**Cleaning and optimizing a Windows computer safely**

“I do my best to make this all as easy as possible, but there are a lot of advanced operations in this guide compared to the rest of the site.”

*[Page last updated 2017-03-07]*

This is a guide to maintenance for Windows 7 and higher. It will also remove many viruses and repair their damage. These procedures can help machines that are several years old. If your computer is a business machine, please ask your IT department first.

All these tasks have been performed by me or my scripts across tens, hundreds, or over a thousand computers. You can read my qualifications [here](https://decentsecurity.com/#/introduction/).

The order of these steps is purposeful. For example - uninstalling some programs, running a temp file clean, and rebooting can leave them in a broken state.

**Do not use registry cleaners or system optimizers.** [Read why](https://decentsecurity.com/#/registry-cleaners/).

**Do not run Windows 10 Telemetry Blockers/Privacy tools.** They often edit operating system settings they shouldn't touch and carelessly **disable security features**, making you vulnerable and breaking Windows functionality. If you're concerned, use the built-in Windows 10 Privacy control panel, which is enhanced in Windows 10 Anniversary Update. Anything more and you're risking future issues.

**If you are updating a Windows 7 computer that's been off for a year, or installing from scratch**, there are known issues. This is my guide that will save you literally hours of your life: [Windows 7 Fast Update](https://decentsecurity.com/enterprise/#/windows-7-fast-update/).

**1.) Test drive and review errors before starting**

* Hard drives can be the silent cause of unexplainable issues, hanging, and crashing. My preferred diagnostic tool is [WinDlg from Western Digital](http://download.wdc.com/windlg/WinDlg_v1_29.zip" \t "_blank). There's no install needed and it works with any drive, even external.  
  Download, run windlg.exe, and double-click the drive to do a quick test. This will take 2 to 10 minutes.
* The built-in [Windows Reliability Monitor](http://www.howtogeek.com/166911/reliability-monitor-is-the-best-windows-troubleshooting-tool-you-arent-using/) will show you a history of errors and problems on the machine.
* [Expert] See if there have been any recent bluescreens (bugchecks) with [BlueScreenView](http://www.nirsoft.net/utils/blue_screen_view.html" \t "_blank).

**2.) Junk programs uninstall**

This section is for the more technically-minded. If you aren't sure, reboot and skip this.

* Start > type "*Programs and Features*" > Enter

From this view, uninstall anything that you know doesn't belong. Read the prompts you get VERY CAREFULLY to make sure you're not agreeing to leave anything behind. If you **don't** know what doesn't belong or are unsure, don't remove anything. That's okay - we'll address that later.

If the antivirus is out of date or expired or having issues, just uninstall it now. Antivirus that isn't updated within the last day is essentially useless. If the antivirus uninstaller is broken, you can use this tool to manually clear it from the machine: [ESET AV Remover](https://help.eset.com/ees/6/en-US/?av_remover.htm).

**Reboot before doing anything below**

**3.) Windows files clean with cleanmgr.exe**

You can save gigs (often 6GB+) cleaning WinSxS, which no other tool can safely touch. The built-in Windows cleaner was [improved via Windows Update in 2013](https://blogs.technet.microsoft.com/askpfeplat/2013/10/08/breaking-news-reduce-the-size-of-the-winsxs-directory-and-free-up-disk-space-with-a-new-update-for-windows-7-sp1-clients/).

1. Start > type "*cleanmgr*" > Hit Ctrl+Shift+Enter to run it as Administrator.
2. *Disk Cleanup* tab > Check everything > Hit *OK*

Cleanmgr will just disappear when it's done. You do not need to wait for it, proceed to the next step.

**4.) Windows Update cache reset (Windows 7 & 8)**

Completely clear the Windows Update cache. This is safe. The folder will be regenerated. Often saves a gig. You don't need to do this for Windows 10.

1. *Start* > type "*services.msc*" > hit Enter.
2. "*Background Intelligent Transfer Service*" > right click > *Stop*
3. "*Windows Update" >* right click > *Stop*.
4. Delete the folder *C:\Windows\SoftwareDistribution*. If it won't let you, stop the services again.

You do not need to manually start the services.

**5.) Temp file clean with CCleaner**

Normally there's no reason to use a utility like CCleaner. However, this is a cursory cleanup to reduce the number of files that antivirus has to scan.

1. Download and install [CCleaner Free](https://www.piriform.com/ccleaner/download" \t "_blank).
2. Launch CCleaner
3. *Options* > *Monitoring* > Uncheck "*Enable system monitoring*" > Uncheck "*Enable active monitoring*"
4. *Cleaner* > scroll to *Advanced* > Check "*Environment Path*."
5. Run a clean

When cleanmgr and CCleaner are done, **REBOOT.**

**6.) Fast virus scan**

Run even if you already have an antivirus. Simple tools to do a quick scan.

At this point, **disable your existing antivirus temporarily** or just uninstall it until you're finished with this guide.

1. [Microsoft Safety Scanner](https://www.microsoft.com/security/scanner/en-us/default.aspx) - This is a no-install antivirus in an EXE from Microsoft. Run a quick scan. Takes ~10 minutes. (~160MB)
2. [Kaspersky Virus Removal Tool](https://www.kaspersky.com/downloads/thank-you/free-virus-removal-tool?form=1)

**7.) Malware/Junkware checkup**

Run if you have any suspicion the computer isn't clean, or if it has ever had an infection in the past.

1. [MalwareBytes AdwCleaner](https://www.malwarebytes.com/adwcleaner/) is a little-known but **very** effective way to get rid of lots of tiny things that hijack a computer. Please manually review all the recommendations before you agree to them. Requires a reboot when done.
2. [MalwareBytes Anti-Malware](https://www.malwarebytes.org/antimalware/) is my go-to for automated cleanup of a broader range of malicious software and system changes. Leave it installed - the free version only cleans up after infections and does not have a real-time scan component so there's no speed impact. If the computer's user is prone to installing junkware, you should consider purchasing Premium.
3. [Google Chrome Reset Tool](https://www.google.com/chrome/cleanup-tool/) is a small tool  from Google that removes junkware that interferes with Google Chrome. It takes like 10 seconds. You don't have to reset Chrome at the end unless you think something is broken.

**8.) Check Windows Update and Firewall**

A classic sign of infection damage are if the following settings cannot be enabled or do not work. Fix them.

1. *Start*> type "*Windows Update*" > hit Enter  
   Check for updates. If it doesn't work, make note of that and continue.
2. *Start* > type "*Windows Firewall*" > hit Enter  
   Make sure it's on or that it says it's being managed by another program. If you want it left off, at least make sure you can turn it on.  
   If it still doesn't work, make note of that and continue.
3. *Start* > type "*services.msc*" > hit Enter  
   Check to see if "Windows Defender" exists. If it doesn't, make note of that and continue.

* If Windows Update doesn't work, repair it with [Microsoft Windows Update FixIt tool](https://aka.ms/diag_wu).
* If Windows Firewall doesn't work, repair it with [Microsoft Windows Firewall FixIt tool](https://support2.microsoft.com/mats/windows_firewall_diagnostic/).
* If Windows Defender is missing, repair it with [Microsoft Windows Defender FixIt tool](https://support.microsoft.com/kb/931849).

If any of the above fixes don't work, you can try the [Windows services repair tool](http://download.webroot.com/wsvcscan.exe) by [Webroot](http://www.webroot.com/" \t "_blank) or the [Services repair tool](http://www.wintips.org/how-to-restore-windows-services-to-their-default-state/) by [ESET](https://www.eset.com/).

**9.) DISM RestoreHealth (Windows 8+)**

This command will scan the Windows operating system for corrupted components and repair them. This may take 20 minutes.

1. Start > type "cmd" > hit Ctl+Shift+Enter
2. A black box will appear
3. Type "dism /Online /Cleanup-Image /RestoreHealth"
4. If any corruption is repaired, reboot the computer

**10.) Install Windows updates and configure automatic update**

**If updates fail Step 1 - FixIt**

Run the [Microsoft Windows Update FixIt tool](https://aka.ms/diag_wu).

**If updates fail Step 2 - System file scan**

1. Start > type "*cmd*" > hit **Ctl+Shift+Enter**
2. A black box will appear.
3. Type "*sfc /scannow*" without the quotes  
   When it finishes, proceed
4. (Win 8+) Type "dism /online /cleanup-image /restorehealth"
5. Reboot when done

**If updates fail Step 3 - Microsoft SUR tool**

1. Download and install the [Microsoft System Update Readiness Tool](https://www.microsoft.com/en-us/download/details.aspx?id=20858). (Windows 7 only)

**If updates fail Step 4 - Reset Windows Update Components**

1. Download and extract "[Reset Windows Update Tool](https://gallery.technet.microsoft.com/scriptcenter/Reset-Windows-Update-Agent-d824badc)" to a folder on your desktop
2. Right click on *ResetWUEng.cmd* > Run as *Administrator*
3. Use options 2, 5, 8, 9, 10, 12, restart, then check for updates

**If updates fail Step 5 - Chkdsk**

Check your hard disk for errors.

1. Start > type "*cmd*" > hit **Ctl+Shift+Enter**
2. A black box will appear.
3. Type "*chkdsk /r*" without the quotes
4. Type "y" and hit Enter
5. Restart the computer

**If updates fail Step 5 - Remove antivirus and reset network stack**

Uninstall your antivirus, reboot, then [follow the instructions here](http://www.hanselman.com/blog/TheNuclearOptionResettingTheCrapOutOfYourNetworkAdaptersInVista.aspx). Note that you will need to reinstall any VPN software after doing this. If you don't know what a VPN is, then you don't need to worry.

**If updates fail Step 6 - CheckSUR.log**

This is only for Windows 7, and is extremely rare that you would ever need to do this. Warning: This is highly technical.

1. Run a hard drive health scan with [WinDlg](http://download.wdc.com/windlg/WinDlg_v1_29.zip" \t "_blank) from Western Digital
2. <https://support.microsoft.com/en-us/kb/2700601>

**11.) Quick scan with SecureAnywhere System Analyzer**

[SecureAnywhere System Analyzer](http://anywhere.webrootcloudav.com/zerol/syswranalyzer.exe) by [Webroot](http://www.webroot.com/" \t "_blank) will do a very fast scan of running processes and important system locations for things marked bad in the "cloud." It triggers on viruses and junkware, and doesn't clean, so you normally want to run it after you've done the initial cleanout of a computer. It's for information only.

**12.) WinSxS cleanup ResetBase (Windows 8+)**

This goes further cleaning WinSxS than the command we ran at the start. We needed to make sure everything was functioning well before we cleared up outdated Windows files. [Technical information about what this does.](https://msdn.microsoft.com/en-us/windows/hardware/commercialize/manufacture/desktop/clean-up-the-winsxs-folder)

1. Start > type "*cmd*" > Hit Ctrl+Shift+Enter to run it as Administrator
2. Type: "*Dism.exe /online /Cleanup-Image /StartComponentCleanup /ResetBase*" without the quotes
3. Hit Enter

**13.) Set UAC to full**

**Listen to me.**Or listen to one of [Microsoft's most senior programmers](https://blogs.msdn.microsoft.com/oldnewthing/20160816-00/?p=94105). UAC is a critical security control that has vast impacts you can't see. It is not computer bubblewrap. It exists for very important reasons. You aren't cool for turning it off.

[Follow these instructions](http://www.tenforums.com/tutorials/3577-user-account-control-uac-change-settings-windows-10-a.html) to **set UAC to the highest option**, "Always notify me." Anything less allows any malware to instantly elevate to administrator level permissions. UAC isn't magic, but it's a layer you want to use.

**14.) Enable SmartScreen (Windows 8+)**

This will check with Microsoft and warn users if they download+run any programs not commonly seen. This will prevent most infections downloaded from fake emails unless the user clicks through the stern warnings.

1. *Start* > type "*SmartScreen*" > click "*Change SmartScreen Settings*"
2. On the left, click "*Change Windows SmartScreen Settings*"
3. Select "*Get administrator approval*" (Windows 8) or "*Warn before running an unrecognized app*" (Windows 10) and hit *Ok*

**15.) Browser upgrade and wipe**

**Many users are still using 32-bit Chrome installations, which do not automatically update to 64-bit. If you do not plan on wiping Chrome, at least install the latest Chrome manually**[**here**](https://www.google.com/chrome/browser)**.**

If the user has any history of computer-hijacking malware or performance issues with browsers, it may be a good idea to completely wipe their cache and settings. Otherwise, this might be overkill. There are simpler reset commands, but this way you know for a fact everything is gone.  
**NOTE**: This wipes saved forms and passwords.

**Microsoft Edge**

At this time I have no real-world virus experience with this browser and have no advice.

**Google Chrome**

We are going to 100% reset Chrome. I'm not talking about clearing registry keys since that feature only activates on domain-joined (company) PCs.

1. [Export Chrome favorites](https://support.google.com/chrome/answer/96816?hl=en).
2. [Uninstall Google Chrome](https://support.google.com/chrome/answer/95319?hl=en).
3. Start > type "*%AppData%\Google*" > hit Enter > Delete the "Chrome" folder
4. Delete the folder *C:\Program Files (x86)\Google\Chrome*
5. Install Google Chrome with the [machine-wide offline installer](https://www.google.com/chrome/browser/desktop/index.html?system=true&standalone=1). You can install it normally, too. I won't go into it.
6. [Import Chrome favorites](https://support.google.com/chrome/answer/96816?hl=en).

**Mozilla Firefox**

We are going to 100% reset Firefox. Firefox doesn't really use the registry so this is simple.

1. [Export Firefox favorites](https://support.mozilla.org/en-US/kb/export-bookmarks-internet-explorer).
2. Uninstall Mozilla Firefox.
3. Start > type *"%AppData%\Mozilla*" > hit Enter > Delete the "Firefox" folder
4. Delete the folder C:\Program Files (x86)\Mozilla Firefox" folder.
5. [Install Firefox from the Mozilla website](https://www.mozilla.org/en-US/firefox/new/).
6. [Import Firefox favorites](https://support.mozilla.org/en-US/kb/export-firefox-bookmarks-to-backup-or-transfer).

**Internet Explorer**

We are going to reset Internet Explorer to default settings. It's not a 100% reset, but it's pretty close. Make sure you have IE11 installed. To be safe, we will backup the bookmarks. Long story.

1. [Backup Internet Explorer favorites](https://kb.wisc.edu/helpdesk/page.php?id=1419)
2. *Internet Explorer* > *Press the Alt key* > *Tools* > *Internet Options* > *Advanced* > *Reset*
3. Check "*Delete Personal Settings*" > Ok

**16.) Browser configuration**

**IMPORTANT NOTE**: There are LOTS of settings in browsers that I am leaving out because I know the rare problems they can cause or that change the browsing experience. Some are also worthless, like enabling certificate revocation or Do Not Track. What I have chosen are carefully selected for the highest reward:risk ratio.

**Microsoft Edge**

1. Install the 'Adblock Plus' extension. I will recommend uBlock Origin Edge once it's further in development.

**Google Chrome**

1. [Install uBlock Origin](https://chrome.google.com/webstore/detail/ublock-origin/cjpalhdlnbpafiamejdnhcphjbkeiagm?hl=en). Ads deliver malware and lead users to install fake programs. There is a small risk of it breaking sites so make sure the user knows to try Internet Explorer if they run into any problem. The overall reward is greater.
2. If it's a laptop, install [HTTPS Everywhere](https://chrome.google.com/webstore/detail/https-everywhere/gcbommkclmclpchllfjekcdonpmejbdp?hl=en). You can also install on desktop.
3. If it's an unskilled user who falls for phishing, install [Bitdefender TrafficLight](https://chrome.google.com/webstore/detail/trafficlight/cfnpidifppmenkapgihekkeednfoenal?hl=en).
4. Menu button > "*About Google Chrome*" to make sure it's the latest version
5. Menu button > "*Settings*" > "*Show advanced settings*..."
   1. Check "*Automatically report details of possible security incidents to Google*"
   2. Check "*Protect you and your device from dangerous sites*"

**Mozilla Firefox**

1. [Install uBlock Origin](https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/). Ads deliver malware and lead users to install fake programs. There is a small risk of it breaking sites so make sure the user knows to try Internet Explorer if they run into any problem. The overall reward is greater.
2. If it's a laptop, install [HTTPS Everywhere](https://www.eff.org/https-everywhere). You can also install on desktop.
3. If it's an unskilled user who falls for phishing, install [Bitdefender TrafficLight](https://addons.mozilla.org/en-US/firefox/addon/trafficlight/).
4. Menu button > "*?*" >  "*About Firefox*" to make sure it's the latest version

**Internet Explorer**

It's important you did the complete IE reset earlier, as I'm assuming everything's back to defaults. Also, don't use IE.

**Turn add-ons back on**

Resetting Internet Explorer disables all add-ons, including things like Adobe Reader. There are some websites where they only display PDFs in an embedded object, so you will want to turn it back on.

1. Press Alt key > *Tools* > *Manage add-ons*
2. Under "*Add-on types*" > *Show all add-ons*
3. Select and re-enable any addons you think are appropriate. Usually the only one is Adobe Reader

**Enable protection of search provider**

1. Press Alt key > *Tools* > *Manage Add-ons*
2. Under "*Add-on types*" select "*Search providers*"
3. Check "*Prevent programs from making changes to my default search provider*"
4. Review and modify search providers as you see fit

**Configure Advanced options**

This will turn on an additional layer of protection for Internet Explorer. Do not do this is the user uses any Internet Explorer plugins, like LastPass.

1. Press Alt key > *Tools* > *Internet Options*
2. *Advanced* tab
3. Check:
   1. *Enable 64-bit processes for Enhanced Protected Mode*
   2. *Enable Enhanced Protected Mode*

**17.) Enroll into cloud protection for Windows Defender**

Windows Security Essentials/Windows Defender has a critical "cloud" component to it called MAPS, which used to be called SpyNet. This improves protection considerably. If you have another antivirus installed, skip this section.

**Windows 7 & 8**

Most users should already be set to MAPS Basic, but while we're in there we're going to set it to MAPS Advanced to assure the highest protection.

1. Start > Search for *Windows Defender* or *Microsoft Security Essentials*
2. *Settings > MAPS > Advanced Membership > Save changes*

**Windows 10**

Microsoft only has On or Off in Win10, which is a good improvement.

* Start > Search for*Windows Defender*
* *Settings > Cloud-based protection > On*

**18.) Update Flash, Adobe Reader, and uninstall Java**

Java is not needed for any modern reason other than obscure software and people who install Minecraft mods. It's safe to uninstall.

**Windows 7:**

Make sure Flash is the [latest version](https://get.adobe.com/flashplayer/) for Internet Explorer and Firefox by opening that link in each browser. If the user only uses Chrome, completely uninstall Flash. There's no reason to have it installed.

I recommend [Adobe Reader DC](https://get.adobe.com/reader/) as opposed to other PDF readers because it silently updates and is 100% compatible with anything the user will do. The security is just vastly better than it was years ago.

**Windows 8:**

The only reason to have Flash installed is if the user insists on using Firefox. Otherwise, uninstall it.

I recommend [Adobe Reader DC](https://get.adobe.com/reader/) as opposed to other PDF readers because it silently updates and is 100% compatible with anything the user will do. The security is just vastly better than it was years ago.

**Windows 10:**

The only reason to have Flash installed is if the user insists on using Firefox. Otherwise, uninstall it.

Microsoft Edge reads PDF files, and Chrome has a reader built-in for web documents, so unless the user needs to interact with editable PDF forms, there's no reason to install a dedicated PDF reader.

**19.) Update drivers**

In order to talk with your computer's hardware, your operating system needs a special piece of software called a "driver" to translate commands. Computer manufacturers often release driver updates for a year or more after a computer is released, to fix issues they uncover. Drivers have low-level access to the operating system and can mess up your computer in exceptional ways if they have bugs. Because of this low-level access, it's sometimes very hard to pinpoint them as the cause of an issue.

Did you know that some graphics drivers have bugs that cause [Microsoft Word to crash](https://support.microsoft.com/en-us/kb/2768648)? Or that a Bluetooth radio driver can hang Outlook? You wouldn't think that would be possible, but I've seen it personally. Unfortunately, most people will suffer through these problems without ever finding a solution. You don't have to.

For these reasons, you should follow the advice of your computer manufacturer on keeping drivers up to date. On Google.com, search for your computer model and go to the manufacturer's website to download them directly.

**Do not use any "driver update programs" or websites not made by the computer or component manufacturer.**It's usually best to stick with the approved versions of drivers hosted on the manufacturer site. The programs you see advertised to update drivers do not carefully test and curate them - instead their incentive is to make it look like everything on your computer needs to be updated all the time, so you keep paying them money. [Also, many of these sites and programs are complete scams.](http://www.howtogeek.com/198758/never-download-a-driver-updating-utility-theyre-worse-than-useless/)

I've selected, deploy, and maintain the driver loadouts for thousands of computers and OS installs across their entire lifecycle in my work. Most people do not have this kind of background in this specialized area. I've seen first-hand how newer versions of drivers downloaded from one site can have unintended consequences. Because of their special access to memory and the OS, drivers have to play together very well. For this reason, business-class computer manufacturers like Dell have special teams for driver testing. This is to make sure their enterprise customers don't have crashes and issues that stop employees from working.

**Here's some common updaters:**

* Intel Chipset Device Software (updates core system drivers) https://downloadcenter.intel.com/download/20775/Intel-Chipset-Device-Software-INF-Update-Utility-
* [Intel Rapid Restore Technology Driver](https://downloadcenter.intel.com/product/55005/Intel-Rapid-Storage-Technology-Intel-RST-) (updates the HDD/SSD driver, can improve speed)
* [Dell SupportAssist](http://www.dell.com/support/contents/us/en/04/article/Product-Support/Self-support-Knowledgebase/software-and-downloads/support-center)
* [Lenovo System Update](https://support.lenovo.com/us/en/documents/tvsu-update)

Note: Do not use the "Intel Driver Update Utility" application on their site, it's bloated.

**20.) Install Windows 7 hotfix rollup**

Disclaimer: *This is an immensely complicated situation that I'm going to try to simplify for you. I have spent literally a cumulative hundred-plus hours going through manually tracking hotfixes and curating packages of Windows fixes. Microsoft has now made most of that work irrelevant with the information I'm going to provide below. If you want the technical details*[*see here*](https://blogs.technet.microsoft.com/mrsnrub/2009/05/14/gdr-qfe-ldr-wth/)*.*

The dirty truth about Windows 7 updates is you're not getting all the fixes and improvements unless you're a corporate customer with a knowledgeable IT team. Until now.

* There's the mainline release of every Windows component, called **GDR**, where they only fix problems they think most people will run into.
* There's another parallel series called **LDR**, that has all the fixes and improvements in GDR, but include extra things Microsoft didn't want to test for wide release. It's not a beta, it's just a different assurance level. It's most things only companies run into.

This was a neato idea that gave them flexibility in quickly getting out fixes. In the end, it's turned out to be kind of a disaster where 99% of machines don't have a lot of fixes, and company machines with IT people that know about this, only have a mix of updates. Ever wonder why your computer at work *sucks* with all these weird bugs they just tell you to reboot to fix? It's because your IT team probably isn't deploying hotfixes that include LDR file editions.

This is the motivating reason for why Windows 10 uses cumulative builds, which include every single fix they develop. To get away from this utter nightmare.

Unless you install a special update that opts you into the LDR release for a component, you're stuck on GDR. Microsoft decided to combine tons of hotfixes into one easy to install package. There's not a huge reason to do this, but if you're looking to refresh a desktop, this update is a massive compilation of fixes.

I recommend you update all your drivers before you install this, because some changes it introduces were not tested on the first editions of older software. I've only run into this one time across tons of computers, but it's a good idea.

[**KB3125574**](https://www.catalog.update.microsoft.com/Search.aspx?q=KB3125574)  
https://www.catalog.update.microsoft.com/Search.aspx?q=KB3125574

**21.) Defragmentation**

Make sure Windows [automatic optimization is turned on](http://www.sevenforums.com/tutorials/3292-disk-defragmenter-schedule-turn-off.html) to run at 1PM every day. It will only launch if the computer is idle. Leaving it at the default can mean weeks between defrags, depending on usage patterns.

Defragmentation is a complicated topic that, in the past. would have been due several pages of discussion. In fact, I wrote a lot about this and just deleted it. These days, users are best served by making sure Windows handles this for them. In fact, the built-in Windows defragmenter [out-performs many paid-for options](http://www.hofmannc.de/en/windows-7-defragmenter-test/benchmarks.html) and for the rest, there is basically no difference. You could even make it worse!

If for some reason you need to ensure a large spinning hard disk drive is contiguous or need to move files forward to shrink a volume, I have been a user of [MyDefrag](http://filehippo.com/download_mydefrag/" \t "_blank) for over a decade. However, I strongly advise against you thinking this is something worth spending time on. Get an SSD instead. They're orders of magnitude faster and start at $60.

**22.) Physical cleaning**

"It's just dust." I used to think that. Heat kills electronic components. Also, computers limit themselves if they aren't being cooled. A literal plug of dust can form behind the heatsink of a laptop. Use canned air - NOT a vacuum. Dust particles rubbing against the plastic nozzle produces static electricity. Additionally, do not spin fans too fast or you'll shred the bearings. If possible, hold the fan with your finger.

**23.) Upgrade to Windows 10**

Let me tell you a story. At my parents house was a terrible, ancient Lenovo desktop running Windows 7. I spent hours working on it. I made progress, it was a lot better. But it was still just a bad experience. It just dragged.

In the Thanksgiving of 2015, I just gave up and upgraded it to Windows 10. It made an incredible difference. Windows 10 has fundamental differences to Windows 7 on how it's designed performance-wise. Additionally, it has many of the latest drivers built-in, with improvements that will never be backported to Windows 7. You should seriously consider this. Windows 7 will be end-of-life in 2020, the clock is already ticking.

If you have extra time, you could consider doing a bare-metal wipe and optimize the machine from scratch. I have an entire [article dedicated to that here](https://decentsecurity.com/#/securing-your-computer/).

**24.) Other troubleshooting**

* [Microsoft Office configuration issue check](https://www.microsoft.com/en-us/download/details.aspx?id=36852)
* [Bypass DNS interception](https://dnscrypt.org/) https://dnscrypt.org/
* [Microsoft Autoruns](https://live.sysinternals.com/autoruns.exe) https://live.sysinternals.com/autoruns.exe
* [View bluescreen crashes](http://www.nirsoft.net/utils/blue_screen_view.html) http://www.nirsoft.net/utils/blue\_screen\_view.html
* [See what's been run on the computer](http://www.nirsoft.net/utils/executed_programs_list.html) http://www.nirsoft.net/utils/executed\_programs\_list.html
* [View injected DLLs](http://www.nirsoft.net/utils/injected_dll.html) http://www.nirsoft.net/utils/injected\_dll.html
* [Powerful alternate uninstaller](http://www.nirsoft.net/utils/myuninst.html) http://www.nirsoft.net/utils/myuninst.html