Ihr PC-Sicherheits-Berater

So schützen Sie Ihre Privatsphäre und sensiblen Daten

2 Wer schaut Ihnen alles beim Surfen zu?
Beim Surfen im Internet sind Sie gläsern wie in einem Haus aus Glaswänden. Nur im Privatmodus surfen Sie sicher.

3 Verrät Ihr Browser Ihren Standort?
Aktuelle Browser übermitteln bei jedem Aufruf einer Webseite Ihren Standort. Stoppen Sie die Überwachung sofort.

5 Werden Sie im Internet ständig überwacht?
Ihr Internet-Anbieter protokolliert genau, wann Sie online sind. Ich verrate Ihnen, wie Sie trotzdem anonym surfen!

7 Ihr sicherer Download vom Verlagsserver
TOR-Browser-Software, vom Chefredakteur für Sie geprüft und garantiert virenfrei. Plus: 7 goldene Sicherheits-Tipps.

Schützen Sie Ihre Privatsphäre: Mit meinen 4 brandneuen Schutzmaßnahmen surfen Sie wirklich anonym!

Warum die ePrivacy-Verordnung Sie nicht schützt

Im Internet werden Sie auf Schritt und Tritt von Datenjägern verfolgt. Die **D**aten**s**chutz**g**rund**ver**o**r**dnung (DSGVO) schützt Sie nur unzureichend.

Denn es fehlt noch die Verordnung zum Schutz Ihrer Privatsphäre im Internet (ePrivacy-Verordnung), die 2018 mit der DSGVO in Kraft treten sollte.

Doch die Verordnung wurde aufs Jahr 2020 verschoben. Firmen protestierten dagegen, denn weniger Daten bedeuten auch weniger Geschäft.

Meine Empfehlung: Warten Sie nicht auf die ePrivacy-Verordnung. Schützen Sie sich noch heute selbst: Schalten Sie die Datenübermittlung einfach ab und löschen Sie Ihre Internet-Spuren regelmäßig.

Viele Grüße, Ihr

Michael-Alexander Beisecker, Deutschlands PC-Sicherheitsexperte Nr. 1

Kostenlose Experten-Hilfe:
Exklusiv für Sie als Abonnenten: Die Sofortauskunft mit zuverlässigen Antworten und professionellen Tipps direkt von der Redaktion.
Redaktions-Hotline: **Mittwoch zwischen 15:00 und 18:00 Uhr, Tel.: 02 08/69 07 977**

Schützen Sie Ihre Privatsphäre im Internet schnell und kostenlos

Wie Sie im Internet anonym surfen und sich nicht ausspionieren lassen

Vier von fünf Deutschen sind um den Schutz ihrer Daten im Internet besorgt. Das geht aus der neuesten Studie „Norton Cyber Security Insights Reports" (Einblicke in die Internet-Sicherheit der Firma Norton) hervor. Diese Sorge ist begründet, denn die meisten Deutschen gehen mit ihren Daten nicht sicher genug um. Dabei sind zum Schutz Ihrer Daten nur vier einfache Schutzmaßnahmen erforderlich, die Ihnen als sicherheitsbewusstem PC-Anwender sicher leichtfallen werden.

Ich höre oft, dass es gar kein anonymes Surfen im Internet geben würde. „Wer will, bekommt meine Daten", ist das Argument. Und tatsächlich können Geheimdienste, Polizei und Staatsanwälte über Ihren Internet-Anbieter erfahren, wann Sie mit welcher IP-Adresse (IP = **I**nternet-**P**rotokoll) im Internet gesurft haben.

Stellen Sie sich vor, Gestapo oder Stasi hätten über eine solche Technologie verfügt! Zum Glück haben wir heutzutage eine rechtsstaatliche Demokratie. Doch die schützt uns nicht vor dem Missbrauch der Informationstechnologie. Nehmen Sie daher Ihr Grundrecht auf Privatsphäre selbst in die Hand. Surfen Sie ab sofort mit meiner Hilfe anonym im Internet.

Anonym surfen: 4 einfach anzuwendende Schutzmaßnahmen reichen

Schutzmaßnahme 1: Verwenden Sie immer den Privatmodus Ihres Browsers
Damit löschen Sie nach jedem Surfen Ihre Internet-Spuren, sodass niemand ein Nutzerprofil über Sie erstellen kann (siehe Seite 2).

Schutzmaßnahme 2: Schalten Sie die Standortübermittlung aus
Schützen Sie sich vor Betrugsattacken und verraten Sie im Internet niemandem Ihren aktuellen Aufenthaltsort (siehe ab Seite 3).

Schutzmaßnahme 3: Ändern Sie ständig Ihre Internet-Adresse
Vertuschen Sie Ihre wahre Identität: So entkommen Sie Ihren Verfolgern im Internet und surfen anonym (siehe ab Seite 5).

Schutzmaßnahme 4: Entfernen Sie alle Ihre Internet-Spuren auch unter Windows
Löschen Sie auf Ihrer Festplatte verräterische Spuren aus Windows: So bewahren Sie Ihre Privatsphäre (siehe Seite 8).

Wenn Sie diese 4 Schutzmaßnahmen durchführen, kann nur jemand an Ihre Daten gelangen, der Ihren PC mit einem Schadprogramm hackt. Doch auch davor schütze ich Sie: Befolgen Sie zeitnah meine Sicherheitsempfehlungen in den aktuellen Ausgaben.

>>> Lesen Sie bitte weiter auf Seite 2

Schutzmaßnahme 1: Verwenden Sie immer den Privatmodus Ihres Browsers

Löschen Sie nach jedem Surfen Ihre Internet-Spuren, damit niemand ein Nutzerprofil über Sie erstellen kann

Bei jedem Internet-Besuch speichert Ihr Browser ein Protokoll aller Ihrer Aktivitäten im Internet auf Ihrer Festplatte. Diese „Internet-Spuren" zeigen auf die Sekunde genau, wo Sie überall waren und von welcher Internetseite Sie wohin gesurft sind. Noch verräterischer sind die Inhalte der besuchten Internetseiten. Schließlich suchen Sie danach, was Sie interessiert und gerade besonders bewegt. Lassen Sie niemanden auf diese Weise Ihre Gedanken lesen. Ich zeige Ihnen, wie Ihre Wünsche und Sorgen Ihre Privatsache bleiben.

Ihr Browser legt bei jedem Internet-Besuch mehrere Listen mit den besuchten Internetseiten, heruntergeladenen Dateien und den eingegebenen Formulardaten an. Sie werden je nach Browser als „Chronik" oder „History" bezeichnet.

Internetseiten-Betreiber speichern Daten über Sie in Cookies und Super-Cookies

Hinzu kommen Informationen von den Betreibern der von Ihnen besuchten Internetseiten. In kleinen Textdateien, den „Cookies" (wörtlich „Kekse") oder auch „Super-Cookies", werden täglich immer mehr Daten über Sie gesammelt.

Im Privatmodus löscht Ihr Browser nach jeder Internet-Sitzung alle über Sie gespeicherten Daten

Damit Ihre Internet-Aktivitäten nicht nachzuverfolgen sind, löscht Ihr Browser am Ende Ihrer Internet-Sitzung im Privatmodus alle gespeicherten Daten.

Die Funktion des Privatmodus lässt sich am einfachsten mit dem Werbeslogan für Las Vegas umschreiben: „Was hier passiert, bleibt hier!" Das scherzhaft als Sündenbabel (englisch „Sin City") bezeichnete Las Vegas will damit ausdrücken, dass nichts nach außen dringt, was Sie dort getan haben.

Gar nichts deutet also mehr auf Ihre Internet-Aktivitäten hin. Selbst die für den Betrieb des Browsers erforderlichen Dateien im Pufferspeicher (Browser-Cache) werden gelöscht.

Keine Sorge, diese Pufferdaten werden von Ihrem Browser einfach wieder neu angelegt. Das Löschen ist also völlig ungefährlich, behebt Browser-Fehler und verbessert Ihre Sicherheit.

Warnung: Super-Cookies werden im Privatmodus nicht zuverlässig gelöscht. Daher ist **Schutzmaßnahme 4** zusätzlich zum Privatmodus erforderlich (siehe Seite 8). Der Privatmodus ändert auch nicht Ihre IP-Adresse, sodass Sie bei besonders sensiblen Daten zusätzlich vollständig anonym surfen sollten (**Schutzmaßnahme 3**, Seite 5).

So rufen Sie den Privatmodus bei Ihrem Browser auf

Der Aufruf des Privatmodus ist bei Ihrem Browser ganz einfach:

Firefox: Der Privatmodus wird bei Firefox als „privates Fenster" bezeichnet. Sie rufen den Privatmodus über das **Menü öffnen**-Symbol ≡ und **Neues privates Fenster** auf.

Firefox zeigt Ihnen eine Kurzeinführung zum privaten Fenster an und blendet das **Maske**-Symbol a in der rechten, oberen Ecke jedes privaten Fensters an.

*Sehen Sie das **Masken**-Symbol bei Firefox, sind Sie in diesem Fenster vor Datenräubern geschützt.*

Mein Tipp: Firefox blockiert ganz automatisch alle Elemente zur Aktivitätenverfolgung. Wünschen Sie die Aktivitätenverfolgung bei einer Internetseite nicht, klicken Sie auf das **Wappen**-Symbol links vor der Internet-Adresse und auf **Blockieren temporär deaktivieren**.

Google Chrome: Der Privatmodus wird bei Chrome als „Inkognito-Fenster" bezeichnet. Sie rufen den Privatmodus über das **Menü**-Symbol ⋮ und **Neues Inkognito-Fenster** auf. Noch schneller geht's, wenn Sie die Tastenkombination Strg+⇧+N drücken.

*Das Wort **Inkognito** und das **Agenten**-Symbol b im Browser Google Chrome weisen Sie beim Surfen auf den Privatmodus hin.*

Microsoft Edge: Der Privatmodus heißt bei Microsoft Edge „InPrivate-Fenster". Klicken Sie auf **Einstellungen und mehr** ··· und wählen Sie **Neues InPrivate-Fenster**. Noch schneller geht's, wenn Sie die Tastenkombination Strg+⇧+P drücken.

Microsoft Edge zeigt Ihnen zu Beginn des Privatmodus diese Information an c, es fehlt aber ein Symbol wie bei Chrome und Firefox.

Warnung: Verwenden Sie den Sprachassistenten Cortana zum Aufruf von Microsoft Edge, wird der Browser nicht im Privatmodus aufgerufen. Alle Ihre Fragen an Cortana werden außerdem immer an die Microsoft-Server übertragen und dort ausgewertet.

Damit stehen Ihre Daten nicht nur Microsoft, sondern auch den amerikanischen Geheimdiensten und in Amtshilfe den deutschen und britischen Geheimdiensten zur Verfügung. Möchten Sie privat surfen, sollten Sie daher konsequent auf einen Sprachassistenten verzichten. Das gilt auch für Alexa von Amazon, Google Assistent und Siri von Apple.

Fazit: Da Sie nun im Privatmodus surfen, werden Ihre verräterischen Internet-Spuren automatisch nach jeder Sitzung gelöscht und Ihre Privatsphäre wird dadurch gut geschützt. Doch Sie können diesen Schutz mit den nächsten Maßnahmen noch perfektionieren.

Schutzmaßnahme 2: Schalten Sie die Standortübermittlung aus

Ihr Schutz vor Betrugsattacken: Verraten Sie im Internet niemandem Ihren aktuellen Aufenthaltsort

Seit Mobiltelefone als intelligent („Smartphones") bezeichnet werden und immer mehr PC-Aufgaben übernehmen, sind sie auch die bevorzugten Spionagewerkzeuge der Geheimdienste in aller Welt. Ein wesentlicher Aspekt dabei ist die Standortübermittlung, die auch im Browser Ihres Desktop-PCs, Notebooks und Tablet-PCs voreingestellt aktiviert ist. Geheimdienste, aber auch Kriminelle und Werbefirmen finden so leicht heraus, von wo aus Sie eine Internetseite aufrufen. Im Unterschied zum Gebrauch von Smartphones können Sie die Standortübermittlung aber bei Ihrem Desktop-PC sicher abschalten und die Genauigkeit beeinflussen.

Verwenden Sie ein Funknetz (WLAN) für die Internet-Verbindung, ist Ihr Standort bis auf 7 Meter genau zu ermitteln. Hat Ihr Rechner ein GPS-Modul (**G**lobal **P**ositioning **S**ystem, oft bei hochwertigen Notebooks anzutreffen und bei Tablet-PCs Quasi-Standard), funktioniert die Standorterkennung bis auf 2 Meter genau.

Wie Sie das genaue Anpeilen Ihres Rechners verhindern

Dagegen ist Ihr Standort nur sehr ungenau zu bestimmen, wenn Sie Ihren PC per Kabel an Ihren Router anschließen. Das ist also ein Trick, um Datenspione auszutricksen. Außerdem ist die Internet-Verbindung per Kabel im Allgemeinen deutlich schneller und störungsfreier als per WLAN.

LESERSERVICE

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

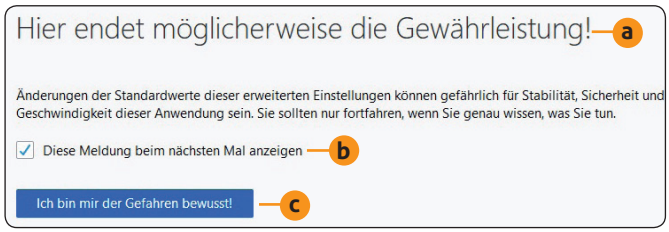
Melden Sie sich dazu einfach kostenlos unter **https://club.computerwissen.de** an und stellen Sie ihm dort Ihre Fragen. **Michael-Alexander Beisecker** und seine Redaktionsmitarbeiter helfen Ihnen gern weiter. Sie erhalten werktags innerhalb von 48 Stunden eine Antwort auf Ihre Frage – garantiert.

So schalten Sie die Standortübertragung in Ihrem Browser ganz aus

Wesentlich besser, als den Ort nur zu verschleiern, ist jedoch, wenn Sie die Standortübermittlung ganz deaktivieren. So geht's:

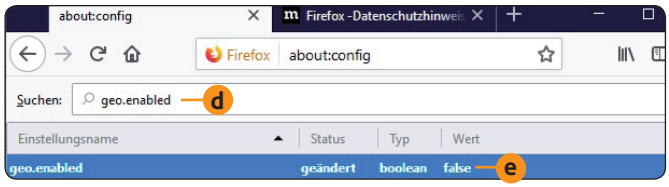
Firefox: Das standortbezogene Surfen, wie es Mozilla bezeichnet, ist bei Firefox voreingestellt aktiviert, lässt sich jedoch über die Konfigurationsvariablen ganz einfach abschalten:

1. Geben Sie ins Adressfenster von Firefox **about:config** ein und bestätigen Sie die Warnung a, dass Sie vorsichtig sein werden. Dazu entfernen Sie den Haken von der Option **Diese Meldung beim nächsten Mal anzeigen** b und klicken auf **Ich bin mir der Gefahren bewusst!** c.



Lassen Sie sich von dieser Warnung nicht abschrecken: Durch das Abschalten der Standortübermittlung besteht keine Gefahr.

2. Schreiben Sie als Suchbegriff **geo.enabled** d ins Feld **Suchen**, damit Ihnen der Einstellungsname **geo.enabled** angezeigt wird. Durch einen Doppelklick auf **geo.enabled** ändern Sie dessen Wert von **true** (wahr) in **false** e (falsch). Die Standortübermittlung ist nun deaktiviert.



Die Standortübermittlung schalten Sie bei Firefox mit einem Doppelklick auf diese Einstellung ab.

3. Schließen Sie das Fenster mit einem Klick auf die **Schließen**-Schaltfläche **X** rechts oben.

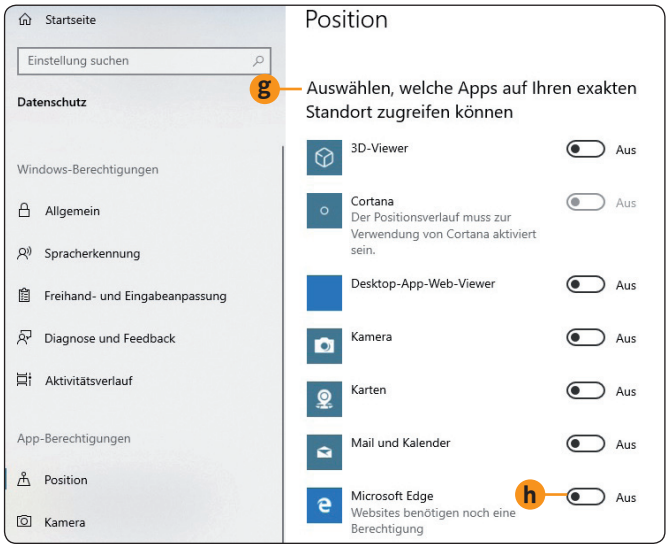
Google Chrome: Im Chrome-Browser gibt es eine Einstellung für die Ortsübermittlung, mit der Sie die Datenübertragung stoppen:

1. Klicken Sie das **Menü**-Symbol ⋮ an und wählen Sie **Einstellungen**.
2. Blättern Sie zum Ende der **Einstellungen** und klicken Sie auf **Erweitert**.
3. Klicken Sie im Abschnitt **Datenschutz und Sicherheit** auf **Website-Einstellungen** und dann auf **Ort**.
4. Klicken Sie auf den Schalter hinter **Vor dem Zugriff nachfragen (empfohlen)** f, sodass sich die Einstellung in **Blockiert** ändert. Schließen Sie die **Einstellungen** mit einem Klick auf das **Schließen**-Symbol **X** rechts oben.

*Beachten Sie, dass sich die Bezeichnung dieses Schalters in **Blockiert** ändert, sobald Sie darauf klicken.*

Microsoft Edge: Beim Edge-Browser unterdrücken Sie die Ortsübermittlung mithilfe der Datenschutz-Einstellungen von Windows 10:

1. Öffnen Sie das **Start**-Menü von Windows 10 und **Einstellungen**.
2. Wählen Sie **Datenschutz** und **Position**.
3. Suchen Sie unter **Auswählen, welche Apps auf Ihren exakten Standort zugreifen können** g den Eintrag für **Microsoft Edge** und ziehen den Schalter nach links auf die Position **Aus** h. Noch schneller geht's, wenn Sie den Schalter zum Umstellen einfach anklicken.



Hier schalten Sie die Standortübertragung für Microsoft Edge aus.

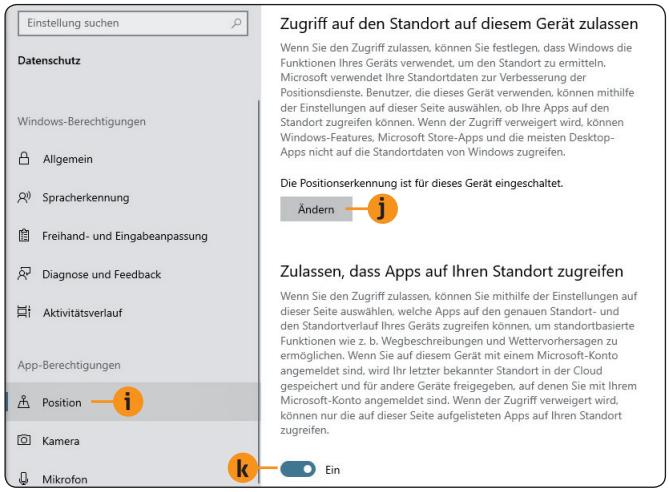
4. Blenden Sie das Edge-Fenster per Klick auf die **Schließen**-Schaltfläche **X** rechts oben aus.

Mein Tipp: Verwenden Sie noch den Browser Internet Explorer, empfehle ich Ihnen aus Sicherheits- und Datenschutzgründen den Wechsel zu Chrome (https://www.google.com/intl/de_de/chrome/) oder Firefox (https://www.mozilla.org/de/firefox/new/).

Was Sie zur Standortübermittlung bei Windows 10 beachten sollten

Im Gegensatz zu Windows 7 ist Windows 10 nicht nur für den Desktop-PC, sondern auch für mobile Geräte wie Tablet-PCs und Smartphones mit Apps entwickelt worden.

Es gibt somit, wie bei Mobilgeräten üblich, eine Vielzahl von Einstellungen zur Positionserkennung, die Sie über **Einstellungen**, **Datenschutz** und **Position** i vornehmen. Die **Positionserkennung** ist bei Windows 10 voreingestellt eingeschaltet, Sie können diese über **Ändern** j auf **Aus** stellen.



*Möchten Sie die Standortübermittlung bei allen Apps und nicht nur bei Edge blockieren, stellen Sie den Schalter k auf **Aus**.*

Mein Tipp: Benötigen Sie die Standortübermittlung für eine Windows-Anwendung, lassen Sie diese aktiviert und bestimmen unter **Auswählen, welche Apps auf Ihren exakten Standort zugreifen können** für jede einzelne Anwendung, ob sie auf Ihre aktuelle Position zugreifen darf oder nicht.

Warum die Standortübermittlung bei Windows 10 so gefährlich für Sie ist

Ist die Standortübermittlung bei Windows 10 eingeschaltet, spielen Sie mit dem Feuer. Nicht nur Ihr Browser greift auf den Standort zu und verrät ihn Interessenten weiter, sondern eine Vielzahl an Apps berichtet ihn ihren Entwicklern. Neben dem Browser Microsoft Edge sind das zum Beispiel die Sprachassistentin Cortana, Mail und Kalender sowie Windows-Karten.

Windows 10 kann Sie überwachen, als wären Sie ein Verbrecher mit elektronischer Fußfessel

Neben der Standortübermittlung gibt es bei Windows 10 mit **Geofence** noch eine Funktion, die bislang im privaten Einsatz vor allem durch die Überwachung von Tieren, Kindern und orientierungslosen Menschen bekannt geworden ist.

Datenschützer kritisieren die Anwendung bei Menschen, da die gefängnisartige Überwachung per Geofence weder die Grundsätze des Datenschutzes noch die der Menschenwürde erfüllt.

Eine App kann bei Windows 10 eine Nachricht übermitteln, wenn Sie einen bestimmten Bereich verlassen oder betreten.

Hacker können über Windows 10 so erfahren, wann Sie nicht zu Hause sind, um bei Ihnen einzubrechen. Oder Geschäftsleute überschütten Sie mit Werbung, wenn Sie mit Ihrem Notebook in deren Nähe gemütlich in einem Café sitzen.

Hier erfahren Sie, ob Sie durch Apps und Geofence ausspioniert werden

Überprüfen Sie daher, ob auf Ihrem Windows-10-PC Apps installiert sind, die Sie per Geofence überwachen. Dazu wählen Sie **Einstellungen**, **Datenschutz** und **Position**. Blättern Sie nach unten bis **Geofence** und lesen Sie den Text darunter. Steht hier, dass wenigstens eine App Geofence verwendet, werden Sie darüber überwacht.

Schalten Sie die Positionsüberwachung wie unter **Was Sie zur Standortübermittlung bei Windows 10 beachten sollten** ab Seite 4 unten beschrieben aus, dann ist auch die Geofence-Überwachung deaktiviert.

Schutzmaßnahme 3: Ändern Sie ständig Ihre Internet-Adresse

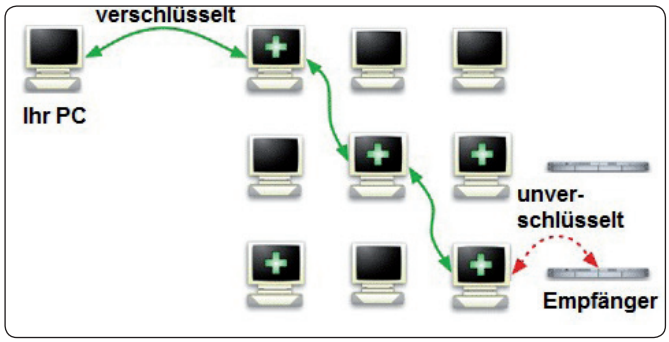
Vertuschen Sie Ihre wahre Identität: So entkommen Sie Ihren Verfolgern im Internet und surfen anonym

Ihr Internet-Anbieter weist Ihnen für Ihren Internet-Zugang eine eindeutige IP-Adresse zu und protokolliert genau, wann Sie damit online gegangen sind. Die IP-Adresse ist also wie die Nummer Ihres Personalausweises ein fälschungssicheres Erkennungszeichen. Sie lässt Ihnen damit im Internet keinerlei Privatsphäre mehr, denn Ihr Browser übermittelt diese Adresse ungefragt sofort an jede aufgerufene Internetseite. Sie können diesen Verrat Ihres Browsers nicht abschalten. Aber ich zeige Ihnen, wie Sie Ihre IP-Adresse ändern, damit niemand außer Ihrem Internet-Provider und Ihnen Ihre wahre Identität kennt.

Sie können die IP-Adresse nicht selbst ändern, sondern benötigen dazu einen Dienstleister mit einem oder mehreren Servern. Solche Dienste werden überwiegend kostenpflichtig angeboten und Sie begeben sich in die Abhängigkeit eines Unternehmens, das Ihr Vertrauen womöglich missbraucht.

Das Tor-Netz: Schutz Ihrer Daten und Ihrer Privatsphäre durch Verschlüsselung

Diese Gefahr besteht beim kostenlos angebotenen Tor-Netzwerk nicht. Die Server werden von Freiwilligen bereitgestellt. Die Datenübertragung zum ersten Server und innerhalb des Netzwerks erfolgt verschlüsselt.



Ihre Daten durchlaufen bei Tor verschlüsselt mehrere Server im Internet, bevor sie dann unverschlüsselt dem Empfänger übergeben werden.

Während Ihre Daten durch das Tor-Netzwerk gereicht werden, ändert sich mit jedem Server die übertragene IP-Adresse. Der Empfänger erhält nur die letzte IP-Adresse des Tor-Netzwerks und nicht Ihre wirkliche Adresse.

Das ist sehr sicher, solange Sie nicht auf einen der gefälschten Tor-Server oder ein gefälschtes Tor-Programm im Internet hereinfallen. Doch keine Sorge, ich schütze Sie vor diesen Gefahren mit meiner sicheren Service-Webseite. Laden Sie Tor von dort herunter, gehen Sie kein Risiko ein.

Schritt für Schritt zu Ihrem Firefox-Browser mit Tor

Für das anonyme Surfen verwenden Sie den Tor-Browser. Das ist ein speziell für das Tor-Netzwerk angepasster Firefox-Browser:

1. Laden Sie zuerst das Installationsprogramm für den aktuellen Tor-Browser über den Link https://www.torproject.org/de/download/ herunter. Sie erhalten damit die Version mit der deutschen Oberfläche.
2. Öffnen Sie per Tastenkombination Strg+J die Download-Liste Ihres Browsers. Starten Sie das heruntergeladene Programm **torbrowser-install-8.5.4_de.exe**. Die Versionsnummer **8.5.4** im Namen kann sich bei einer aktuelleren Version ändern. Im Fall der 64-Bit-Version steht im Namen zusätzlich **win64**.
3. Wählen Sie das Installationsverzeichnis oder bestätigen Sie das Standardverzeichnis mit **Installieren**.
4. Auf der nächsten Seite behalten Sie die Haken bei den Optionen **Tor Browser ausführen** und **Add Start Menu & Desktop shortcuts** (Start-Menü-Eintrag und Desktop-Verknüpfungen) bei. Das erleichtert Ihnen den Aufruf des Browsers.
5. Zum Abschluss der Installation klicken Sie auf **Fertigstellen**.

Voreingestellt installiert sich Tor auf Ihrem Desktop. Sie finden dort den Ordner **Tor Browser** und darin das Programm **Start Tor Browser** zum Aufruf des anonymen Internet-Zugangs. Während der Installation wird auch automatisch eine Verknüpfung zum **Start**-Menü von Windows eingerichtet.

So bedienen Sie den Tor-Browser

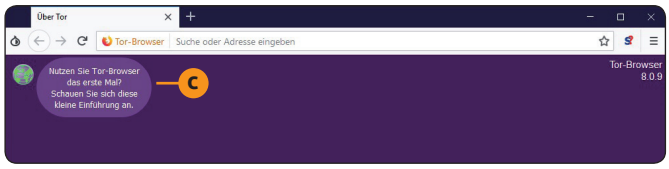
Starten Sie nun den Tor-Browser und nehmen Sie die Ersteinrichtung vor:

1. Rufen Sie den Tor-Browser über das **Weltkugel**-Symbol auf dem Desktop oder in der Taskleiste auf.
2. Beim ersten Aufruf von Tor werden Sie gefragt, ob Ihre Internet-Verbindung direkt oder über eine Vermittlung (Bridge, Proxy-Server) erfolgt. Wählen Sie als privater Anwender in Europa hier **Verbinden** a.

*Die zweite Auswahl **Konfigurieren** b benötigen Sie nur im außereuropäischen Ausland, wenn Sie einen Firmenrechner verwenden oder selbst einen Proxy-Server eingerichtet haben.*

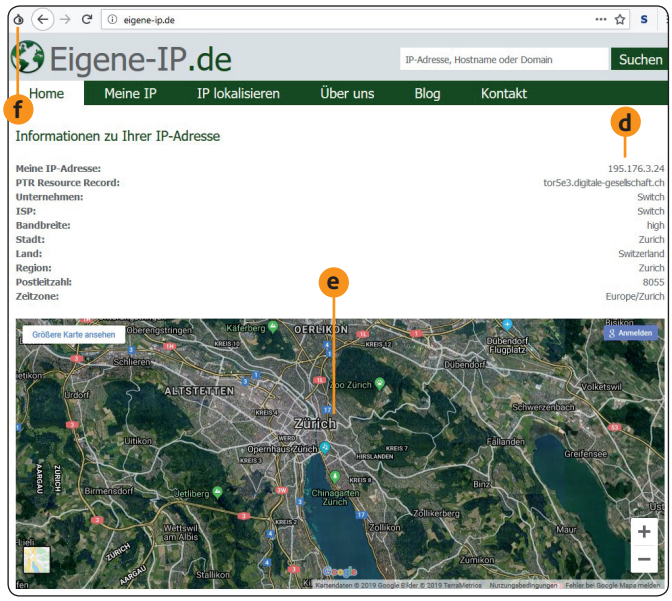
3. Tor zeigt nun, wie bei jedem nachfolgenden Aufruf auch, kurz ein Fenster mit einem Laufbalken an, während die Verbindung zum Tor-Netzwerk hergestellt wird.
4. Es erscheint die Startseite des Tor-Browsers. Das ist die anonyme Suchmaschine DuckDuckGo. Verwenden Sie zur Internet-Suche nur diese Suchmaschine oder die Suchmaschine Startpage, damit Google keine Daten von Ihnen erhält. Startpage können Sie über den Link https://www.startpage.com/de/ aufrufen.

Mein Tipp: Auf der Startseite werden Ihnen sowohl eine kurze Tor-Einführung c als auch unterhalb des Eingabefeldes das Browser-Handbuch angeboten.



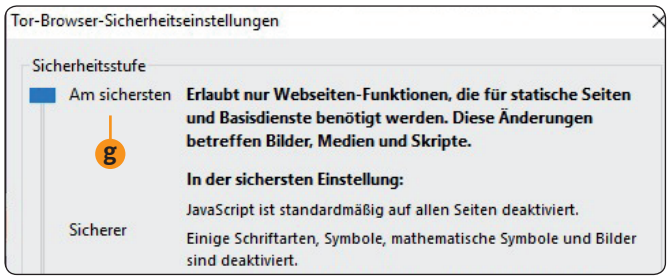
Tor startet mit der anonymen Suchmaschine DuckDuckGo.

5. Rufen Sie die Webseite **eigene-ip.de** mit dem Tor-Browser auf. Sie sehen Ihre neue IP-Adresse (d) und Ihr „neuer Wohnort" wird Ihnen in einer Google-Maps-Karte angezeigt (e).



Wie Sie auf der Karte sehen, befinden Sie sich für den Betreiber der besuchten Webseite in Zürich (e).

6. Der Tor-Browser ist auf geringe Sicherheit eingestellt, damit Sie beim Aufruf von Webseiten keine großen Einschränkungen haben. Höhere Sicherheit erhalten Sie über das **Zwiebel**-Symbol (f) und **Sicherheitseinstellungen**. Ziehen Sie den Schieber auf **Sicherer** oder **Am sichersten** (g) und klicken Sie auf **OK**.



Ziehen Sie den Schieberegler nach oben auf eine sicherere Einstellung.

Mein Tipp: Wägen Sie gut zwischen Sicherheit und Funktionalität ab. Je höher Sie in Schritt 6 die Sicherheit einstellen, umso weniger Webseiten-Funktionen stehen Ihnen zur Verfügung. In der höchsten Sicherheitsstufe werden JavaScript und HTML5-Videos unterdrückt.

Es gibt ansonsten von der Bedienung her keine Unterschiede zwischen Ihrem vertrauten Firefox-Browser und dem Tor-Browser. Sie brauchen sich also nicht umzustellen.

Schnellübersicht: 7 goldene Sicherheits-Tipps, damit Ihre Internet-Verbindung geschützt bleibt

Tor verändert Ihre IP-Adresse nach außen. Doch damit Ihre Tarnung nicht auffliegt und Ihre Privatsphäre dauerhaft umfassend geschützt ist, sollten Sie meine 7 Sicherheits-Tipps beachten:

1. Nutzen Sie für Tor nur den hier vorgestellten Tor-Browser.
2. Öffnen Sie neben Tor keinen weiteren Browser, er würde parallel Ihre echte IP-Adresse verraten.
3. Installieren Sie keine zusätzlichen Browser-Erweiterungen im Tor-Browser.
4. Überprüfen Sie bei jeder Internetseite, ob diese als **https:**//www.webseite.de statt **http:**//www.webseite.de geöffnet wird, und geben Sie nötigenfalls nur auf **https**-Seiten Ihre Daten ein.
5. Öffnen Sie keine heruntergeladenen Dokumente, während Sie mit Tor online sind. Tor warnt insbesondere vor DOC- und PDF-Dateien, da die damit verknüpften Anwendungen Ihre echte IP-Adresse weitergeben könnten.
6. Empfehlen Sie Tor weiter, damit eine möglichst große Anzahl Ihrer Bekannten ebenfalls anonym surft und Sie ähnlich wie ein Fisch in einem Fischschwarm in der Gruppe weniger auffällig für Geheimdienste und Hacker sind.
7. Öffnen Sie nur bekannte Dateien aus sicheren Quellen, damit Sie trotz Tor nicht durch einen Trojaner ausspioniert werden.

Impressum

Ihr PC-Sicherheits-Berater, ISSN 2196-9299

Dieses monothematische Supplement „Ihr Leitfaden zum anonymen Surfen im Internet" 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

Schutzmaßnahme 4: Entfernen Sie alle Ihre Internet-Spuren auch unter Windows

Löschen Sie auf Ihrer Festplatte verräterische Spuren aus Windows: So bewahren Sie Ihre Privatsphäre!

Windows liefert Ihnen kein Tool zum Schutz Ihrer Privatsphäre mit, daher empfehle ich Ihnen die kostenlose Version des Reinigungs-Tools Wipe. Das einfach zu bedienende Tool mit deutscher Oberfläche bietet denselben Funktionsumfang wie das bekannte Tool CCleaner, das ich Ihnen aus Sicherheitsgründen nicht mehr empfehle.

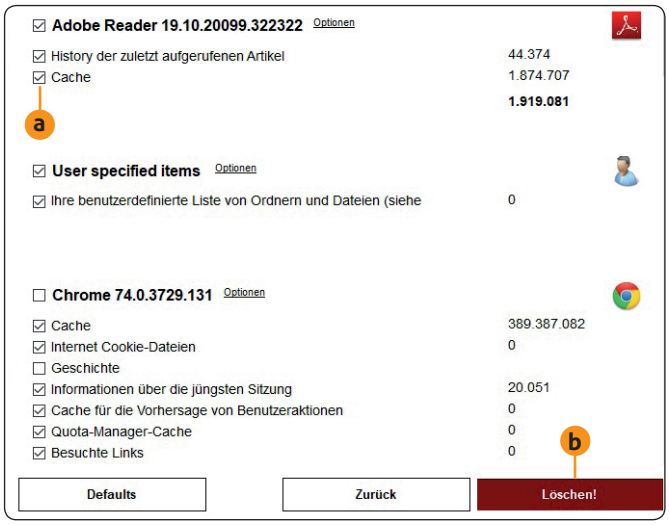
Installieren Sie Wipe mit der deutschen Oberfläche

1. Wipe steht Ihnen am Link (https://privacyroot.com/software/setups/setup_wipe.exe) zur Verfügung. Das Herunterladen des Installationsprogramms **setup_wipe.exe** startet automatisch. Bestätigen Sie das Herunterladen per Klick auf **Datei speichern**.
2. Öffnen Sie die Download-Liste Ihres Browsers mit der Tastenkombination Strg+J und starten Sie das Programm **setup_wipe.exe**.
3. Folgen Sie dem Installationsassistenten mit **Nächster Schritt**. Es werden Ihnen weitere Tools angeboten, die ich Ihnen jedoch nicht empfehle. Setzen Sie daher keinen weiteren Haken außer bei **Wipe** und klicken Sie auf **Nächster Schritt**.
4. Sie werden nach Ihrer E-Mail-Adresse gefragt, die Sie aus Datenschutzgründen jedoch nicht eingeben sollten. Klicken Sie auf **Nächster Schritt** und **Fenster schließen**.

Entfernen Sie die Internet-Spuren von Ihrem PC

Zum Schutz Ihrer Privatsphäre lassen Sie nun Wipe bei Ihren Browsern, bei Ihren installierten Anwendungen und bei Windows selbst nach verräterischen Internet-Spuren suchen. Das können zum Beispiel Einträge in Cache-Speichern (Pufferspeichern), gelöschte Dateien im Papierkorb oder Listen von Ihnen geöffneter Dateien sein:

1. Rufen Sie **Wipe** über das **Start**-Menü auf oder geben Sie **wipe** ins Suchfeld der Taskleiste ein und doppelklicken Sie **Wipe** dann in der Suchliste an.
2. Warten Sie nun, bis Wipe automatisch alle Ihre installierten Anwendungen erkannt hat und das Hauptmenü eingeblendet wird.
3. Klicken Sie auf **Einzelheiten**.
4. Blättern Sie durch die angezeigte Programm- und Dateiliste. Wählen Sie bei den angezeigten Anwendungen wie Adobe Reader, Chrome, Firefox und Microsoft Reader, welche Internet-Spuren gelöscht werden sollen. Setzen Sie einen Haken a oder entfernen Sie bei vorausgewählten Daten den Haken, wenn Sie diese nicht löschen möchten.
5. Überprüfen Sie Ihre Auswahl noch einmal und klicken Sie auf **Löschen!** b.



Schützen Sie Ihre Privatsphäre mit Wipe, indem Sie die Internet-Spuren Ihrer installierten Programme löschen lassen.

Ihre Vorteile: Sie haben mit Wipe gezielt die Internet-Spuren entfernt, die Ihre Privatsphäre beeinträchtigen. Das Löschen erfolgt sicher, sodass auch ein Hacker oder ein Schadprogramm Ihre Surfspuren nicht wieder hervorholt.

Durch die drei vorherigen Maßnahmen geben Sie beim Surfen außerdem nur so viele Informationen preis, wie gerade unbedingt erforderlich sind. Unterstützen Sie diese Einstellungen, indem Sie mit Ihren Daten im Internet sehr sparsam umgehen und nur dann etwas in Formulare eintragen, wenn die Internetseite über jeden Zweifel erhaben und die Dateneingabe unbedingt erforderlich ist.

3 goldene Regeln für anonymes Surfen

1. Rufen Sie Webseiten immer mit verschlüsselter Verbindung (**https**) auf.
2. Fügen Sie zum Tor-Browser keine neuen Erweiterungen hinzu.
3. Verwenden Sie für Ihre Suche im Internet statt der Suchmaschine Bing oder Google die anonymen Suchmaschinen DuckDuckGo oder StartPage.