



Ihr PC-Sicherheits-Berater

So schützen Sie Ihre Privatsphäre und sensiblen Daten

3 Sind Werbeprogramme auf Ihrem PC versteckt?

Spüren Sie mit meiner Schritt-für-Schritt-Anleitung alle unerwünschten Programme auf und löschen Sie diese per Mausklick.

4 Senden Spionagedienste Ihre Daten ins Internet?

Schützen Sie sich vor der Daten-Schnüffelei: Kontrollieren Sie mit meiner Hilfe, ob auf Ihrem PC Spionagedienste aktiv sind.

5 Stoppen Sie die App-Werbung von Microsoft

Erteilen Sie Microsoft Hausverbot auf Ihrem PC. Das Installieren der Werbe-Apps hört dann unverzüglich auf.

6 Was verrät Ihr Browser über Sie?

Toolbars überwachen alle Ihre Eingaben im Internet. Befreien Sie Ihren Browser daher von diesen Internet-Spannern.

So arbeiten Sie an einem sauberen PC: Löschen Sie alle verborgenen Spionagedienste

Spioniert Windows 10 Sie hinterhältig aus und verletzt Ihre Privatsphäre?

Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) hat eine Studie mit der Bezeichnung „SiSyPHuS Win10“ zur Sicherheit von Windows 10 in Auftrag gegeben.

Jetzt wurde ein erstes Zwischenergebnis veröffentlicht. Im Bericht „Analyse der Telemetrikkomponente in Windows 10“ gibt das BSI konkrete Empfehlungen, wie Sie die Datenübertragung vollständig deaktivieren.

Über unsere sichere Service-Webseite gelangen Sie direkt zu diesem Bericht. Er erfordert allerdings zum Verständnis fortgeschrittene Systemkenntnisse und das Umsetzen kostet Sie erheblich Zeit.

Die Fernwartungsdaten sind nicht die einzige Spionage-Lücke: Microsoft spioniert Sie weitaus mehr über seine Apps aus. Es gibt also wichtigere Datenschutz-Maßnahmen als nur die Fernwartungsdaten zu unterdrücken.

Meine Empfehlung: Reinigen Sie Ihren PC mit den nachfolgenden 7 Reinigungsaktionen von allen unerwünschten Microsoft-Apps und sonstigen Werbeprogrammen.



Viele Grüße, Ihr

Michael-Alexander
Beisecker,
Deutschlands

PC-Sicherheitsexperte Nr. 1

Finden und deinstallieren Sie alle unnötigen Apps, Dienste und Programme

Säubern Sie Ihren PC in nur 7 Reinigungsaktionen

Kaufen Sie einen neuen PC, enthält dieser zusätzlich zu Windows 10 oft unerwünschte Werbeprogramme, die sich nur schwer entfernen lassen. Die Gefahr unerwünschter Programme besteht auch beim Herunterladen von Programmen aus dem Internet. Mit meinen 7 Reinigungsaktionen entdecken und entfernen Sie die lästigen Werbeprogramme und erhalten die Kontrolle über Ihren PC zurück.

Ich finde bei Leserbesuchen immer wieder reihenweise unerwünschte Programme auf den Geräten. Das trifft sowohl auf brandneue PCs und Notebooks zu als auch auf viele Jahre alte Rechner. Da sind selbst meine erfahrensten Leser überrascht, was sich auf ihren sorgsam konfigurierten PCs für üble Software-Schmarotzer befinden.

Früher hatten Sie die Kontrolle: Ein neuer PC enthielt nichts weiter als das Betriebssystem. Jetzt ist schon das Betriebssystem Windows 10 mit Werbe-Apps verseucht und es werden täglich mehr. Denn Microsoft installiert ständig neue Apps über den Windows Store, ohne Sie um Erlaubnis zu fragen oder sich darum zu kümmern, ob Sie diese Apps überhaupt interessieren.

Sie entgehen dem Programm-Terror nicht mehr wie früher durch Download-Enthaltensamkeit und Programm-Disziplin. Selbst in Ihren wichtigsten Programmen wie dem Internet-Browser verbergen sich dubiose Erweiterungen, die Daten übertragen oder Sie gar zu Werbeseiten entführen.

Meine Lösung: Enttarnen Sie sämtliche Spionageprogramme auf Ihrem PC – bis hin zum letzten heimlich laufenden Hintergrunddienst. Schalten Sie die ganzen Gefahren mit meiner Anleitung einfach ab!

Fegen Sie alle unerwünschten Programme von Ihrem PC:

- Reinigungsaktion 1: Reagieren Sie nicht auf hartnäckige Werbefenster (siehe Seite 2).
- Reinigungsaktion 2: Ermitteln Sie alle nicht von Ihnen installierten Programme (siehe Seite 3).
- Reinigungsaktion 3: Finden Sie die Spionagedienste der Werbeprogramme (siehe Seite 4).
- Reinigungsaktion 4: Deinstallieren Sie die unerwünschten Programme (siehe Seite 4).
- Reinigungsaktion 5: Entfernen Sie die nicht benötigten Apps (siehe Seite 5).
- Reinigungsaktion 6: Machen Sie die Browser-Erweiterungen unschädlich (siehe Seite 6).
- Reinigungsaktion 7: Kontrollieren Sie Ihren PC noch einmal mit dem Gratis-Tool The PC Decrapifier (siehe Seite 8).

Diese 7 Reinigungsaktionen garantieren Ihnen einen sauberen PC.

>>> Lesen Sie bitte weiter auf Seite 2

Reinigungsaktion 1: Reagieren Sie nicht auf hartnäckige Werbefenster

Diese erste Reinigungsaktion ist ganz wichtig bei neuen Notebooks, aber auch bei älteren PCs, bei denen hartnäckig Werbefenster eingeblendet werden. Es erscheinen Dutzende von Werbefenstern und Meldungen, die Ihnen weisen, dass Sie etwas geschenkt bekommen, eine Anmeldung nötig sei oder dass Sie das betreffende Angebot unbedingt brauchen. Teilweise wird der gesamte Bildschirm verdeckt und Sie werden praktisch wie bei einem Erpresser-Trojaner davon abgehalten, auf den Windows-Desktop zu gelangen. Es ist ganz wichtig, dass Sie hier die Ruhe bewahren und die folgenden sieben Regeln befolgen. Starten Sie die Überprüfung am besten gleich, so behalten Sie immer die Kontrolle über Ihren PC.

Regel 1: Keine Schaltfläche anklicken

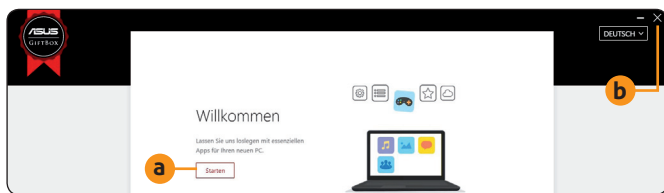
Klicken Sie in Werbefenstern nicht auf die angebotenen Schaltflächen wie zum Beispiel **Starten** **a**. Es werden sonst Programme installiert, die Sie nachher nur sehr schwer wieder loswerden.

Regel 2: Lassen Sie sich nicht erpressen

Versperren Ihnen Fenster wie im Fall der ASUS-GiftBox (siehe Bild bei Regel 3) den Weg, nutzen Sie die drei Symbole rechts oben im Fenster: Schließen Sie das Fenster über das **Schließen-Symbol** **b**, verkleinern Sie es per Klick auf das **Verkleinern-Symbol** oder legen Sie es über das **Minimieren-Symbol** in der Taskleiste ab. Sie können die Werbeprogramme auch über **[Alt]+[F4]** nacheinander schließen, mit **[Alt]+[↵]** zu einem anderen Fenster wechseln oder bei Windows 10 einfach auf einen anderen Desktop wechseln und von dort aus die folgenden Reinigungsaktionen durchführen.

Regel 3: Haben Sie Geduld und geben Sie nicht auf

Manche Fenster reagieren wie im Fall der ASUS-GiftBox zunächst nicht, weil eine Wartezeit bzw. verzögerte Reaktion einprogrammiert ist. Warten Sie ab und versuchen Sie das Schließen einfach immer wieder. Irgendwann gibt das Programm auf und blendet sich aus.



Die Werbung belegt den gesamten Bildschirm und hindert Sie daran, zum Windows-Desktop zu gelangen.

Regel 4: Schützen Sie Ihre E-Mail-Adresse

Egal, was man Ihnen verspricht, geben Sie auf keinen Fall Ihre E-Mail-Adresse für eine Registrierung oder angebliche News heraus. Sie werden sonst mit Spam-Mails überschüttet – häufig auch von ganz anderen Firmen als dem PC- oder Software-Hersteller.

Regel 5: Legen Sie kein Registrierungskonto an

Nur wenn es die erweiterten Garantiebedingungen erfordern oder Sie sonst keine aktuellen Treiber erhalten, sollten Sie Ihr Notebook oder ein gekauftes Gerät beim Hersteller re-

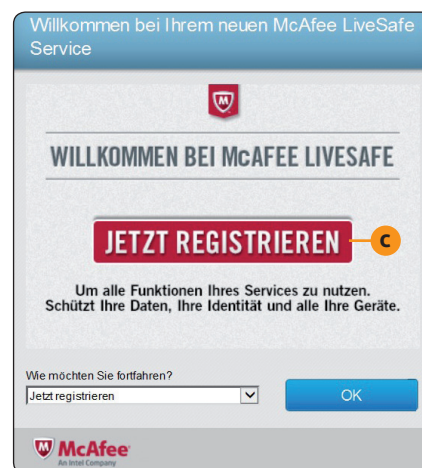
gistrieren – aber auch nur da und nicht bei einem Drittanbieter. Das geht häufig auch per Postkarte oder über die Webseite des Herstellers und Sie müssen dazu kein Werbeprogramm verwenden.

Regel 6: Fallen Sie nicht auf Lockangebote herein

Auf neuen Notebooks wird zum Beispiel McAfee Live Safe angeboten. Hierbei handelt es sich um ein kostenpflichtiges Paket aus Antiviren-Programm und Online-Speicher. Die Falle: Es kostet nach der Testphase stolze 80 € pro Jahr. Im Werbefenster wird Ihnen das verschwiegen und Sie werden sofort zur Registrierung aufgefordert **c**. Handeln Sie wie in Regel 5 beschrieben und lassen Sie sich nicht von diesen fiesen Lockangeboten verleiten.

Regel 7: Geben Sie niemals Ihre Bankkontodaten heraus

Spätestens wenn Sie nach Kontodaten gefragt werden, brechen Sie die Anmeldung ab. Ganz gleich, was man Ihnen verspricht, es ist eine Falle. Niemand fragt nach Ihren Kontodaten, wenn er kein Geld abbuchen will!



Böse Falle: Diese Werbung sieht aus wie eine Registrierung für einen kostenlosen Dienst, doch wenn Sie darauf hereinfallen, kommt eine Rechnung!

Fazit: Lassen Sie sich von den Werbefenstern nicht beeinflussen und schon gar nicht zu etwas zwingen, was Sie nicht möchten. Suchen Sie geduldig nach einem Weg, wie Sie dieses Fenster schließen oder zumindest verkleinern können. Häufig hilft die Tastenkombination **[Alt]+[F4]**. Mit den nächsten Reinigungsaktionen werden Sie diese lästigen Fenster und vor allem die dazugehörigen Programme los.

Reinigungsaktion 2: Ermitteln Sie alle nicht von Ihnen installierten Programme

Unerwünschte Werbeprogramme sind häufig nicht in der Systemsteuerung unter „Programme und Features“ (Windows 10) bzw. „Programme und Funktionen“ (Windows 7) eingetragen. Sie werden wie Schadprogramme versteckt, damit Sie die Programme nicht finden und deinstallieren. Zusätzlich laufen im Hintergrund teilweise Spionagedienste, die auch nach dem Entfernen der Werbeprogramme weiter aktiv sind. Doch keine Sorge: Sie werden kein Werbeprogramm übersehen, wenn Sie systematisch an die Suche herangehen und die nachfolgende Anleitung Schritt für Schritt ausführen.

1. Sehen Sie sich die Symbole auf dem Windows-Desktop **a** an und notieren Sie, welche Programme darüber gestartet werden. Selbst bei einem nagelneuen PC finden Sie hier etliche Programmsymbole. Zu Windows gehörende Symbole wie **Papierkorb** brauchen Sie nicht in Ihre Liste einzutragen.
2. Öffnen Sie das **Start-Menü** **b** und gehen Sie alle aufgeführten Programme durch. Achten Sie auf nicht zu Windows gehörende Programme wie solche des PC-Herstellers und anderer Firmen. Notieren Sie sich die nicht benötigten Programme.



Mein Tipp: Werfen Sie einen kritischen Blick auf Antiviren-Programme und Sicherheitspakete wie McAfee LifeSafe. Bei neuen PCs sind oft mehrere solcher Programme vorinstalliert, obwohl aus Sicherheitsgründen nur eines installiert sein sollte. Die Sicherheitsprogramme behindern sich gegenseitig und Schadprogramme nutzen diese Sicherheitslücke aus, um auf Ihren PC zu gelangen.

3. Sehen Sie sich die Symbole in der Taskleiste an **c**. Hier sind die meisten der fiesen Werbeprogramme versammelt, die Ihnen die Zeit stehlen und Sie um Ihr Geld bringen wollen.
4. Öffnen Sie mit einem Klick auf das ^-Zeichen rechts in der Taskleiste – das Symbol **Ausgeblendete Symbole einblenden** – den Info-Bereich (Systray unten rechts in der Taskleiste). Dort sehen Sie die Symbole der automatisch gestarteten Programme **d**. Zeigen Sie mit dem Mauszeiger auf ein Symbol, erfahren Sie den Programmnamen. Halten Sie die Namen aller Ihnen unbekannten Programme auf Ihrer Liste fest.
5. Klicken Sie bei Windows 10 mit der rechten Maustaste auf das **Start-Symbol** und wählen Sie **Task-Manager**, um das gleichnamige Windows-Dienstprogramm aufzurufen. Sehen Sie im Register **Autostart** nach, welche Programme automatisch mit Windows gestartet werden.

Schreiben Sie sich alle Programme auf, die nicht direkt zu Windows gehören. Ein Beispiel ist eine Office-Testversion oder ein nicht von Ihnen installiertes Antiviren- oder Datensicherungsprogramm.

Verwenden Sie Windows 7, öffnen Sie mit **Windows + R** das **Ausführen**-Fenster, geben Sie **msconfig** ein und drücken Sie die Eingabetaste **[Enter]**. Wechseln Sie in das Register **Systemstart**.



Die Symbole auf dem Desktop, in der Taskleiste und im Info-Bereich weisen Sie auf Werbeprogramme hin.

6. Gehen Sie Ihre Liste der gefundenen Programme durch und suchen Sie nach den Tools des PC-Herstellers und Programmen, die Sie nicht selbst installiert haben. Informieren Sie sich im Internet und auf Herstellerseiten über die Programme und entscheiden Sie dann, welche Sie entfernen möchten.



Notieren Sie sich Programme, bei denen der Begriff „Testversion“ **e** erscheint; es sind immer Werbeprogramme.

Meine Empfehlung: Deaktivieren und deinstallieren Sie in den nachfolgenden Schritten alle Programme, die Sie nicht interessieren. Aber seien Sie vorsichtig bei Anwendungen, die Sie nicht kennen, damit Sie nicht ein wichtiges Systemprogramm entfernen.

LESERSERVICE

Redaktionshilfe: Fragen Sie bei Sicherheitsbedenken immer zuerst Ihren persönlichen PC-Sicherheits-Berater Michael-Alexander Beisecker.

Melden Sie sich dazu einfach kostenlos unter <https://club.computerwissen.de> an und stellen Sie ihm dort Ihre Fragen.

Michael-Alexander Beisecker und seine Redaktionsmitarbeiter helfen Ihnen gern weiter. Sie erhalten werktags innerhalb von 48 Stunden eine Antwort auf Ihre Frage – garantiert.

Reinigungsaktion 3: Finden Sie die Spionagedienste der Werbeprogramme

Sie haben nun mit Reinigungsaktion 2 eine Liste Ihrer Programme erstellt und eine Auswahl getroffen. Bevor Sie die Programme deinstallieren, erforschen Sie noch deren Umfeld. Werbeprogramme haben häufig integrierte Spionagedienste, die teilweise auch nach der Deinstallation weiterlaufen und Daten ins Internet senden. Das beeinträchtigt Ihre Privatsphäre und stellt ein Sicherheitsrisiko dar. Außerdem benötigen diese Dienste Windows-Ressourcen und Internet-Bandbreite, die Sie besser für nützliche Anwendungen verwenden. Ich habe schon erlebt, dass PCs wegen solcher Spionagedienste extrem langsam waren. Die Besitzer wollten schon einen neuen PC kaufen, dabei mussten nur die schädlichen Dienste deaktiviert werden. Machen Sie diese fiesen Spionagedienste in nur 7 Schritten ausfindig.

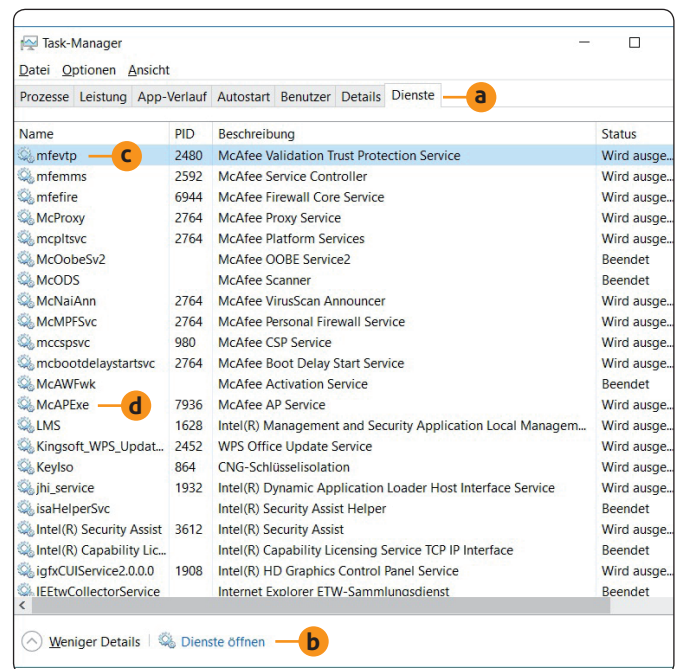
Sie können die Dienste bei Windows 10 auch über den Task-Manager aufrufen (siehe Seite 3, Schritt 5). Die folgende Anleitung funktioniert jedoch sowohl mit Windows 10 als auch Windows 7 und somit mit allen Ihren PCs:

1. Öffnen Sie mit **Windows + R** das **Ausführen**-Fenster.
2. Geben Sie **services.msc** ein und drücken Sie die Eingabetaste **[Enter]**. Das **Dienste**-Fenster öffnet sich.



Mein Tipp: Öffnet sich bei Ihnen das **Dienste**-Fenster nicht, wählen Sie den Weg über den Task-Manager wie auf Seite 3 Schritt 5 beschrieben. Aktivieren Sie im Task-Manager das Register **Dienste** **a**. Wählen Sie am unteren Rand **Dienste öffnen** **b**. Das **Dienste**-Fenster öffnet sich.

3. Wählen Sie nacheinander alle Dienste aus und lesen Sie die dazugehörige Angabe in der Spalte **Beschreibung**.
4. Gehört ein Dienst nicht zu Windows und wird nicht für eines der erwünschten Programme benötigt, klicken Sie den Eintrag mit der rechten Maustaste an und wählen **Eigenschaften**.
5. Notieren Sie sich den Eintrag unter **Pfad zur EXE-Datei**.
6. Stellen Sie **Starttyp** auf **Deaktiviert** und klicken Sie unter **Dienststatus** auf **Beenden**. Schließen Sie das Fenster **Eigenschaften** per Klick auf **OK** und blenden Sie auch das **Dienste**-Fenster wieder aus.
7. Rufen Sie den **Windows-Explorer** auf und schauen Sie, welches Programm in diesem Pfad installiert ist.



Auf dem untersuchten neuen ASUS-PC liefen 13 Dienste der Firma McAfee im Hintergrund (**mfefvt** **c** bis **McAPExe** **d**) und behinderten die Installation des gewünschten Antiviren-Programms.

Meine Empfehlung: Überprüfen Sie, ob die Dienste zu Programmen gehören, die Sie auf Ihrer Liste haben. Diese Programme deinstallieren Sie nachfolgend mit der Reinigungsaktion 4.

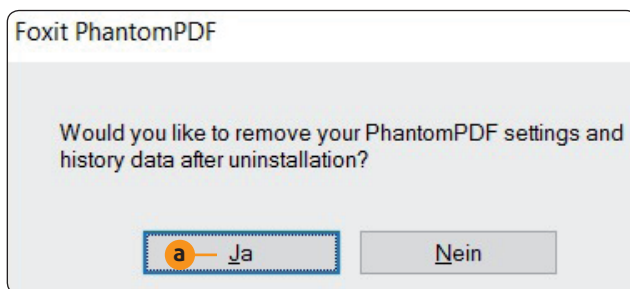
Reinigungsaktion 4: Deinstallieren Sie die unerwünschten Programme

Nachdem Sie in Reinigungsaktion 2 die unerwünschten Programme festgelegt und in Reinigungsaktion 3 deren versteckte Dienste deaktiviert haben, lassen sich die meisten Werbeprogramme recht einfach über die Systemsteuerung von Windows entfernen. Zu den Ausnahmen wie Apps und Browser-Erweiterungen kommen wir in den anschließenden Reinigungsaktionen. Verbannen Sie die unerwünschten Programme ganz einfach per Mausklick.

Schritt für Schritt verbannen Sie die störenden Werbeprogramme von Ihrem PC:

1. Öffnen Sie mit **Windows + R** das **Ausführen**-Fenster. Geben Sie **control** ein und drücken Sie die Eingabetaste **[Enter]**.

2. Stellen Sie **Anzeige** oben rechts auf **Große Symbole** und wählen Sie **Programme und Features** (Windows 10) oder **Programme und Funktionen** (Windows 7).
3. Klicken Sie auf die Überschrift **Name**, damit die installierten Programme alphabetisch sortiert werden.
4. Klicken Sie die nicht benötigten Programmeinträge mit der rechten Maustaste an und wählen Sie **Deinstallieren**. Folgen Sie dann dem Assistenten zur Deinstallation.
5. Sie werden teilweise mehrere Abfragen erhalten, ob Sie das Programm wirklich deinstallieren möchten **a**. Bleiben Sie standhaft und klicken Sie auf **Ja**.



Lassen Sie sich nicht verunsichern, wenn während der Deinstallation Abfragen in englischer Sprache erscheinen.

Übersetzungshilfe starten: Fremdsprachliche Meldungen lassen Sie sich in Minutenschnelle vom Google-

Übersetzer übersetzen. Sie erreichen den Google-Übersetzer am Link

<https://translate.google.com/?hl=de>.

Wenn Ihnen eine Meldung unverständlich ist, können Sie mich und meine Mitarbeiter aus der Redaktion selbstverständlich jederzeit über den Computerwissen Club um Rat fragen. Wir helfen Ihnen gern weiter:

<https://club.computerwissen.de>.



6. Deinstallieren Sie alle nicht benötigten Programme und starten Sie den PC neu. Jetzt sollten keine Werbefenster mehr erscheinen.
7. Gehen Sie die Schritte der Reinigungsaktion 2 erneut durch und sehen Sie sich den Desktop, das **Start**-Menü, die Taskleiste, den Info-Bereich sowie das Register **Auto-start** des Task-Managers an. Überprüfen Sie auch noch einmal – wie in Reinigungsaktion 3 beschrieben – die Dienste. Finden Sie hier noch Hinweise auf Werbeprogramme, deinstallieren Sie diese nach Möglichkeit ebenfalls.

Meine Empfehlung: Stellen Sie fest, dass noch Werbe- und Spionageaktivitäten vorhanden sind, aber Sie finden dafür keinen Programmeintrag in der Systemsteuerung, suchen Sie nicht lange. Es handelt sich wahrscheinlich um eine App oder eine Browser-Erweiterung. Dazu kommen wir in den nächsten beiden Reinigungsaktionen.

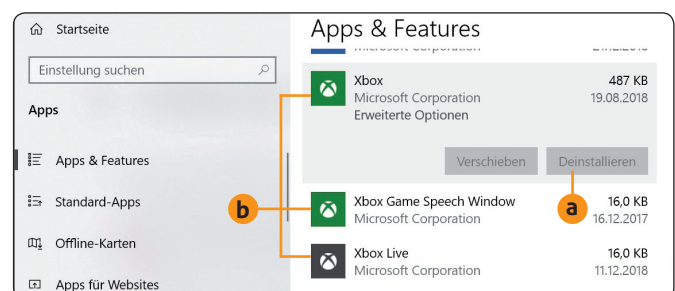
Reinigungsaktion 5: Entfernen Sie die nicht benötigten Apps

Verwenden Sie Windows 7, können Sie gleich mit der Reinigungsaktion 6 fortfahren, denn Windows 7 unterstützt keine Apps. Im Fall von Windows 10 sind Werbeprogramme jedoch häufig als App installiert. Apps sind in der Systemsteuerung unter „Programme und Features“ nicht aufgeführt. Überprüfen Sie daher bei Windows 10 auch die Einstellungen, bevor Sie mit Reinigungsaktion 6 Ihren Browser von Spionageprogrammen und Browser-Entführern befreien.

In Windows 10 deinstallieren Sie Apps über die **Einstellungen**. Ich zeige Ihnen hier am Beispiel der vorinstallierten Xbox-Apps für die Microsoft-Spielekonsole, wie Sie Apps mit wenigen Mausklicks deinstallieren:

1. Öffnen Sie das **Start**-Menü  und klicken Sie auf das **Einstellungen**-Symbol  links.
2. Wählen Sie **Apps** und dann links das Register **Apps & Features**.
3. Die Liste Ihrer Apps ist nach **Name** sortiert. Ändern Sie diese Sortierung per Klick auf den Pfeil in **Installationsdatum**. So finden Sie bei nachfolgenden Kontrollen am schnellsten die heimlich installierten Apps der letzten Wochen.
4. Gehen Sie die Liste der installierten Apps durch, klicken Sie auf die unerwünschten Einträge und wählen Sie

Deinstallieren **a**. Neben zahlreichen von Microsoft heimlich installierten Spielen und Xbox-Apps für diese Spiele **b** finden Sie hier vorinstallierte Apps des PC-Herstellers wie Dropbox und von Geräte-Herstellern wie Apple.



Deinstallieren Sie die 3 Xbox-Einträge, wenn Sie keine Xbox-Spielekonsole besitzen und auch auf Ihrem PC keine PC-Spiele verwenden.

Microsoft installiert heimlich Werbe-Apps und stellt gelöschte Apps wieder her: Stoppen Sie die Werbeflut

Microsoft installiert bei den Windows-10-Updates heimlich Werbe-Apps wie den Netflix-Streaming-Dienst und Xbox-Spiele.



Solche Spiele-Apps können Sie nur mit einem Eingriff in die Registrierungsdatenbank dauerhaft löschen.

Löschen Sie solche Werbe-Apps, sind sie wenige Stunden später wieder da, weil sich Microsoft einfach über Ihre Wünsche hinwegsetzt und die Apps ein weiteres Mal, ohne Sie zu fragen, installiert.

Als sicherheitsbewusster PC-Anwender können Sie die Neuinstallation von Werbe-Apps jedoch über eine Änderung in der Registrierungsdatenbank unterbinden:

1. Öffnen Sie mit **Windows + R** das **Ausführen**-Fenster.
2. Geben Sie **regedit** ein und drücken Sie **Enter**.
3. Bestätigen Sie der Benutzerkontensteuerung das Ausführen des Registrierungseditors mit **OK**. Der Registrierungseditor öffnet sich.
4. Navigieren Sie zum Pfad **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ContentDeliveryManager**.
5. Klicken Sie den Zweig **ContentDeliveryManager** mit der rechten Maustaste an und wählen Sie **Löschen**.
6. Schließen Sie den Registrierungseditor.

7. Führen Sie die 4 Schritte der zu Beginn der Reinigungsaktion 5 stehenden Anleitung auf Seite 5 unten erneut aus und löschen Sie die neu von Microsoft installierten Werbe-Apps ein zweites Mal. Sie werden von Microsoft anschließend nicht mehr neu installiert.



Mein Tipp: Das Löschen des Zweigs **ContentDeliveryManager** führt zum Deaktivieren der Blickpunkt-Funktion von Windows 10. Der Sperrbildschirm zeigt daher keine wechselnden Hintergrundbilder mehr an. Legen Sie Wert auf die Blickpunkt-Funktion, sollten Sie den Zweig **ContentDeliveryManager** daher nicht löschen.

Zusatz-Tipp für Sie als sicherheitsbewusste PC-Anwender: Stören Sie die Kacheln von Apps im **Start**-Menü, klicken Sie mit der rechten Maustaste darauf und wählen auch hier **Deinstallieren**.

Fazit: Mit der hier von mir vorgestellten Registrierungsänderung blockieren Sie diese Werbe-Apps für den Moment. Nicht nur PC- und Geräte-Hersteller wie Apple installieren dreist heimlich Dutzende von Apps auf Ihrem PC, sondern auch Microsoft selbst tut dies bei Windows 10. Wenn Sie die Apps löschen, installiert Microsoft sie sogar einfach wieder neu – und zwar auf allen Desktop-PCs, Notebooks und Tablets mit Windows 10, bei denen Sie sich über das Microsoft-Konto angemeldet haben.

Bleiben Sie aber am Ball und achten Sie in meinen monatlichen Ausgaben des PC-Sicherheits-Beraters auf Windows-10-Hinweise, denn schon morgen kann Microsoft durch ein Update wieder neue Werbe-Schweereien einführen.

Reinigungsaktion 6: Machen Sie die Browser-Erweiterungen unschädlich

Sie haben nun mit den Reinigungsaktionen 3, 4 und 5 bei den laufenden Diensten, den installierten Programmen und den Apps aufgeräumt. Doch womöglich kommen immer noch Werbeeinblendungen oder Sie werden mit dem Browser auf Werbeseiten entführt oder über den Browser ausspioniert. Das liegt an den Browser-Erweiterungen, die wie Dienste, Programme und Apps ebenfalls vorinstalliert oder heimlich installiert werden können. Räumen Sie also auch bei den Erweiterungen gründlich auf.

Die häufigste Form der unerwünschten Browser-Erweiterungen sind Toolbars (Symbolleisten). Die Anbieter werben mit Vorteilen wie sicherer Suche oder schnellem Zugriff auf häufig benötigte Webseiten oder Informationen.

In Wirklichkeit geht es darum, Ihr Verhalten im Internet auszuspiionieren, Ihre Daten zu analysieren und mit der eingeblendeten Werbung Geld zu verdienen. Dazu werden die Startseite und die Suchmaschine geändert.

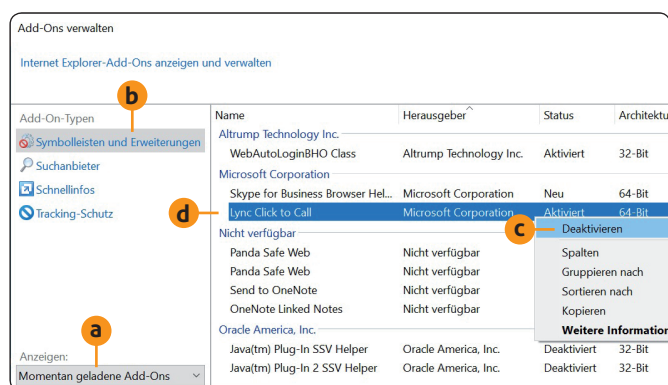
Im Internet bieten vor allem Suchmaschinen und Online-Shops wie Amazon solche Toolbars an, aber auch Antiviren-Programmhersteller wie Avira bieten eigene Toolbars.

Das Problem: Die Toolbars werden überwiegend heimlich oder unbemerkt zusammen mit anderen Programmen installiert. Beachten Sie daher meine 7 Regeln auf Seite 8, um die Toolbar-Installation zu vermeiden.

So entfernen Sie unerwünschte Erweiterungen manuell

Die Toolbars sind häufig manuell nicht oder nur sehr schwer zu entfernen. Sie sollten es aber im ersten Schritt versuchen:

- **Microsoft Edge:** Klicken Sie auf das **Menü-Symbol** [...] und wählen Sie **Erweiterungen**. Klicken Sie auf die unerwünschten Erweiterungen und wählen Sie jeweils **Deinstallieren**.
- **Internet Explorer:** Klicken Sie auf das **Zahnrad-Symbol** und wählen Sie **Add-Ons verwalten**. Ändern Sie die Anzeige von **Momentan geladene Add-Ons** **a** in **Alle Add-Ons**. Gehen Sie die Einträge unter **Symbolleisten und Erweiterungen** **b** durch. Klicken Sie nicht erwünschte Erweiterungen mit der rechten Maustaste an und wählen Sie **Deaktivieren** **c**.



Entfernen Sie aus Datenschutz- und Leistungsgründen die Erweiterung **Lync Click to Call** **d**.

- **Firefox:** Geben Sie ins Adressfeld **about:addons** ein. Überprüfen Sie die Einträge unter **Erweiterungen** und **Plugins**. Nicht erwünschte Erweiterungen entfernen Sie per Klick auf die Schaltfläche **Entfernen**. Unerwünschte Plugins stellen Sie auf **Nie aktivieren**.
- **Google Chrome:** Klicken Sie in das Adressfeld und geben Sie **chrome://extensions** ein. Entfernen Sie nicht erwünschte Erweiterungen mit einem Klick auf **Entfernen**.

Suchen Sie mit dem Tool Malwarebytes AdwCleaner nach Toolbars

Führen Sie nach der manuellen Kontrolle Ihrer Erweiterungen immer noch zusätzlich eine Suche mit Malwarebytes AdwCleaner durch, denn dieses kostenlose Tool findet auch versteckte Toolbars und andere Werbe- und Spionageprogramme:

1. Laden Sie **Malwarebytes AdwCleaner** von der Adresse <https://de.malwarebytes.com/adwcleaner/> herunter.
2. Öffnen Sie mit **(Strg)+[J]** die Download-Liste Ihres Browsers und starten Sie zum Überprüfen Ihres PCs die heruntergeladene Datei **adwcleaner_Version.exe**. Der Programmname ist je nach aktueller Version unterschiedlich. Es ist keine Programminstallation erforderlich. AdwCleaner ist sofort einsatzbereit.
3. Klicken Sie auf **Jetzt scannen** **e** und lassen Sie etwaige Bedrohungen entfernen.
4. Die entfernten Dateien und Registry-Einträge können Sie über das Register **Quarantäne** **f** einsehen.



Die Oberfläche von Malwarebytes AdwCleaner ist in Deutsch und einfach zu bedienen.

Fazit: Sie haben nun mit den Erweiterungen ein weiteres Werbeprogramm-Versteck durchsucht und unerwünschte Werbe- und Spionageprogramme entfernt. Malwarebytes AdwCleaner findet auch hartnäckige Werbeprogramme, denn es durchsucht die Registrierungsdatenbank nach deren Startbefehlen und versteckten Einträgen.

Stellen Sie nach dem Neustart Ihres PCs immer noch verdächtige Aktivitäten fest, ist Ihr PC wahrscheinlich durch ein Schadprogramm infiziert und nicht nur durch ein Werbeprogramm vollgemüllt. Schreiben Sie mir dann über den Computerwissen Club. Meine Mitarbeiter aus der Redaktion oder ich schicken Ihnen gerne eine individuelle Anleitung, wie Sie auch diese gefährlichen Programme loswerden: <https://club.computerwissen.de>.

Impressum

Ihr PC-Sicherheits-Berater, ISSN 2196-9299
Dieses monothematische Supplement
„Ihr Leitfaden für Ihren spionagefreien PC“
gehört zu dem Titel
„Ihr PC-Sicherheits-Berater“.
Computerwissen, ein Verlagsbereich der
VNR Verlag für die Deutsche Wirtschaft AG

Vorstand: Richard Rentrop
Chefredakteur: Michael-Alexander Beisecker
(V.i.S.d.P.), Oberhausen
Herausgeberin: Patricia Sparacio
Adresse: Verlag für die Deutsche Wirtschaft AG,
Theodor-Heuss-Str. 2-4, 53177 Bonn
Telefon: 0228/9550190, Fax: 0228/3696350
Eingetragen: Amtsgericht Bonn HRB 8165

Die Beiträge in „Ihr PC-Sicherheits-Berater“ wurden mit Sorgfalt recherchiert und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Daher ist eine Haftung, auch für telefonische Auskünfte, ausgeschlossen. Vervielfältigungen jeder Art sind nur mit Genehmigung des Verlags gestattet.

© Copyright 2019 by Verlag für die Deutsche Wirtschaft AG;
Bonn, Bukarest, Manchester, Warschau

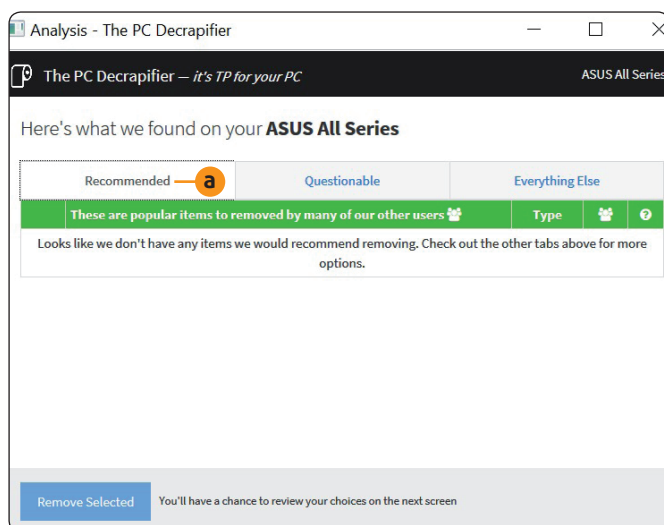


Reinigungsaktion 7: Kontrollieren Sie Ihren PC noch einmal mit dem Gratis-Tool The PC Decrapifier

Sie haben während der Reinigungsaktionen 1 bis 6 wahrscheinlich alle unerwünschten Apps, Dienste, Erweiterungen und Programme unter Kontrolle bekommen und entfernt. Starten Sie jedoch zur Sicherheit noch einmal das Tool The PC Decrapifier. Dieses Tool vergleicht Ihre installierten Programme mit seiner großen Datenbank unerwünschter Programme. Sind noch Programme vorhanden, die Sie entfernen sollten, werden Sie informiert.

Die Installation und Bedienung von The PC Decrapifier (deutsch sinngemäß „Müllentsorger“) ist mit dieser Schritt-für-Schritt-Anleitung ganz einfach. Sie benötigen keinerlei Vorkenntnisse:

1. Laden Sie zuerst die kostenlose Free-Version von **The PC-Decrapifier** am Link <https://www.pcdecrapifier.com/> herunter.
2. Öffnen Sie anschließend mit **(Strg)+(J)** die Download-Liste Ihres Browsers.
3. Starten Sie danach das heruntergeladene Programm **pc-decrapifier-Version.exe**. Dabei ist **Version** ein Platzhalter für die Versionsangabe wie zum Beispiel **3.0.1**. The PC Decrapifier startet sofort ohne Installation.
4. Klicken Sie auf **Analyze** und das Tool untersucht Ihren PC. Die Programme auf Ihrem PC werden in drei Register einsortiert: **Recommended** (Entfernen empfohlen), **Questionable** (fragwürdig, eventuell benötigte Programme) und **Everything Else** (restliche Programme).
5. Sehen Sie sich die Einträge in den drei Registern an und setzen Sie per Mausklick einen Haken vor alle Programme, die Sie entfernen möchten.
6. Klicken Sie auf **Remove Selected** (ausgewählte Programme entfernen) und PC Decrapifier deinstalliert diese Programme.



Finden Sie im Register **Recommended** **a** keine Einträge, haben Sie Ihren PC sauber aufgeräumt.

Ihre 7 Regeln zum Schutz vor neuen Werbe- und Spionageprogrammen

1. Achten Sie auf Download-Seiten von Programmen auf vorgewählte Optionen für unerwünschte Zusatzprogramme. Hier möchten Ihnen die Hersteller unerwünschte Toolbars oder andere Programme unterjubeln. Deaktivieren Sie diese Optionen. Meist muss dazu ein voreingestellter Haken entfernt werden.
2. Falls Sie ein Tool an dem genannten Link nicht finden sollten, installieren Sie es über unsere sichere Service-Webseite: www.pc-sicherheitsberater.de.
3. Überprüfen Sie jedes heruntergeladene Programm vor der Installation mit dem Online-Virens Scanner VirusTotal. Dazu laden Sie das heruntergeladene Installationsprogramm über die Schaltfläche **Wählen Sie eine** zu VirusTotal hoch und klicken auf **Scannen**. Öffnen Sie die Datei nur, wenn die über 70 Sicherheitsprogramme von VirusTotal keine Spionage- oder sonstige gefährliche Funktion melden.
4. Installieren Sie auch keine Programme über Links in E-Mails oder gar E-Mail-Anhänge. Es handelt sich sehr wahrscheinlich um gefährliche Trojaner.
5. Achten Sie während der Installation auf vorausgewählte Optionen für Drittprogramme und deaktivieren Sie sie.
6. Wählen Sie die benutzergeführte Installation statt der Standardinstallation. Optionen für unerwünschte Programme oder Programmteile sind oft nur dort sichtbar.
7. Achten Sie während der Installation darauf, ob das Installationsprogramm zum gewünschten Programm gehört oder vom Download-Anbieter stammt. Brechen Sie eine Installation sofort ab, wenn ein Download-Manager oder der Chip-Installer erscheint. Suchen Sie nach einem sauberen Download ohne solche Zusatzprogramme.

Fazit: Ihr PC ist nun frei von Werbe- und Spionageprogrammen. Sie werden nicht mehr durch Werbebildschirme genervt und durch vorinstallierte Programme ausspioniert. Zudem startet und reagiert Windows schneller. Führen Sie die hier beschriebenen Kontrollen regelmäßig jeden Monat durch, damit Ihr PC sauber bleibt. Sind Sie dabei unsicher, welche Apps, Dienste, Erweiterungen oder Programme Sie entfernen und welche Sie behalten sollen, berate ich Sie gerne über den Computerwissen Club: <https://club.computerwissen.de>.