How can I avoid a forced upgrade to Windows 10?

Having studied this issue during a several months, my advice is this:

- Uninstall all updates listed below (if there).
- Update your Windows 7 or 8 manually, avoiding suspicious updates.
- Install GWX Control Panel and make it autostart, so that it checks your computer each time you start it up. Check this application regularly for an update of it. For example, the finding under "Are Windows Update OS Upgrades enabled" can one day, for whatever reason, have changed to "yes", and then you can revert that immediately. See also here.
- Immunize your computer against telemetry with Spybot Anti-Beacon. See here.
- **ATTENTION!** KB3161608 of June 20, 2016, so far appears suspicious to me. See this description https://support.microsoft.com/en-us/kb/3161608. **Concerning later rollups, see here!**

Addition 6.24.2016: A new Problem!
Since some time, a real nuisance when installing an update is that it takes an eternity until the computer (at least in Windows 7) has checked through the list of already installed updates. Only after that can the installation continue. See the following articles:
KB3161664 replaces KB3153199
Windows 7 update scans taking forever?
Microsoft releases KB 3161647, KB 3161608 to fix slow Windows 7 update scans

This is not only a problem when one updates directly from the Internet, which I do not do, but now also turns out to be one (since April or May 2016) when updating manually. Also in this case the update installs in real snail pace if you want to install several of them, one after the other, without a restart (except at the end). It then concerns only the second and following updates in the row, but not the first one. Therefore, there is a workaround: it works smoothly if you restart the computer after *each* update, i.e.: install them only one by one. According to the recommendation in the first of the above articles, I did install KB3135445 from February 2016 (but no other of the updates mentioned in these articles). After that it worked without that molesting delay. I, however, hesitate to install further updates to Windows Update, as long as I do not know what this does to the immunity to Windows 10. If the problem comes back again, I will have to install a later update to Windows Update.

Since earlier updates do not cause such a problem, this seems to indicate that Microsoft has since changed something in the update format that requires a later version of Windows Update.

Addition 7.16.2016
In the list below with updates you should better not have, I have added just a few more in a reddish brown color, which I have from another source. Probably not very important, but judge from your gut feeling…

Addition 7.23.2016
BEWARE! The update rollup KB3172605 of July 21 for Windows 7 is could possible be a "neat" way to sneak in all updates you tried to keep out of your computer… ~~But: ALL CLEAR? Allegedly this rollup is safe and contains a collection of singular files and no past updates.~~ A list of its contents is found here: http://download.microsoft.com/download/7/7/5/775C786B-D9C1-41DF-AAFD-155FF28EA0A1/3172605.csv. Cf. https://support.microsoft.com/en-us/kb/3172605. No! Not all clear! See below.

Addition 7.24.2016
Just a few improvements in the list of unwanted files and some additions to the list of *host* file entries at the end.

Addition 8.10.2016
Among the updates from August 2016 KB3167679 seems a bit strange to me since it has to do with "Authentication Methods" and I could first not download it with Firefox, but I could with Internet Explorer (that I normally never use). – and next day it worked with Firefox, too… Yet: About what

kind of authentication is it? It may be a bit oversuspecting, yet Microsoft has already before tried to make life with Windows 7 harder, such as with the notorious update KB3133977. About this, see: "Microsoft Windows Update KB3133977 Is Deadly" and After installing Microsoft Update KB3133977 for Windows 7, some users may encounter a "Secure Boot Violation". After the "red screen alarm" the impudent suggestion came to switch to Windows 10 to "solve the problem"…

Addition 8.18.2016

I must regrettably take back the ALL CLEAR? above from 7.23.16! The new procedure of Microsoft with monthly issues of "rollups" does not make your Windows 7 or 8 as much safer as they want you to believe. Rollup KB3172605 of July 2016 contains (as has been found out in the meantime) some little things that, after all, have to do with telemetry. The same may then very well be valid for the rollup KB3179573 of August 2016. Cf. the article Win7 and 8.1 to get cumulative updates – you no longer control your Win7 or 8.1 machine. The new tactics appears to be to bring Windows 7 and 8 closer to Windows 10 in respect to privacy and espionage! *For that reason I will preliminarily install no such rollup…* **[Continued 8.20]** This article explains the plans: Further simplifying servicing models for Windows 7 and Windows 8.1 in which is stated: "Over time, Windows will also proactively add patches to the Monthly Rollup that have been released in the past. Our goal is eventually to *include all of the patches we have shipped in the past* since the last baseline, so that the Monthly Rollup becomes fully cumulative and you need only to install the latest single rollup to be up to date. We encourage you to move to the Monthly Rollup model to improve reliability and quality of updating all versions of Windows" (my enhancement). **This pretty much says it all…**

Addition 9.29-30.2016

KB3184122 apparently also requires an update KB3185319 to Internet Explorer version 11, if you have it, but no to earlier versions. However, it is advisable to have no higher version than 9 and use it only exceptionally. For reasons mentioned above I skipped the September rollup KB 3185278. The update KB3184143 removes the Get Windows 10 app and other software related to the Windows 10 free upgrade offer that expired on July 29, 2016 – that you should not have… and it could happen that the computer does not start after you install it…

Addition 10.12.2016

It has happened! Microsoft has now taken an evil step to stop independent updating of Windows 7 and 8! With the updates in October, they definitely introduced a new updating procedure, see **Simplifying updates for Windows 7 and 8.1**, **Further simplifying servicing models for Windows 7 and Windows 8.1** and **More on Windows 7 and Windows 8.1 servicing changes**. "Simplifying" here means *complicating* for the user who wants to pick himself or herself what update he/she trusts and wants to install. The new ***in***convenience rollups give us no choice, except between security updating and total updating. The latter also includes non-security updates. But both will undoubtedly include updates many of us would not trust very much, since they could be related to telemetry and possibly other functions useful in spying on us, and they may "roll up" with older updates we have already chosen to not install. That is the obvious motivation for this "simplification". However, there is hope that ways to circumvent this will be found so that we may still have a choice for privacy. I will follow up what appears about in the web. In the meantime, I will stop updating and finally get a bit more involved with Linux Mint…

Addition 10.13.2016

Read: **Say good-bye to individual patches on Windows 7 and 8** and **Microsoft is changing the way it patches Windows 7 and 8.1. Here's what we know -- and what to do to keep having Windows your way**. One is talking about a "patchocalypse"…

Microsoft claims that this circus is established to "improve" their system by means of *involuntary* "feedback", but it is very obvious indeed that it is a further step towards total surveillance over the Internet and its users.

With this, much of what is written below is already outdated…

Avoid KB3170735 and all other updates to Windows Journal. Windows Journal should not be used since it is a massive security hole in Windows.

Until now, we always had to pay for a new version, and now we will get it for free? Such "generosity" is already suspicious… Is it Windows 10 or Windows NSA?

Thus very many computers that had Windows 7 or 8 will now have been upgraded to Windows 10 even without asking. This happened if the following update is (or was) installed that is offered since the beginning of July 2015 and has been installed (smuggled in) automatically for many users: KB3035583, first offered as optional but now declared to be "important". In that case your Windows probably was automatically upgraded to Windows 10 on July 29, 2015 or rather soon after. If you did not want that, you needed to uninstall that update in time (and now it will be too late).

Below are updates listed that you should not have *if you do not want Windows 10*, and also ***do not want extra spy functions in Windows 7 or 8***, which are similar to those in Windows 10. This list is put together from various sources.

Updates *you should not have* (as per September 2016)

General updates (for Windows 7, or both for Windows 7 and 8)

KB971033 Update that describes Windows Activation Technologies. License validation check
KB2505438 Tracks performance, breaks some fonts
KB2506928 Problem with links in Outlook, may spy
KB2545698 Fixes some blurry fonts in IE9, may spy
KB2574819 For Remote Desktop Services – unless needed!
KB2592687 For Remote Desktop Services – unless needed!
KB2660075 Problem with Samoa time zone, may spy
KB2670838 Updates platform for Windows 7 SP1 (seems suspicious). Breaks AERO functionality and can blur some fonts
KB2726535 Adds South Sudan to list of countries, may spy
KB2830477 For Remote Desktop Services – unless needed!
KB2876229 Unless you use Skype (Skype spies, too!)
KB2882822 Update for adding itracerelogger interface support
KB2902907 For MS Security Essentials, that should not be used anyway!
KB2922324 Telemetry
KB2923545 Update for the Remote Desktop Protocol
KB2938066 Probably update to Update Client
KB2952664 Compatibility update for upgrading Windows 7. Nags about Windows 10
KB2966583 Improves the Update Readiness Tool so that it can be executed *without user interaction*
KB2970228 New currency symbol for Russian ruble
KB2977759 Compatibility update for Windows 7 RTM = W10 Diagnostics Compatibility telemetry
KB2990214 Aids in transitioning from Windows 7 to 10
KB2996978 No description found
KB2994023 RDP 8.1 client for Windows 7 disconnects, may spy
KB2999116 Windows 10 universal C Runtime in Windows 7
KB3008273 Update rollup for Windows 8 and for an issue with Windows 7
KB3012973 Upgrade to Windows 10 Pro
KB3014460 Windows 10 Insider preview install
KB3015249 Adds telemetry points to consent.exe
KB3021917 Update to Windows 7 SP1 that determines if performance issues may be encountered when 10 is installed. Sends telemetry back to Microsoft
KB3022345 Telemetry
KB3035583 Creates the annoying "Get Windows 10 App" notification in your taskbar
KB3042058 Contains Winlogon spying
KB3046480 For a .NET Framework issue when upgrading Windows 7 or 8
KB3050265 Update to the Windows Update client for Windows 7. Also states that there are "general improvements that are made to support upgrades to later version of Windows." WU service updated to accept upgrade to W10 + other fixes
KB3065987 Makes "improvements" to Windows Update Client for Windows 7, pushing of Windows 10
KB3065987-v2 Cf. above
KB3065988-v2 For Windows Update Client
KB3068707 Telemetry
KB3068708 Telemetry
KB3074677 Windows 10 Upgrade preparation
KB3075249 Adds telemetry points to consent.exe

KB3075851 Makes “improvements” to Windows Update Client for Windows 7, pushing of Windows 10
KB3075853 For Windows Update Client
KB3079821 Enables Windows 7 to activate Windows 10
KB3080079 Supports a TLS function that may not be needed
KB3080149 Telemetry
KB3081437 Windows 10 Upgrade preparation
KB3081954 Prepares Upgrade and adds telemetry
KB3083324 New update client (may ease upgrade to Windows 10)
KB3083710 New update client (may ease upgrade to Windows 10)
KB3086255 Update for the graphics component in windows (breaks safedisc)
KB3088195 Has a key logger on the Kernel Level
KB3090045 Windows 10 Upgrade Update for Windows 7/8
KB3093983 Contains IE spying
KB3094176 Aids upgrade to Windows 10 (See below)
KB3095649 Actually for Windows 8 and not needed for Windows 7
KB3102810 Fixes issue with Windows Update, but also preparers for Windows 10 in Windows 7
KB3123862 Updated capabilities to upgrade windows 7 and windows 8.1
KB3112343 Enables additional upgrade scenarios from Windows 7 to Windows 10
KB3125574 Telemetry for Windows 7
KB3135445 For Windows Update, probably preparing for upgrade
KB3138612 A new version of KB3135445
KB3139929 Security update for internet explorer and upgrade to Windows 10
KB3146449 Windows 10 upgrade
KB3150513 Compatibility update for windows
KB3170735 Windows Journal update
KB3172605 Update rollup
KB3173040 Windows 10 Upgrade notice
KB3179573 Update rollup
KB3181988 Fixes an error that is caused by rollup KB3125574 that should, however, not be installed
KB3184143 removes the Get Windows 10 app and other related software
KB3185278 Update rollup

Updates for Windows 8:
KB2976978 Compatibility update, prepares for Windows 10
KB3008273 Update rollup for Windows 8 and for an issue with Windows 7
KB3015249 Adds telemetry points to consent.exe
KB3035583 Creates the annoying “Get Windows 10 App” notification in your taskbar
KB3044374 Aids in transitioning to 10
KB3046480 For a .NET Framework issue when upgrading Windows 7 or 8
KB3050267 Update to the Windows Update client for Windows 8.1. Also states that there are “general improvements” that are made to support upgrades to Windows 10
KB3058168 Activates Windows 10 from Windows 8 or Windows 8.1
KB3064683 For OOBE modifications to reserve Windows 10 in Windows 8.1
KB3065988 For Windows Update Client
KB3065988-v2 For Windows Update Client
KB3072318 Windows 10 Upgrade preparation for Windows 8
KB3075249 Adds telemetry points to consent.exe
KB3081454 Windows 10 Upgrade preparation
KB3102812 Fixes issue with Windows Update, but also preparers for Windows 10 in Windows 8
KB3083325 Telemetry - Windows 10 Upgrade preparation
KB3083711 Update for Windows Update Client for windows 8.1
KB3090045 Windows 10 Upgrade Update for Windows 7/8
KB3065988 For Windows Update Client
KB3112336 Enables additional upgrade scenarios from Windows 8.1 to Windows 10
KB3135449 For Windows Update, probably preparing for upgrade
KB3138615 A new version of KB3135449
KB3146449 Updated internet explorer 11 capabilities to upgrade windows 8.1 and windows 7
KB3172614 Update rollup
KB3179574 Update rollup
KB3185279 Update rollup

About KB3094176 = Windows Management Framework 5.0 includes updates to Windows PowerShell: ***Desired State*** Configuration, ***Remote Management***, ***Management Instrumentation***. *Seems designed to take control over your computer!* Similarly, the “Application Compatibility Toolkit 5.6” could possibly want to take control over which applica-

tions you are allowed to have. Don't install them! It has already been reported that Microsoft may block or uninstall certain applications in Windows 10, and they will in any case want to "clean" your Windows 7 or 8 from any precautions against an unwanted upgrade.

About KB3050267: Windows 10 upgrade preparation but also adds the option in GPEDIT to disable Windows 10 upgrade altogether so you may want to actually install this and then remove it again…

It is recommended to not use the Internet Explorer, but if you do, use IE9 and no higher version. Installing IE10 or IE11 automatically also installs KB2670838 that you will not want. Better install IE10 BlockerToolkit and IE11 BlockerToolkit.

And how do you remove an update manually? Go to the *Control Panel* and then to *Programs and Features* and click *View installed updates*. You can enter an update KBxxxxxxxx in the search field up to the right. If it is installed, it will be shown. In that case, right-click on it and then click *Uninstall*. Then restart the computer.

Does Microsoft now bring out sneak updates that do not really serve security, but rather surveillance also in Windows 7 and 8, besides preparation for Windows 10? That appears likely and would not be very astonishing… ***The fact that Windows 10 will no more be free after July 31, 2016, has on good grounds led some to speculate that by then also Windows 7 and Windows 8 will have become updated so as to also have many of the spy functions that Windows 10 has.***

Updates are intended for correcting functional problems and close "loop-holes" in the software. But, theoretically, Microsoft could actually use an update to *create* a loophole for sneaking something in.

Never install an update related to telemetry! It may now be better to not update Windows 7 or 8 immediately, and certainly *not automatically*! Not before checking the Internet about the experience of others with the actual update. One webpage that is helpful for checking this is http://forums.mydigitallife.info/printthread.php?t=64561&pp=10&page=1 (register to get access to all information).

After an accidental upgrade to Windows 10, you can "roll back" to the previous version This is possible only within 30 days and only if the previous system is not deleted. – but what spy functions may then still remain from Windows 10?

- To do this, first open the Windows Start menu and Select Settings from the menu.
- Select Update & Security.
- Click the Recovery Icon then select "Go back to a previous version of Windows". Click "Get started" to begin.

GWX Control Panel is an application that searches for GWX.exe and reports it for deletion, and sets your computer such that it prevents downloading files that prepare for the installation of Windows 10. GWX.exe is a very big file that installs Windows 10. I have the Control Panel as autostart so that I after every start of Windows 7 immediately can see if something has changed or if the system is still immune to Windows 10. I also made it run in the monitoring mode so that it can alarm if something changes in this respect while the system is running. The unwanted file GWX.exe can also be removed using GWX Removal Tool.

Windows 7 and higher also have a "Snipping Tool" (in C:\Windows\system32\SnippingTool.exe) that can make screen dumps. This can (if remotely activated) serve espionage attempts. It can be turned off as follows (enabling "Do not allow…" disables the tool):

- Click Start, type gpedit.msc, press Enter to open Local Group Policy Editor (only in Windows Professional, Ultimate or Enterprise).
- Navigate to *Computer Configuration* > *Administrative Templates* > *Windows Components* > *Tablet PC* > *Accessories* > double click "*Do not allow Snipping Tool to run*".
- Select *enabled*, click OK.

Windows 10 contains a neat collection of spy and control functions, see: Windows 10: Your privacy is dead. The control functions may, furthermore, interact with your computer to change what Big

Brother does not want you to have. There might possibly also be a kill-switch built in, with which Microsoft (or someone else) could deactivate your system, or a part of it.

Primary surveillance functions are (and they most probably are not all):

- Information about your device and applications.
- Surveillance of your Internet activities.
- Collecting information about voice input features like speech-to-text.
- Information about the opening of a file, information about the file itself, the application used to open the file, and how long it takes.
- Information about when you enter a text, maybe collecting typed characters (key logging).

Updates to Windows 10 are mandatory and automatic updating can (almost) not be turned off, see also Windows 10 Automatic Updates Start Causing Problems. There are, however, certain possibilities to prevent forced updating – until Microsoft may put an end to that. That way, Microsoft can smuggle whatever they want into your computer. The nice excuse is, of course, that this would be for your own good. It would be fine if this were only for your safety, but it will certainly also be for the "safe function" of the surveillance system, that is: more clever spy and control functions.

See Windows 10 and Privacy, an extensive overview of what you have to do in Windows 10 to at least stop a lot of its spying. There is an application DoNotSpy10 that can do much of it for you, but beware: It may install adware if you do not click that option away. Another one that really looks interesting is Destroy Windows 10 Spying, (with less description at the author's page) that adds many URLs to your hosts file to be blocked, since they are used to report to Microsoft, directly or indirectly. These URLs are listed in the link and you can alternatively enter them yourself in your hosts file, if you know how. The tool may also take some additional action. It is recommended to use not only for Windows 10, but also for Windows 7 and 8, where some newer updates can be suspected to add spy functions. But again: be conscious of what you do. Microsoft warns against such tools, but who is naive enough to take that seriously? O&O Software is a company that is run by Scientology, but nevertheless has some good software. They have issued a free antispy-tool for silencing Windows 10: O&OShutUp10. More Tools for taming Windows 10 are Disable Windows 10 Tracking and Win10Privacy (can allegedly also deactivate mandatory updating). But one may quite safely assume that no such tool protects to 100%: Windows 10 Still Phones Home With Data In Spite of Privacy Settings, Even when told not to, Windows 10 just can't stop talking to Microsoft.

A few such applications are compared in this video.

A newer and apparently better tool for Windows 7, 8 and 10 for the same purpose is Spybot Anti-Beacon (forum here). I used it successfully but it is advisable to set a restore point before using this or a similar tool.

There are, however, certain tricks to stop automatic updating in Windows 10 that have been discovered along the way: How to Prevent Windows 10 From Automatically Downloading Updates, A workaround to Turn Off Windows Update in Windows 10, Disable/Turn Off Automatic Updates In Windows 10, Here's How and Windows 10 Hack: 3 Ways To Stop Forced Updates. It then remains to find a source for downloading updates to manually install them. Since I do not have and do not want Windows 10, I have not (yet) investigated this. Cf. How to Check for and Install Windows Updates in Windows 10. (One possibility could be Portable Update.)

It would not at all be astonishing if Microsoft occasionally sneaks in an update that **reverts these settings to default. Therefore: check these settings regularly! And they may also "update" to another and new way of spying.**

That Big Brother wants everyone to have Windows 10 to be surveyed and manipulated is so obvious that it needs a good portion of naivety and gullibility to not want to see it. That Microsoft also wants to make money from personal advertizing, for which they want to know everything about you, will rather come in the 2nd place.

It is then no wonder that the number of persons who concern themselves with Linux is growing, to sooner or later change to that system. It is also no wonder that Microsoft itself since 2003 secretly works on a Linux system (see here, here and here). They will, of course, want a Linux in the same sense as Windows 10, serving Big Brother. But: Is Microsoft now also trying to invade Linux systems with spying intentions? May no Linux user ever install a Microsoft "tool"!

Is all this mere "conspiracy theory"? Or conspiracy facts? Wait, and you will see for yourself…

Now it would no way be astonishing if Microsoft would soon try to let a new update sneak into your computer that does more or less the same as KB3035583. To guard yourself against this possibility, I recommend to deactivate automatic updates and only update manually. And, of course, too keep as many spy functions out to your system as possible.

Guard your computer against unwanted updates. *Never install an update related to telemetry!*

WARNING!!! On top of all this circus about Microsoft's new spyware there is now a ransomware on the loose in the Internet. **Never open an e-mail that offers you to download a Microsoft 10 installation file!** See That Windows 10 update message could be ransomware in disguise. A ransomware is a blackmail virus that blocks you from access to your data unless you pay a considerable amount to unlock it. See also CTB-Locker ransomware being pushed by fake Windows 10 Update emails.

Kill Windows 10 (permanently)
This interesting tool is found and described here. It, among a few other things, removes a lot of unwanted updates from Windows 7 and 8. Download a Readme file about it here. Download it as a cmd file here. Before you click download, unmark the box "Download with Secured Download manager". Alternate mirror link. **Suggestion: create a restore point before running this file.**

I have run this without any problem. First I checked that none of the updates mentioned here is installed. When KILLWindows10.cmd once hanged, it was probably while trying to uninstall an already uninstalled update. After a restart, it ran through it all. It also hides unwanted updates from Windows Update and it disables a number of unwanted "scheduled tasks".

***Additional information*: New Intel CPUs Have NSA Exploitable Secret Hidden Backdoor: New Intel CPUs come with a hidden backdoor that can allow hackers or the NSA to control your computer remotely even while PC is turned off.**

How to guard your computer from installing unwanted updates.

For Windows 7 in English

Semi-manual updating
First:

1. Click the start menu and enter "Services" in the search field.
2. In the list of services that appears, go down to "Windows update", right-click and go to "Properties". If it is set otherwise, change it to "Manual" and click "OK". Then right-click again and click "Start".

Then:
Control Panel > Windows Update > Change settings.

3. Choose "Check for updates but let me choose whether to download and install them".
4. Go back to the previous panel (<) and choose "Check for updates".
5. After the two lists of all available updates have appeared, go through the lists of "important" and "optional" updates. Unmark and right-click the ones you never want to install and choose "hide update".
6. Mark only the updates you do want to download and install. Go back to the previous window and click "Install". You can first click at the update to see a description.
7. If you before had another setting under "Change settings", go back and revert to it. Stop the service if it was not already running before.

In case you otherwise never want to update this way, but only fully manually (see below), go back to 1. and 2., stop the "Windows Update" service and change Properties to "Disable". Even if you do want to update this way again, it is a good idea to keep the service set at "Disable" in the meantime. It appears possible that this service can otherwise be started from an external source. It is for the same reason also advisable to keep the update setting at "Never check for updates (not recommended)". In the Control Panel click Windows Update > Change Settings to do that.

Fully manual updating
Download all actual updates as follows:

- http://www.microsoft.com/en-us/search/DownloadResults.aspx?q=%22windows%207%22%20updates&sortby=-availabledate, then chose "Newest to oldest" in "Sort by" if not already so.

and/or here (example):

- https://technet.microsoft.com/library/security/ms16-jun – for June 2016. Correspondingly for other months: ms16-may for May 2016, etc. This page becomes available only on the official update day, but then it stays and remains available for a long time. This page shows only critical updates.

[Für aktuelle deutschsprachige Aufdatierungen entsprechend:
http://www.microsoft.com/de-de/search/DownloadResults.aspx?q=%22windows%207%22%20updates&sortby=-availabledate
bzw. https://technet.microsoft.com/de-de/library/security/ms16-jun – für Juni 2016, und analog für andere Monate.

Motsvarande för aktuella svenskspråkiga uppdateringar:
http://www.microsoft.com/sv-se/search/DownloadResults.aspx?q=%22windows%207%22%20updates&sortby=-availabledate.
På länken https://technet.microsoft.com/sv-se/se-se/library/security/ms16-jun står det visserligen "Sverige (Svenska)" uppe till höger, men den visas ändå på engelska. Klicka där "Executive summaries".]

Now change the Windows Update service to "Manual" and start it, as described above (1. and 2.), because downloaded updates can be installed only when this service is running. Install the updates and when it is done, change the service setting from "Manual" to "Disabled" and stop the service. Stay disconnected from the Internet when you do this.

Check your updates
To check them, download and install MBSA = Microsoft Baseline Security Analyzer. Start it and run a scan of your computer. This takes quite some time and at the end you will be shown all "missing" updates (including the ones you did not want to install…). If you here find an update that you really have missed, note it to download it afterwards. To find it, enter "KBxxxxxxx" in your browser search, where xxxxxxx is the number of the update.

MBSA works only when the Windows Update Service is running.

NEVER INSTALL AN UPDATE THAT HAS TO DO WITH TELEMETRY. And be *suspecting* about updates for "customer experience" – that "experience" might not be very positive after all...

Block upgrade in Windows 7/8.1 Pro/Ultimate/Enterprise

1. Open *gpedit.msc* with administrative rights.
2. Go to *Computer Configuration* > *Administrative Templates* > *Windows Components* > *Windows Update*.
3. Find *Turn off the upgrade to the latest version of Windows through Windows Update* and double-click it.
4. In the window that opens mark *Activate* and click *OK*.

This should prevent downloading the upgrade to Windows 10 in the form of a Windows update. The entry is present only if updates preparing for upgrade are installed.

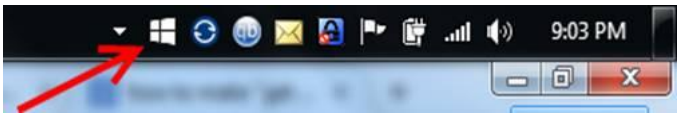
Block upgrade in Windows 7 Home/8.1 Core

In the home- und core-editions of Windows 7 and Windows 8.1, resp., there is no Local Group Policy Editor. Here the Registry editor is needed.

1. Run the Registry Editor *as administrator*.
2. Navigate to the following branch:
   HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate
3. In the key *WindowsUpdate* add the DWORD value (32 Bit) *DisableOSUpgrade* and set it to 1.

This also blocks the download of Windows 10.

Eliminate the Get Windows 10-App



If the updates that prepare for Windows 10 are installed, the symbol to the left appears in the task field. It remains to get rid of that, too, which can be achieved with the Registry Editor.

1. Start the Registry Editor *as administrator*.
2. Navigate to *HKLM\Software\Microsoft\Windows\CurrentVersion\WindowsUpdate\OSUpgrade*
3. In the key *OSUpgrade*, change the DWORD value (32 Bit) *ReservationsAllowed* from 2 to 0.

If the key and the value are not there, the respective upgrades are not installed.

Addition 1: There is another way to block GWX. In the Registry, go to *HKLM\SOFTWARE\Policies\Microsoft\Windows* and add the subkey *Gwx*. Add the DWORD entry *DisableGwx* in the subkey and set it to 1. After restarting Windows, the upgrade symbol will have disappeared.

Addition 2: You may try the following script to block Windows 10 upgrade offer to establish registry entries with a reg file that block Windows 10:

1. Close all open applications.
2. Press the **Windows-Key + R**.
3. Enter **notepad** and click **OK**.
4. Copy the following in Notepad:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\GWX]
“DisableGWX“=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]
“DisableOSUpgrade“=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\WindowsUpdate\OSUpgrade]
“AllowOSUpgrade“=dword:00000000
“ReservationsAllowed“=dword:00000000
```

5. Save as **Upgrade.reg**.
6. Run **Upgrade.reg** with a double-click. Confirm with Yes and then OK.
7. Restart your computer.
8. Test its behavior.

Before changing registry settings it is recommended to first make an backup of the registry that could be reinstalled instead of the modified one, if needed. A good backup application is Registry Backup.

The most important web-links to block in your hosts file:

a.ads1.msn.com
a.ads2.msn.com
a-0001.a-msedge.net
ad.doubleclick.net
adnexus.net
adnxs.com
ads.msn.com
ads1.msads.net
ads1.msn.com
az361816.vo.msecnd.net
az512334.vo.msecnd.net
choice.microsoft.com
choice.microsoft.com.nsatc.net
compatexchange.cloudapp.net
corp.sts.microsoft.com
corpext.msitadfs.glbdns2.microsoft.com
cs1.wpc.v0cdn.net
df.telemetry.microsoft.com
diagnostics.support.microsoft.com
fe2.update.microsoft.com.akadns.net
feedback.microsoft-hohm.com
feedback.search.microsoft.com

feedback.windows.com
i1.services.social.microsoft.com
i1.services.social.microsoft.com.nsatc.net
oca.telemetry.microsoft.com
oca.telemetry.microsoft.com.nsatc.net
pre.footprintpredict.com
preview.msn.com
rad.msn.com
redir.metaservices.microsoft.com
reports.wes.df.telemetry.microsoft.com
services.wes.df.telemetry.microsoft.com
settings-sandbox.data.microsoft.com
sls.update.microsoft.com.akadns.net
sqm.df.telemetry.microsoft.com
sqm.telemetry.microsoft.com
sqm.telemetry.microsoft.com.nsatc.net
statsfe1.ws.microsoft.com
statsfe2.update.microsoft.com.akadns.net
statsfe2.ws.microsoft.com
survey.watson.microsoft.com
telecommand.telemetry.microsoft.com
telecommand.telemetry.microsoft.com.nsatc.net
telemetry.appex.bing.net
telemetry.appex.bing.net:443
telemetry.microsoft.com
telemetry.urs.microsoft.com
vortex.data.microsoft.com
vortex-sandbox.data.microsoft.com
vortex-win.data.microsoft.com
watson.live.com

This interesting website suggest to also include the following entries, in which those having opencandy are especially bad:

a.ads2.msads.net
adsmockarc.azurewebsites.net
api.opencandy.com
b.ads1.msn.com
b.ads2.msads.net
bi.bisrv.com
bingads.microsoft.com
cdn.opencandy.com
dl.delivery.mp.microsoft.com
image.online-convert.com/convert-to-ico
media.opencandy.com
offer.alibaba.com
sb.scorecardresearch.com
softonic.com
sourceforge.net
spynet2.microsoft.com
spynetalt.microsoft.com
sqm.microsoft.com
tracking.opencandy.com
tracking.opencandy.com.s3.amazonaws.com
watson.ppe.telemetry.microsoft.com
watson.telemetry.microsoft.com
watson.telemetry.microsoft.com.nsatc.net
wes.df.telemetry.microsoft.com
www.bestvistadownloads.com
www.softonic.com

Softonic is a not very reliable software download site, whereas I would not consider sourceforge bad. Alibaba is a Chinese e-commerce site. Another one I would include myself is www.brothersoft.com, which like softonic has its own downloader, which to me is a bit suspicious.