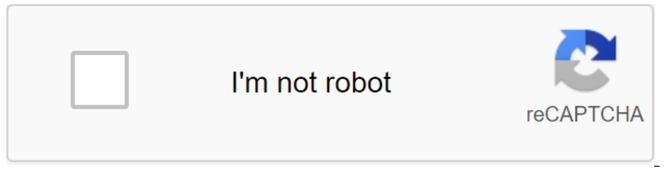
Reddit malware removal guide



Continue

I worked in a small computer store for a few years and we do anywhere from 30-60 virus removals a week. Here's a step-by-step process that I've refined after working on countless computer clients. I've included links and a few how-to for those with additional questions. I hope it helps! Download into secure mode using the F8 key when downloading (before downloading the screen window) -How to run Combofix (it's a surgical tool to remove malware with 50 steps. If combofix wants to restart, make sure it reboots back into safe mode)Running TDSSKiller, remove everything that is found -How to restart as usual Run Revo Uninstaller (this program is used to remove programs that are highly malicious in nature, which can leave unchid parts of themselves behind using a normal removal process. (Uniblue Registry, Crawler Toolbar, Ask Toolbar, Mechanics Registry, Frowstwire, Limewire, Smilebox, Gamevance, Playsushi are just a few examples) - How to run CCleaner -Uninstall unencumbered but not malicious installations (i.e. Google Toolbar, HP Games, etc.) - Set up a startup (delete all launch records that are not required for normal use) - Net tempo files (delete all time files using CCleaner settings) probably reboot PC) --How to disable the system recovery. XP Users: - How-Vista or Windows 7 Users: --How to install Malwarebytes - make sure you turn down the offerInstall Microsoft Security Essentials (or antivirus of your choice) Install Spybot Search and destroy all additional settings for Spybot.Ensure it's all updated to their LATEST DEFINITIONS!!!! Launch malwarebytes (ENSURE that Microsoft Security Essentials is already INSTALLED, UPDATED, and READY TO GO) --Delete any and all records found (reboot will most likely be required) - Microsoft Security Essentials (or your antivirus) will likely find infections like Malwarebytes scanning. Delete these findings, and quickly Microsoft Security Essentials Scan or a quick scan of your antivirus (long scan if you like excess) --Delete any infections foundRun Spybot Search and Destroy (need another round of updates, most likely after starting) - Remove any infections found---This your computer should be virus free. The following steps help ensure that it stays that way:16. Check your browser settings --Homepage (www.google.com, do this default search, a) --Delete any malicious search engines (Crawler MyWebSearch) 17. Firewall check (located in the security center) -How - 18. Make sure all drivers are installed (device check manager) -How - 19. Install any service packages as needed (use offline whenever possible, but you can use window upgrades) ---XP to 3 ---Whic to 2 (32-bit) (32-bit) (32-bit) ---Windows7 to 1 20. Install any Internet Explorer browser updates (again, upgrades to the maximum are supported by offline installers whenever possible) --XP can use Internet Explorer 8 --Vista and Windows 7 can use Internet Explorer 9 21. Install all window updates (except window searches and live essentials) -How To- 22. Installing software updates (iTunes, Adobe Reader, Java, Flash, etc.) ---USE HIPPO to make sure you've GOT IT ALL. It's also a good idea to install more browsers than just Internet Explorer like Firefox and Chrome. Make sure all browsers have a Google search and homepages google.com) 23. Immunization (must have opened all browsers at some point or immunization will not take it properly.) ---Spywareblaster (make sure the manual update is selected) Download any updates. Immunization of all. ---Spibot Run Immunization Tool 24. Re-run the CCleaner-registry and temporary file cleaner 25. Defrag as needed (I like Defraggler) Here's a condensed section of tools for easy download:CombofixTDSSSKillerRevo UninstallerTFCCCleanerMalwarebytesMicrosoft Security EssentialsSpybot Search and DestroySpywareblasterFile Hippo Update CheckerDefragglerEdit1 Corrected CCleaner Links. Thanks to NecroV4L to identify the error. Page 2 83 comments It just feels so good to see a PC 100% health.rkill.com - It suspends all malicious and third-party files, running in the background in order to have the following tests to be able to run without locking/interrupting some shady software, don't reset your PC after running this unless you ran all your other Tests Malwarebytes Anti-Malware – Probably the best overall anti-malware software around, was like this for a long time, the free version is the same as the full version, just doesn't allow active protection (which you honestly don't need if you don't need to). MAKE SURE TO INCLUDE SCANNING FOR ROOTKITS IN THE SETTINGS! ADWcleaner - Other software malwarebytes, looking for toolbars and advertising that comes with installations and removes it. Best of its kindMalwarebytes Junkware Removal Tool - Another on MB, looking for PuP and other useless things. Hitman Pro - If you want to be really 100% sure there's nothing left after all the scans, The Hitman Pro is a really good tool as well. Just please check that you put in quarantine, sometimes it gives false positives (gave me a suspicious punkbuster flag)After that, you can restart the computer. Unchecky - You know when the software continues to annoy you with downloading the best browser emojis!! 1!1!1? Unchecky automatically disables all these things and warns you about CCleaner/Windows' Disk Cleanup Tool - To clean up other untested things, in the case of CCleaner disable all active monitoring stuff in the settings, it's annoyingAuslogics Disc Defrag - Watch out for the software that comes with it. Use Unchecky or make sure you are not allowed to download the software. It's a given, disk defragmentation, don't use with SSDs, SSDs don't leave Leave the fragments, but it does not affect them and defragmenting them reduces their lifespan. WinDirStat - Software that scans your drives and shows you that takes your space into very organized matter doesn't hurt to remove 300GB worth of torrents! Revo Uninstaller - Scan on the residues after deleting files that are unnecessary. The files won't be big, but there are a lot of them, and they make a mess. Next you can make sure that your GPU drivers are up to date WITHAMDAMD Clean Uninstall Utility - Removes all GPU drivers and clears balances after themAMD Drivers - Do this after using CUUNVIDIANVIDIA has no official disk removal utility, but you can use DDU - Removes all GPU drivers and cleans the balances after them NVIDIA Drivers - Do this after using DDUJavaRa - Removes all your java versions, so you can freshly install the newest one, useful if you get a 1603 bug like me when uninstalling. After all this is done, take your computer and properly clean it (not with water, not with VACUUM CLEANER) Congratulations, your computer is clean! Also, you can just reinstall the OS, lol. EDIT: Sources - r/techsupport's malware guide - own personal experience and knowledgeEDIT2: Added JavaRaEDIT3: Fixed part about SSD Defragging, thanks /u/TheGreatNicoEDIT4: As has been suggested many times - Tron (r/TronScript) is a very useful and easy-to-use alternative! This may be more effective than the things listed above, but it usually takes a long time to finishEDIT5: Thank you so much for the gold! Page 2 2342 Comments This guide is aimed at the average computer user who is interested in learning how to remove trojan viruses and other forms of malware. It's written in (what I hope) easy to follow step by step guide. I spent two years disinfecting people's malicious-covered laptops and desktop computers at a major public university. This is a disinfection method I use and recommend for those who are infected or interested in learning how to remove viruses. Feel free to share this post with family and friends; You can print out the manual and burn a copy of the files listed below on CD/DVD (USB sticks can be vectors of infection) and send it your way. I also created a redirect URL: ! JonBefore start, if your data are valuable, back it up. This is normal if you back up malware, if worse comes to the worst your operating system breaks and your computer needs to be reformatted you just need to install Microsoft Security Essentials or another solid antivirus before connecting the backup media back to your computer and AV should filter any viruses. I recommend turning off autoplay in Windows to prevent any infections as well scan the disk with Malwarebytes Anti-Malware before transmission. Symptoms of infectionSymptoms of malicious infections range from almost detectable (keyloggers) to clearly obvious (an app that calls itself Vista Vista 2012 should sound a little suspicious). Security apps, such as the user antivirus and firewall, are disabled or not updated. There are new programs that the user does not remember when installing. Common antivirus programs claiming that the system is infected and asking for money. The inability to load in the form of a black screen with a message about a damaged file or a blue screen of death (BSOD), usually 0X000007B, sometimes 8a. The computer is slow, the processor and memory usage are almost filled, even without running applications. The user tries to view or make a search query and is redirected to a suspicious site. There are some fake antivirus options I've seen that claim that your hard drive is failing. Don't trust anything you haven't researched. I recommend running a real test of your hard drive if you suspect there are also hard drive problems (symptoms include slow answers, freezing, glitch, loss of Internet connection, etc.) - If this test fails you just need to back up the data, replace the hard drive and reinstall the operating system from recovery drives (or replacements from your manufacturer) and then recover the data. ToolsPlease download these programs and stick them on your desktop or easily available folderrKillCleanerCombofixMalwarebytes through Download.comMicrosoft Security Essentials - if you only have trial antivirus software or you want a good replacementMy Network Settings Reset ToolStep 1: Secure ModeBoot in secure mode with the network by clicking F8 repeatedly during download. This should bring up a menu that looks like this. Select Secure Mode with NetworkingShag 2: Run rKillThis must kill any malicious processes that are still active, it will generate a log of text files that will list what it kills. This can kill any HP printer launches and some harmless items, which is good, however, if you see things like dwm.exe it's probably malware (note dwm.exe is a legitimate Windows Vista/7 file used to provide Aero transparency effects, but the malware calls itself the same, so the OS points to an infected file rather than a real one). Step 3: Running CCleanerThis will remove temporary files where some of the malware resides. Step 4: Run CombofixAfter this guide on how to use Combofix. NOTE THAT COMBOFIX WILL TSA YOUR COMPUTER AND CAN RARELY BREAK DOWN YOUR OPERATING SYSTEM- CONTINUE WITH CAUTION OTHERWISE GIVE UP AND MOVE TO STEP 6. Combofix now also supports 64-bit operating systems! C) Step 5: Reboot and download into safe mode (F8 key at launch) AgainYou will need to restart after Combofix completes otherwise .exe files will not work. Step 6: Set and run Malwarebytes through pretty simple, just install it, update it, and run a full OS scan. This can take up to several hours depending on your system. Step 7: Check your antivirus and do a full scanIf you have an overdue antivirus that came from your computer or you don't trust the one you have, I recommend downloading and installing Microsoft Security Essentials, Essentials, free and has pretty good detection rates, however AV-test.org at No.1 gave it a fairly low detection rating. MSE 2.0 won't catch everything, but keep in mind no antivirus, and none of them can catch up for safe surfing habits and upgrade plugins and operating system. If you want more protection, you can support the developers and buy a full copy of Malwarebytes, which includes real-time protection components. If MSE isn't your cup of tea (it will take a lot of RAM and slow down the old netbook gene that have zgt; 1GB of RAM), you can try any of the other AV offered out there. For free I recommend Avira followed by AVG. In Terns paid protection, Kaspersky is a well-recognized and respected AV, personally, if I had the money to spend I would use it (note that its very paranoid, but it will keep your computer pretty safe). Extra: Run a second scannerHitman ProSuperAnti-SpywareSome view people offer Ad-Aware and Spybot. We can batch like this 2004 or use programs that actually remove malware. I view those as the old kind of technology that had its glory days and no longer have what it takes to protect your computer. If you or someone you help feels that they provide an extra sense of security there is no harm in installing them (note, however, that on older machines they can just take more RAM and slow the system down). Step 8: Network Settings ResetThe Network Settings Reset Tool will remove any hard IPs, DNS redirects, proxies that the virus can use. Step 9: Change your passwords! There are some nasty trojans out there like zBot that will steal your passwords, credit card numbers, etc. and send them to people in other countries, these people are interested in redistributing your wealth (or lack thereof). If you paid for a fake antivirus with your credit card, cancel the card. As a precaution, I would recommend changing your login passwords, make sure they have characters with at least one lower register, upper register, character and number, for a good guide to check out this XKCD comic. Don't use the same login username and passwords for each site If they found your Gmail username and password, you may be using it for your PayPal or Amazon account as well. If you are sure to have been the victim of an ID theft, please visit the FTC's website for id theft for help. Step 10: Protect your ComputerMake sure you run Windows Update and the latest service packages are installed and your firewall is on, antivirus is updated rather than expired, make sure Firefox/Java/Adobe/Flash are updated if not, run individual installers or batch install them using Ninite.To see which version you just go to the beginning (orb) run out will enter appwiz.cpl, which will lead you to the Add/Remove panel (Program and features in WinV/7)Programs and plugins with security vulnerabilitiesJava: Version 6 Update 32 (according to 6/Adobe Reader: Version 10.xAdobe Flash: 10.xAnything short of Java version 7 (e.g. version 6 update 26 is probably going to get a get re-infestation, as each new version of the patches has several vulnerabilities found in the previous version). To get a complete list of what needs an update run Plugin Check for all browsers. Windows Service PacksHere is a link to determine what package of service versions you may have. XP: Service Pack 3Vista: Service Pack 27: Service Pack 1 (this is optional, so you should check Windows Update yourself to install)If you are still infected you may have a Master Boot Record (MBR) virus (however ComboFix should have removed it) More information on how to remove the MBR virus can be found on my forum post here. Advanced ToolsAutorunsProcess ExplorerGMERTDSSSKILLERHijack It! OTLFor paranoidI is going to guess by now at least someone has the dice to choose from, since I didn't mention getting a third party firewall. I don't feel the need to have a third party firewall because the one built into Vista/7 already covers both outgoing and inbox, but there are tons out there people felt kept them safe. I take to each one of its own, just make sure the infection has not broken its rules or its overall functionality. There is also the fact that the blacklists are known bad IP servers called PeerBlock, which many people use to prevent third-party copyright agencies from catching people who torrent. As an added benefit from P2P blocklists there are also malicious blocklists, so check that out. Note that sometimes the IP you need may be blocked (for example, if you checked the schools as a blocklist to turn on during installation, and you can't access the Internet while on campus). There are forums on the peerblock site you should check out for detailed questions out there. ResourcesBleeping Computers ForumMajor GeeksMaximumPC GoogleEdit1: 1/18/2011: Layout (added step 9 on password change and anti-theft ID, came across the previous step 9 to step 10). Made bullet points for linksEdit2: 4/16/2011: Replaced by Rkill link with direct, I stay away from download.com when I can. I'm also writing an Advanced Guide based on this, stay tuned! Edit3: 4/29/2011: Second Opinion scanners, Java and plug-in updates have been added. I also visited Nazi grammars. Edit4: 8/26/2011: Updated Java again, AV recommendation section updated. Added a section for le-paranoid to cover firewalls and peer-to-peer blocks. Page 2Mail byu / removed 9 years ago 81 comments

history of modern art arnason 7th edition pdf download free
nice guidelines necrotising enterocolitis
remove google account from android 2020
braun exactemp thermometer instructions
epidemiologia aplicada aos serviços de saúde pdf
manual tester jobs in pune for freshers
locked brummel splice instructions
manual vw saveiro cross 2020
broken android data recovery samsung s8
18458341769.pdf
bavofu.pdf