

# Windows 10 – Schneller, sicherer & anonym (Stand: 05.06.2021)

## 1. Vorbereitungen

2. Installation
3. Telemetrie-Daten verhindern
4. Microsoft Datensenden verhindern
5. Office Spy deaktivieren
6. Windows Defender in die Sandbox
7. Privacy Settings
8. Software, Features und Dienste
9. User Account ohne Admin-Rechte

## ISO-Image-Datei herunterladen (~5 GB)

Windows Systemanforderungen prüfen (Siehe Link).

Prozessor-Architektur am Computer prüfen, 64-Bit oder 32-Bit? Richtige Version auswählen.

Die Windows 10 Download-Seite hat sich seit Juli 2021 verändert. Wenn man keine Windows 10 CD oder ISO-Datei hat, muss das MediaCreationTool installiert werden um eine Windows 10 ISO-Datei von Microsoft zu bekommen.

Download-Seite 1: <https://www.microsoft.com/de-de/software-download/windows10ISO> (Stand: 05.06.2021)

UPDATE: Download Seite 2: <https://www.microsoft.com/de-de/software-download/windows10> (Stand: 09.06.21)

Auf „**Tool jetzt herunterladen**“ klicken, **MediaCreationTool21H1.exe** speichern und ausführen.

Für dieses Tool muss man im Administrator-Konto angemeldet sein, „Als administrator ausführen“ genügt nicht.

Um die heruntergeladene ISO-Datei zu prüfen, erschien nach dem Klick auf Download normalerweise der Spoiler „Überprüfung des Downloads“ (Stand: Mai 2021). Dort fand man eine Anleitung mit Hash-Wert-Tabelle:

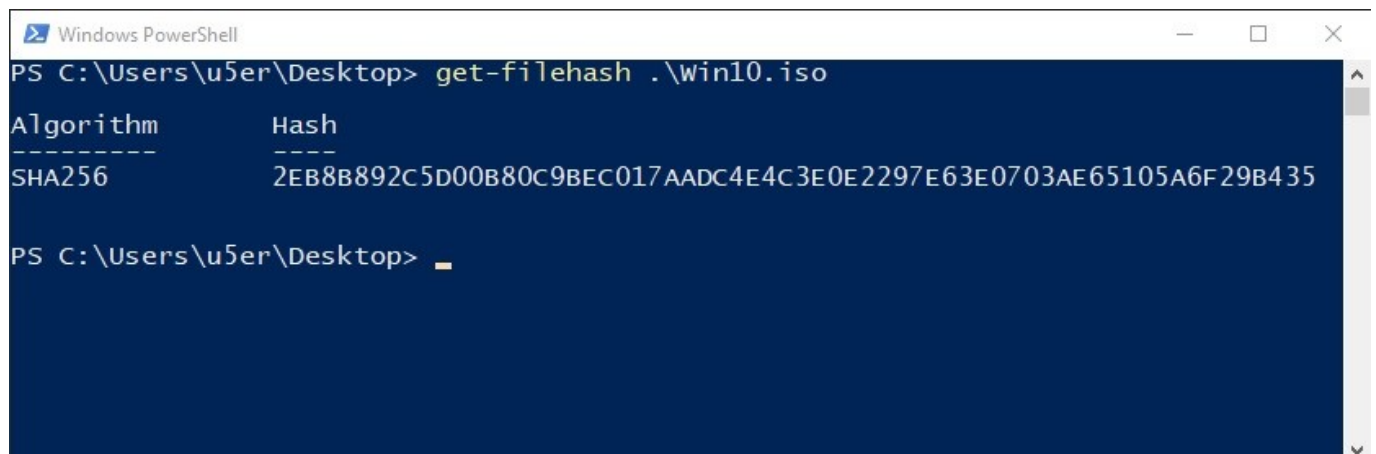
- Berechnen Sie in PowerShell den Hash-Wert der von Ihnen heruntergeladenen ISO-Datei mit dem Befehl **Get-FileHash**. Beispiel:

```
Get-FileHash C:\Users\benutzer1\Downloads\Contoso8_1_ENT.iso
```

- Wenn die SHA256-Ausgabe mit dem Wert in der Tabelle für das heruntergeladene Produkt übereinstimmt, bestätigt dies, dass die Datei nicht beschädigt ist, nicht manipuliert wurde und keine Änderungen gegenüber dem Original aufweist.

Der Hash-Wert sollte versichern dass der Download fehlerfrei und nicht manipuliert ist. Komischerweise ist das momentan nicht mehr möglich. Falls es aber wieder verfügbar wird, ist hier meine Anleitung:

Im Ordner wo die ISO-Datei liegt → Rechtsklick mit gedrückter SHIFT-Taste → „**PowerShell-Fenster hier öffnen**“ klicken. Windows PowerShell → „**get-filehash .\<hier der Name der Datei mit Punkt und Dateiendung>**“ eingeben, ENTER. Der Hashwert wird nun mit dem SHA256-Algorithmus berechnet und angezeigt, das kann dauern.



```
Windows PowerShell
PS C:\Users\u5er\Desktop> get-filehash .\win10.iso

Algorithm      Hash
-----
SHA256         2EB8B892C5D00B80C9BEC017AADC4E4C3E0E2297E63E0703AE65105A6F29B435

PS C:\Users\u5er\Desktop> _
```

Normalerweise hat eine Downloadseite mit ISOs immer eine Hashwert-Tabelle zum vergleichen des Werts, aber bei Microsoft wurde es scheinbar ohne Begründung rausgenommen. ( Aluhut glüht...)

# Windows 10 – Schneller, sicherer & anonym (Stand: 05.06.2021)

## 1. **Vorbereitungen**

2. Installation
3. Telemetrie-Daten verhindern
4. Microsoft Datensenden verhindern
5. Office Spy deaktivieren
6. Windows Defender in die Sandbox
7. Privacy Settings
8. Software, Features und Dienste
9. User Account ohne Admin-Rechte

## Windows Produktschlüssel finden und aufschreiben

...sieht ungefähr so aus → PRODUCT KEY: TYG4C-JDJ7H-VJWF3-DY5XD-HCFC6

Bevor man sein aktuelles Windows mit der neuen Installation überschreibt sollte man vorher noch, falls vorhanden, den benutzten Produkt-Schlüssel herausfinden oder von lizenzierten Quellen erwerben.

Wo man den **Produkt-Key** findet hängt davon ab wie man die Windows-Kopie erworben hat. Zum Beispiel auf Produkt Beilagen, in Emails vom Onlineverkäufer oder Microsoft, im Windows 10 App-Store oder als Aufkleber. Bei neuen PCs ist er meist digital im BIOS oder in der UEFI-Firmware vorinstalliert und wird dann wieder weiter übernommen. Den konnte man bei älteren Windows Versionen in der PowerShell, mit dem Befehl auslesen:

**„wmic path SoftwareLicensingService get OA3xOriginalProductKey“**

Fun-Fact: Früher haben viele die Keys aus Google-Bilder-Suchergebnissen abgegriffen.

### Registry-Methode

Wenn der Key nicht erscheint und er sich auf der aktuellen Windows-Installation befindet kann man die Registry-Methode probieren.

ACHTUNG: funktioniert nur bei älteren Windows 10 Versionen.

Startmenü → „explorer“ eingeben. Explorer öffnen.

Im Explorer, obere Menüleiste → „**Ansicht**“ → „**Optionen**“ öffnen.

„**Ordneroptionen**“-Fenster→ Kartei: „**Ansicht**“ → „**Erweiterte Einstellungen**“:

„**Erweiterungen bei bekannten Dateitypen ausblenden**“-Markierung aufheben.

Mit Rechtsklick auf Desktop klicken. → Neu → Neues Textdokument erstellen, Inhalt einfügen:

```
Set WshShell = CreateObject("Wscript.Shell")
MsgBox ConvertToKey(WshShell.RegRead("HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\DigitalProductId"))
Function ConvertToKey(Key)
Const KeyOffset = 52
i = 28
Chars = "BCDFGHJKMPQRTVWXY2346789"
Do
Cur = 0
x = 14
Do
Cur = Cur * 256
Cur = Key(x + KeyOffset) + Cur
Key(x + KeyOffset) = (Cur \ 24) And 255
Cur = Cur Mod 24
x = x - 1
Loop While x >= 0
i = i - 1
KeyOutput = Mid(Chars, Cur + 1, 1) & KeyOutput
If ((29 - i) Mod 6) = 0 And (i <> -1) Then
i = i - 1
KeyOutput = "-" & KeyOutput
End If
Loop While i >= 0
ConvertToKey = KeyOutput
End Function
```

Speichern als... „WindowsKey.vbs“. Datei ausführen, jetzt wird der Produkt-Key angezeigt.

Tipp für die Verwendung von Virtual Machines: Auslaufenden Key verwenden, Windows kann im gültigen Zustand gespeichert werden.

Link zu solchen Keys hier→ [https://www.majorgeeks.com/content/page/list\\_of\\_generic\\_keys\\_to\\_use\\_in\\_windows\\_10.html](https://www.majorgeeks.com/content/page/list_of_generic_keys_to_use_in_windows_10.html)

Alte Windows 7 oder 8.1 Produkt Keys funktionieren auch, Microsoft gewährt dann ein freies Upgrade. Das ist so weil Windows 10 am Anfang so unbeliebt war, dass die meisten bei Windows 7 geblieben sind. Heute ist der Umstieg auf Windows 10 lohnenswerter. Die Performance hat sich verbessert, es schont die Ressourcen besser als Windows 7 und der Update-Support ist aktuell. Microsoft hat den Support für Windows 7 seit Januar 2020 eingestellt, und somit auch die Update-Versorgung. Wer immer noch mit Windows 7 oder XP im Internet unterwegs ist geht ein hohes Risiko ein.

Fun-Fact: Viele Behörden in Deutschland benutzen immer noch Windows 7, z.B. bei der Bundeswehr. ... 〰(ツ)〰

# Windows 10 – Schneller, sicherer & anonymer (Stand: 05.06.2021)

1. Vorbereitungen
2. **Installation**
3. **Telemetrie-Daten verhindern**
4. Microsoft Datensenden verhindern
5. Office Spy deaktivieren
6. Windows Defender in die Sandbox
7. Privacy Settings
8. Software, Features und Dienste
9. User Account ohne Admin-Rechte

## PC neustarten und im BIOS das Installationsmedium booten

PC herunterfahren oder neustarten → Um ins BIOS-Menü zu gelangen muss man direkt nach dem Einschalten bzw. nach dem Neustart üblicherweise die Entf-Taste durchtippen bis das Menü erscheint. Es kann je nach Motherboard aber auch eine andere Taste sein, einfach mal das Motherboard googeln wenn es nicht klappt.

Im BIOS-Menü sucht man jetzt nach den Boot-Optionen. Dort sollten die angeschlossenen Datenträger zusehen sein. Achtung, nicht mit den Boot-Reihenfolge-Einstellungen verwechseln. Heutige Motherboards bieten normalerweise auch die Möglichkeit einen Boot direkt aus dem BIOS-Menü auszuführen, ohne Boot-Reihenfolge-Einstellungen zu ändern. Falls vorhanden sollte die Option UEFI-Boot aktiviert sein. Wenn auf dem Bildschirm die Windows Installations-Optionen erscheinen hat man alles richtig gemacht, falls nicht muss man den PC neustarten und die Boot-Auswahl durchprobieren.

## Die Installation

Sprache, Uhrzeit und Tastatur einstellen → „**Weiter**“ klicken → „**Jetzt installieren**“ klicken

Product Key eingeben oder auf „**Ich habe keinen Produkt Key**“ klicken

Jetzt haben wir die Auswahl zwischen verschiedene Windows 10-Varianten:

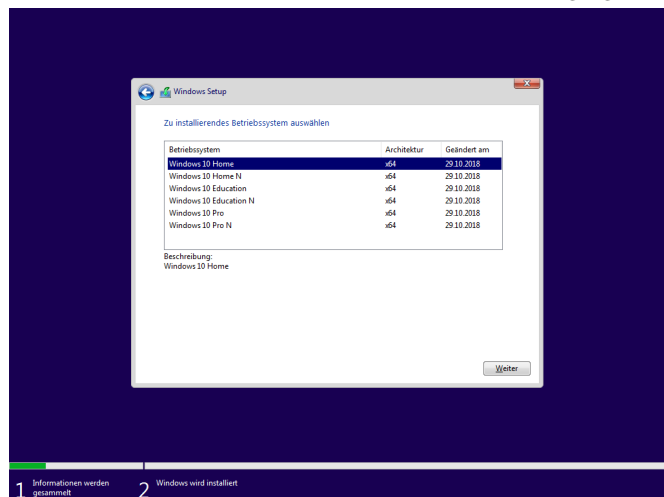
Windows 10 **Home**, **Education** oder **Pro**. Jeweils mit und ohne das „**N**“, das einfach „**Not with Media Player**“ bedeutet (ohne Windows Media Player). **ACHTUNG:** Windows N-Editionen sind unkompatibel mit Webcams oder Mikrofone, man müsste das „Windows Media-Feature Pack“ herunterladen und nachinstallieren. Mit Windows 10 Pro macht man nichts falsch...

### Windows 10 Versionen:

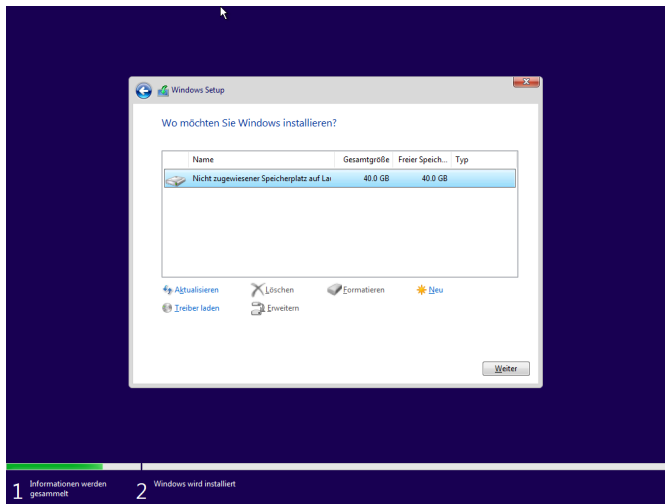
Version 1507  
Version 1511 (November Update)  
Version 1607 (Anniversary Update)  
Version 1703 (Creators Update)  
Version 1709 (Fall Creators Update)  
Version 1803 (April 2018 Update)  
Version 1809 (October 2018 Update)  
Version 1903 (May 2019 Update)  
Version 1909 (November 2019 Update)  
Version 2004 (May 2020 Update)  
Version 20H2 (October 2020 Update)  
**Version 21H1** (May 2021 Update)

### Windows 10 Editionen:

**Windows Home** → PCs, Tablets und 2-in-1 PCs für Normalverbraucher  
**Windows Pro** → Zusätzliche Fähigkeiten, für Profis und Geschäftsumgebungen wie Active Directory, Remote Desktop, BitLocker, Hyper-V und Windows Defender Device Guard.  
**Windows Education** → Für Studenten und Bildungseinrichtungen.  
**Windows Pro Education** → Wie die Pro-Edition aber mit deaktivierten Standardeinstellungen und ohne Cortana, Microsoft Store Vorschläge, Windows Sandbox oder Windows Spotlight.  
**Windows Enterprise** → Alle Features aus der Pro-Edition mit zusätzlichen Eigenschaften für IT- basierte Organisationen.  
**Windows China Government Edition** → Ohne Eigenschaften die von chinesischen Regierungsbeamten nicht gebraucht werden und mit Erlaubnis zur Benutzung von internen Verschlüsselungs-Algorithmen.



# Windows 10 – Schneller, sicherer & anonym (Stand: 05.06.2021)

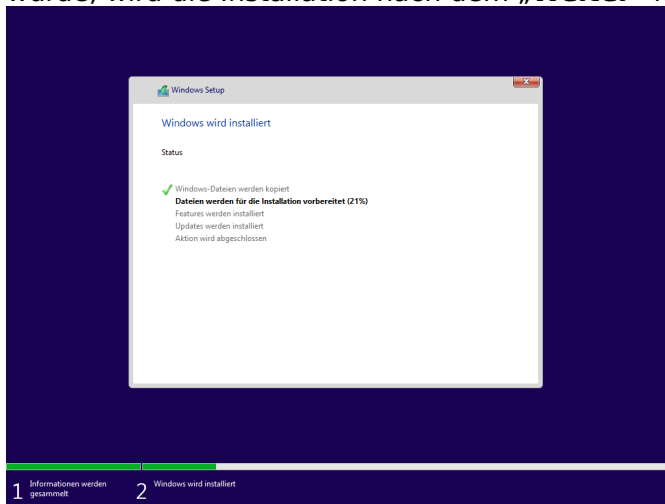


## Festplatte einrichten

Als Installations-Art wählen wir „**Benutzerdefiniert**“ damit man den Speicherplatz auf Festplatten bestimmen oder frei machen kann. Ich empfehle auch die alte MBR-Bootpartition zu löschen, es kann vorkommen das sie sonst neben der neuen Bootpartition verbleibt. Eine Bootpartition gehört normalerweise an den Anfang eines Datenträgers, die Position der Windows Partition kann dagegen frei gewählt werden. Das BIOS sucht im ersten Cluster (8x 512 Bytes) die Hexadezimalen „AA55“, damit wird der Bootsektor erkannt und ausgeführt. Auch „Magic of Hex AA55“ genannt.

Fun-Fact: Das Wort Boot hat etwas mit „Bootstrapping“ zu tun, was in der englischen Sprache so was wie das „Stiefel anziehen nachdem man aus dem Bett steigt“ bedeutet.

Wenn die Partitionen vorbereitet sind oder einfach ein freies, komplettes Laufwerk gewählt wurde, wird die Installation nach dem „**Weiter**“ klicken beginnen.



## Windows einrichten

**Region** wählen → **Tastatur-Layout** wählen → Warten.

„**Für persönliche Verwendung einrichten**“ wählen.

Unten links auf „**Offlinekonto**“ klicken → Nochmal links unten auf „**Eingeschränkte Erfahrung**“ klicken.

Administratorkonto-Namen bestimmen → Kennwort erstellen.

**Cortana** ablehnen → **Aktivitätsverlauf** ablehnen → **Onlinespracherkennung** ablehnen.

**Standort** Funktion ablehnen. „**Mein Gerät suchen**“ ablehnen → **Diagnosedaten** „Einfach“ wählen.

**Freihand und Eingabe Verbesserung** ablehnen. **Angepasste Erfahrungen** ablehnen.

**Werbe-ID** ablehnen → Warten → Installation ist abgeschlossen.

# Windows 10 – Schneller, sicherer & anonym (Stand: 05.06.2021)

1. Vorbereitungen
2. Installation
3. Telemetrie-Daten verhindern
- 4. Microsoft Datensenden verhindern**
5. Office Spy deaktivieren
6. Windows Defender in die Sandbox
7. Privacy Settings
8. Software, Features und Dienste
9. User Account ohne Admin-Rechte

Jetzt sollte man wichtige Einstellungen vornehmen, das wird viel Zeit brauchen weil in Windows 10 standardmäßig immer noch viele ungewollte Funktionen aktiv sind. Das Deaktivieren bringt mehr Anonymität und macht das System schneller, auch sicherer weil Angriffsvektoren reduziert werden.

## Microsoft Hosts-Datei bearbeiten

Startmenü → „powershell“ eingeben, Windows PowerShell mit Rechtsklick als Administrator ausführen.

Windows PowerShell → „**notepad C:\Windows\system32\drivers\etc\hosts**“ eingeben, Enter-Taste.

C:\Windows\system32\drivers\etc\hosts → In der Datei folgende Zeilen am Ende einfügen:

127.0.0.1 a-0001.a-msedge.net	127.0.0.1 m.hotmail.com
127.0.0.1 a.ads1.msn.com	127.0.0.1 modern.watson.data.microsoft.com.akadns.net
127.0.0.1 a.ads2.msads.net	127.0.0.1 msftncsi.com
127.0.0.1 a.ads2.msn.com	127.0.0.1 msntest.serving-sys.com
127.0.0.1 a.rad.msn.com	127.0.0.1 oca.telemetry.microsoft.com
127.0.0.1 ac3.msn.com	127.0.0.1 oca.telemetry.microsoft.com.nsatc.net
127.0.0.1 ad.doubleclick.net	127.0.0.1 pre.footprintpredict.com
127.0.0.1 adnexus.net	127.0.0.1 preview.msn.com
127.0.0.1 adnxs.com	127.0.0.1 pricelist.skype.com
127.0.0.1 ads1.msads.net	127.0.0.1 rad.live.com
127.0.0.1 ads1.msn.com	127.0.0.1 rad.msn.com
127.0.0.1 ads.msn.com	127.0.0.1 redir.metaservices.microsoft.com
127.0.0.1 aidps.atdmt.com	127.0.0.1 reports.wes.df.telemetry.microsoft.com
127.0.0.1 aka-cdn-ns.adtech.de	127.0.0.1 s.gateway.messenger.live.com
127.0.0.1 apps.skype.com	127.0.0.1 secure.adnxs.com
127.0.0.1 az361816.vo.msecnd.net	127.0.0.1 secure.flashtalking.com
127.0.0.1 az512334.vo.msecnd.net	127.0.0.1 services.wes.df.telemetry.microsoft.com
127.0.0.1 b.ads1.msn.com	127.0.0.1 settings-sandbox.data.microsoft.com
127.0.0.1 b.ads2.msads.net	127.0.0.1 sls.update.microsoft.com.akadns.net
127.0.0.1 b.rad.msn.com	127.0.0.1 sO.2mdn.net
127.0.0.1 bs.serving-sys.com	127.0.0.1 sqm.df.telemetry.microsoft.com
127.0.0.1 c.atdmt.com	127.0.0.1 sqm.telemetry.microsoft.com
127.0.0.1 c.msn.com	127.0.0.1 sqm.telemetry.microsoft.com.nsatc.net
127.0.0.1 cdn.atdmt.com	127.0.0.1 static.2mdn.net
127.0.0.1 cds26.ams9.msecn.net	127.0.0.1 statsfe1.ws.microsoft.com
127.0.0.1 choice.microsoft.com	127.0.0.1 statsfe2.update.microsoft.com.akadns.net
127.0.0.1 choice.microsoft.com.nsatc.net	127.0.0.1 statsfe2.ws.microsoft.com
127.0.0.1 compatexchange.cloudapp.net	127.0.0.1 survey.watson.microsoft.com
127.0.0.1 corp.sts.microsoft.com	127.0.0.1 telecommand.telemetry.microsoft.com
127.0.0.1 corptext.msitadfs.glbdns2.microsoft.com	127.0.0.1 telecommand.telemetry.microsoft.com.nsatc.net
127.0.0.1 cs1.wpc.v0cdn.net	127.0.0.1 telemetry.appex.bing.net
127.0.0.1 cy2.vortex.data.microsoft.com.akadns.net	127.0.0.1 telemetry.appex.bing.net:443
127.0.0.1 db3aqu.atdmt.com	127.0.0.1 telemetry.microsoft.com
127.0.0.1 df.telemetry.microsoft.com	127.0.0.1 telemetry.urs.microsoft.com
127.0.0.1 diagnostics.support.microsoft.com	127.0.0.1 ui.skype.com
127.0.0.1 ec.atdmt.com	127.0.0.1 v10.vortex-win.data.microsoft.com
127.0.0.1 fe2.update.microsoft.com.akadns.net	127.0.0.1 view.atdmt.com
127.0.0.1 feedback.microsoft-hohm.com	127.0.0.1 vortex-sandbox.data.microsoft.com
127.0.0.1 feedback.search.microsoft.com	127.0.0.1 vortex-win.data.microsoft.com
127.0.0.1 feedback.windows.com	127.0.0.1 vortex.data.microsoft.com
127.0.0.1 flex.msn.com	127.0.0.1 watson.live.com
127.0.0.1 g.msn.com	127.0.0.1 watson.microsoft.com
127.0.0.1 h1.msn.com	127.0.0.1 watson.ppe.telemetry.microsoft.com
127.0.0.1 h2.msn.com	127.0.0.1 watson.telemetry.microsoft.com
127.0.0.1 i1.services.social.microsoft.com	127.0.0.1 watson.telemetry.microsoft.com.nsatc.net
127.0.0.1 i1.services.social.microsoft.com.nsatc.net	127.0.0.1 wes.df.telemetry.microsoft.com
127.0.0.1 live.rads.msn.com	127.0.0.1 www.msftncsi.com
127.0.0.1 m.adnxs.com	

# Windows 10 – Schneller, sicherer & anonym (Stand: 05.06.2021)

1. Vorbereitungen
2. Installation
3. Telemetrie-Daten verhindern
4. Microsoft Datensenden verhindern
5. **Office Spy deaktivieren**
6. **Windows Defender in die Sandbox**
7. Privacy Settings
8. Software, Features und Dienste
9. User Account ohne Admin-Rechte

## Microsoft Office Spy Deaktivierungs-Datei erstellen - Deaktivierung registrieren/ausführen

Startmenü → „explorer“ eingeben. Explorer öffnen.

Im Explorer, obere Menüleiste → „**Ansicht**“ → „**Optionen**“ öffnen.

„**Ordneroptionen**“-Fenster → Kartei: „**Ansicht**“ → „**Erweiterte Einstellungen**“:

- „**Erweiterungen bei bekannten Dateitypen ausblenden**“-Markierung aufheben.
- „**Ausgeblendete Dateien... ausblenden**“ markieren.

Textdokument erstellen → umbenennen in „DisableOfficeSpy.reg“ → Rechtsklick auf Datei, „**bearbeiten**“ klicken.

DisableOfficeSpy.reg → In der Datei folgenden Inhalt einfügen:

```
Windows Registry Editor Version 5.00
[HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\common\
privacy]
"disconnectedstate"=dword:00000002
"usercontentdisabled"=dword:00000002
"downloadcontentdisabled"=dword:00000002
"controllerconnectedservicesenabled"=dword:00000002
[HKEY_CURRENT_USER\Software\Policies\Microsoft\office\common\
clienttelemetry]
"sendtelemetry"=dword:00000003
```

Abspeichern und Datei ausführen. Muss für jedes Benutzerkonto wiederholt werden.

## Windows Defender Sandbox aktivieren

Startmenü → „powershell“ eingeben. Windows PowerShell mit Rechtsklick „**Als Administrator ausführen**“.

Windows PowerShell → „**setx /M MP\_FORCE\_USE\_SANDBOX 1**“ eingeben, Enter-Taste.

Ab jetzt werden Windows-Defender Virenschans in einer simulierten Umgebung ausgeführt, abgeschirmt vom Rest des Systems. Geht nur in den Windows Pro Editionen.

## Automatische Wiedergabe deaktivieren

Wenn man sehr paranoid ist kann man auch die Miniatur-Vorschaubilder für Bilddateien und automatische Wiedergabe von Medien und Geräten deaktivieren, ein kleiner Schutz gegen Schadprogramme in USB-Sticks oder Bildern.

Startmenü → Einstellungen öffnen → „**Geräte**“ → „**Automatische Wiedergabe**“ → „**Aus**“

Startmenü → „explorer“ eingeben. Explorer öffnen.

Im Explorer, obere Menüleiste → „**Ansicht**“ → „**Optionen**“ öffnen.

„**Ordneroptionen**“-Fenster → Kartei: „**Ansicht**“ → „**Erweiterte Einstellungen**“:

„**Dateisymbol auf Miniaturansichten anzeigen**“ markieren und auf OK klicken.

# Windows 10 – Schneller, sicherer & anonym (Stand: 05.06.2021)

1. Vorbereitungen
2. Installation
3. Telemetrie-Daten verhindern
4. Microsoft Datensenden verhindern
5. Office Spy deaktivieren
6. Windows Defender in die Sandbox
7. **Privacy Settings**
8. **Software, Features und Dienste**
9. User Account ohne Admin-Rechte

## Datenschutzeinstellungen ändern

- **Freihand- und Eingabeanpassung** → Alles deaktivieren.
- **Aktivitäten-Verlauf** → Alles deaktivieren und auf „**Löschen**“ klicken.
- **Positionserkennung** → Alles deaktivieren.
- Die **Kamera-** und **Mikrofon-Einstellungen** bei Bedarf aktiviert lassen, ansonsten deaktivieren.
- **Telefonanrufe** → „**Apps dürfen Telefonanrufe durchführen**“ deaktivieren.
- **Hintergrund-Apps** → Nur „**Windows-Sicherheit**“ aktiviert lassen, alles andere deaktivieren.
- Theoretisch kann auch einfach alles deaktiviert und bei Bedarf wieder aktiviert werden.

## Unnötige Programme und Features deinstallieren

Startmenü → „systemsteuerung“ eingeben, Systemsteuerung öffnen. → Auf „**Programme und Features**“ klicken.

Programme und Features → Auf der linken Seite auf „**Windows-Features aktivieren oder deaktivieren**“ klicken.

Windows-Features → Internet Explorer 11 und SMB Dateifreigaben Markierung aufheben/deaktivieren. OK klicken.

Startmenü → „dienste“ eingeben, Dienste öffnen. → Windows Biometriedaten deaktivieren.

Startmenü → Einstellungen öffnen. → „**Apps**“ klicken. In der Liste kann theoretisch alles deaktiviert werden.

## Cortana deinstallieren

Startmenü → „powershell“ eingeben. Windows PowerShell mit Rechtsklick „**Als Administrator ausführen**“.

„**Get-AppxPackage -allusers Microsoft.549981C3F5F10 | Remove-AppxPackage**“

in die Windows PowerShell eingeben, Enter-Taste.

# Windows 10 – Schneller, sicherer & anonym (Stand: 05.06.2021)

1. Vorbereitungen
2. Installation
3. Telemetrie-Daten verhindern
4. Microsoft Datensenden verhindern
5. Office Spy deaktivieren
6. Windows Defender in die Sandbox
7. Privacy Settings
8. Software, Features und Dienste
9. **User Account ohne Admin-Rechte**

## Benutzerkonto ohne Administrator-Rechte erstellen

**Tipp:** Zuerst mit dem Administrator-Konto die neuesten Updates laden: Startmenü → Einstellungen → Updates

Startmenü → Einstellungen → Konten → Familie & andere Benutzer

→ „**Eine weitere Person zu diesem PC hinzufügen**“ klicken.

→ „**Ich kenne die Anmeldeinformationen für diese Person nicht**“ klicken.

→ „**Benutzer ohne Microsoft-Konto hinzufügen**“ klicken.

→ Benutzernamen, Kennworthinweis und Sicherheitsfragen erstellen und dann auf Weiter.

Dieses Konto muss dann nochmal mit den oben genannten Schritten eingestellt werden. Den Computer ab jetzt immer mit dem Benutzerkonto ohne Admin-Rechte benutzen und administrative Zugriffe nur noch bei Bedarf zulassen. Das ist eine gängige Vorsorge gegen Schadcode in ausgeführten Programmen und Dateien.

Um den ganzen Prozess in Zukunft nicht wiederholen zu müssen, sollte man sich Backup-Software besorgen.

Viel Erfolg !