall Software:

Viruses are sometimes created via damaged documents. If you are transferring a set of files to your USB drive, make sure the transfer is complete before you eject the device. Always use the Safely Remove Hardware feature of Windows OS. This is because partially transferred or damaged files can in turn corrupt other files on your USB drive…

==========

5.Always Safely Remove USB Devices:

==========