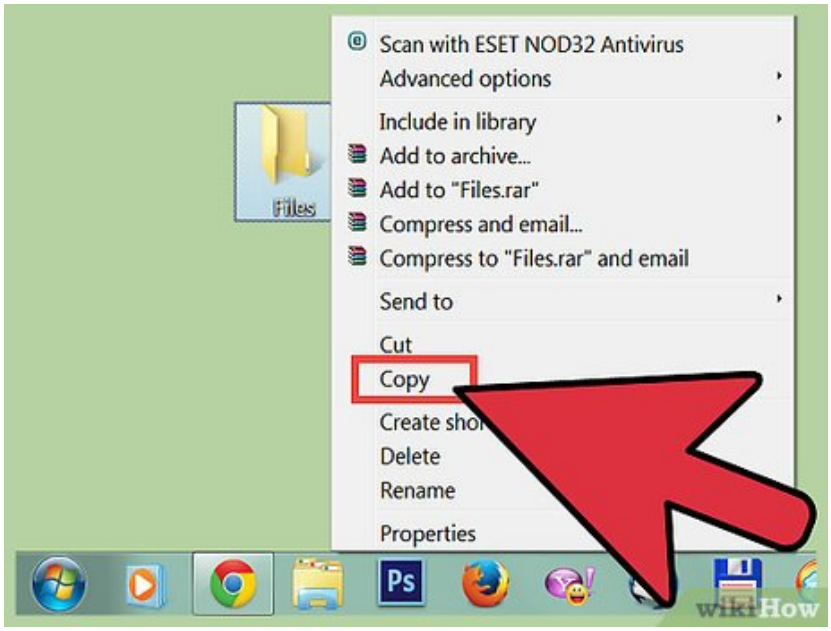
How to Fix a Malware Infection on Your Computer

Viruses, malware, and spyware can wreak havoc on your computer; they can cause damage to your important files or even allow hackers to steal important information. Worst of all, your computer can become unusable, requiring purchase of a...

Method 1 of 2:

Fixing a computer that can boot up

1. 

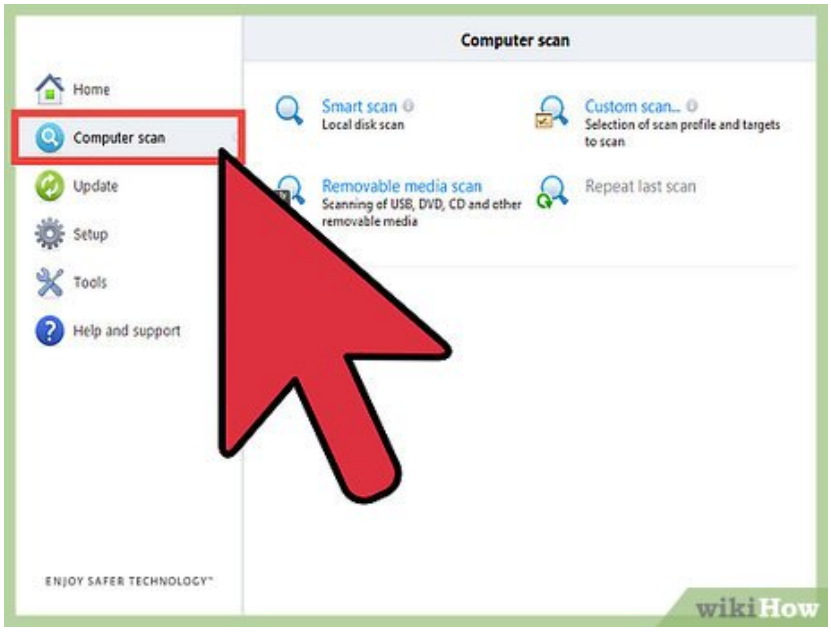
Back up your important files. If you have a particularly stubborn infection on your computer, it may become impossible to solve the infection without reinstalling your operating system. Sometimes, using anti-malware programs may also damage your computer.

1. Copy your files to a USB flash drive.
2. If you have access to an online file backup service, use that.

2. 

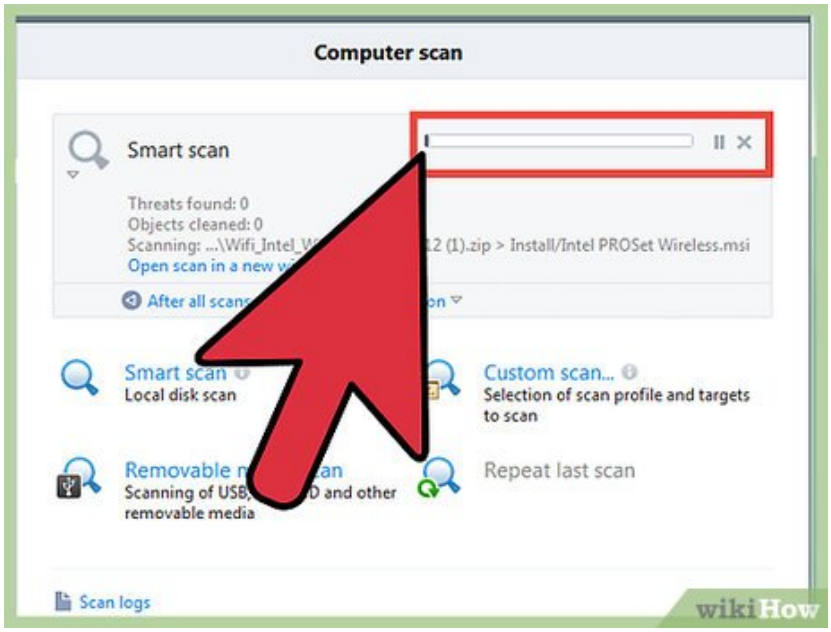
Download an anti-malware program. There are many free options available, such as Malwarebytes Antimalware or SuperAntiSpyware. Some anti-malware programs allow on-demand free trials, and are therefore also usable for removing malware.

1. If you already have an anti-malware program installed, then update the virus definitions. Anti-malware definitions need to be kept up-to-date in order for the anti-malware programs to remove viruses.
2. If a virus prevents you from downloading or running an anti-malware program, run the program in Safe Mode with Networking by tapping F8 repeatedly when your computer is starting up, and selecting "Safe Mode with Networking". This works because only operating system core files start up in Safe Mode.
3. If running the anti-malware program in Safe Mode also does not work, you can use Malwarebytes Chameleon or Rkill to kill malware processes which may be preventing you from running an anti-malware product.

3. 

Scan with the anti-malware program. Quarantine or clean any infections that are found.

1. Be sure to turn on "Scan for Potentially Unwanted Programs" in the program's settings. Some programs may have legitimate uses, but can also be used by hackers for malicious reasons; this is why they are considered potentially unwanted. Potentially unwanted programs include keyloggers and adware, which may have legitimate uses.
2. Update your virus definitions before scanning.

4. 

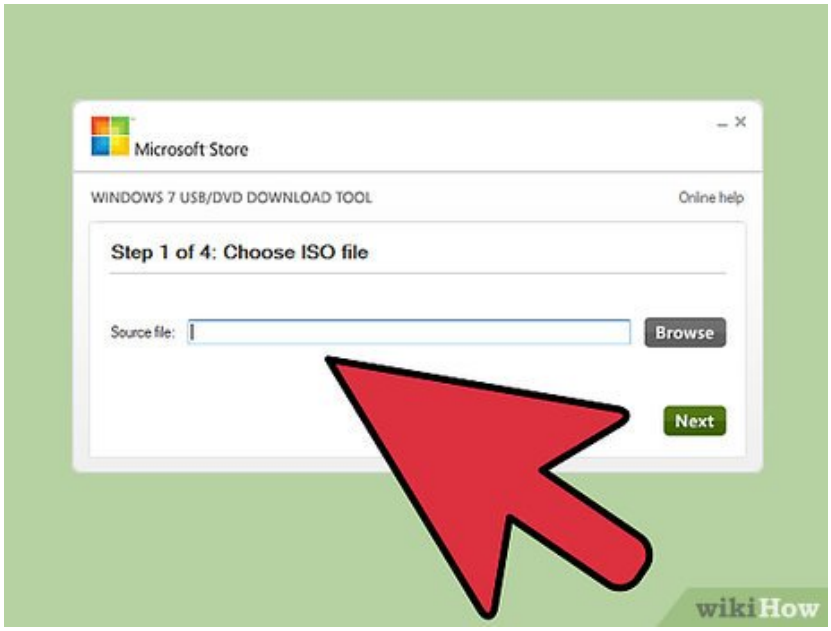
Check to see if the problem has been fixed. If it is not, then install a different program and see if it becomes fixed. If no programs can fix your problem, then you may want to consider reinstalling your computer. Note that there still may be malware left on your computer even if the malware problem appears to be fixed. Use a different anti-malware application, just to make sure.

Method 2 of 2:

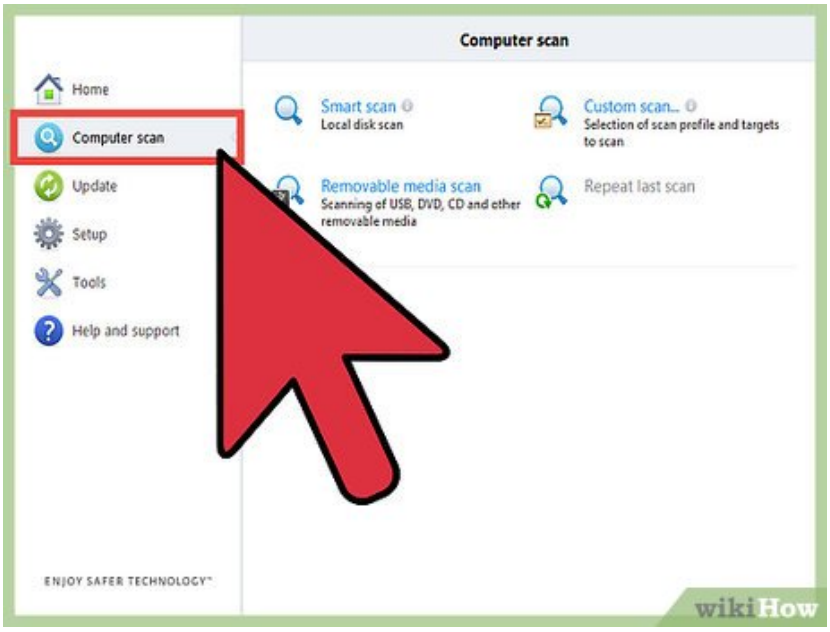
Fixing a computer that cannot boot up

1. 

Back up your important files. You can do this by changing your BIOS settings to allow booting from removable media. Then, you burn Lubuntu, a version of Linux, onto a CD. Insert the Lubuntu Live CD into your computer's CD drive, and restart. You will boot into Lubuntu. Then, you should use the file manager program included with Lubuntu, PCFanFM, to copy your files onto a flash drive.

2. 

Burn a bootable rescue disk onto a CD, and insert it into your computer's CD drive. Bootable rescue disks are provided for free by major anti-malware software vendors, as long as you have spare CDs with you.

3. 

Scan for the malware. The rescue disk should include tools to scan your computer for malware which may be preventing your computer from starting up.