Verfolgt im Netz

Tracking Wer im Internet surft, wird von Firmen überwacht – oft ohne es zu merken. Die Methode heißt Tracking. Wie sie funktioniert und welche Risiken sie birgt.

Was gibt es Neues vom FC Bayern München? Stellt sich der Fußballfan diese Frage, kann er im Internet nach Antworten suchen, zum Beispiel auf dem Portal des Fernsehsenders Sport1. Während er die Seite liest, liest die Seite ihn: Bis zu 73 „Tracker“ haben wir auf Sport1.de gefunden. Sie saugen fleißig Informationen über den Besucher ab. Das kann seine Verweildauer sein, das Betriebssystem seines Computers, die Adresse der zuvor besuchten Seite oder sein Standort.

Die moderne Büchse der Pandora

Diese Verfolgung des Surfverhaltens heißt Tracking. Sie findet auf fast jeder Seite im Internet statt. Bei den Spionen handelt es sich oft um Werbenetzwerke, Datenanalysefirmen oder soziale Plattformen. Über die Jahre häufen sie immense Datenmengen an, aus denen sich umfangreiche Persönlichkeitsprofile erstellen lassen. Sie erlauben präzise Rückschlüsse auf Interessen und Bedürfnisse des Nutzers, seine finanzielle Lage, den Beziehungsstand, gesundheitliche Probleme, politische Haltungen und sexuelle Präferenzen.

Firmen sammeln all diese Infos mithilfe von Trackern. Dabei handelt es sich um Software, die den Nutzer und sein Surfverhalten genau beobachtet. Es gibt einen Hauptgrund, weshalb die Betreiber von Internetseiten fremden Firmen erlauben, auf ihren Portalen zu spionieren: Sie wollen mit dem Einblenden von Werbung Geld verdienen. Je passgenauer Anzeigen werbender Firmen auf die individuellen Interessen und Vorlieben des Surfers zugeschnitten sind, desto erfolgversprechender ist die Werbung. Die akkurate Anpassung an den Nutzer funktioniert aber nur, wenn er umfassend ausgeforscht wird. Mal überwachen ihn nur zwei Unternehmen auf einer Seite, mal sind es 30 oder 40.

Gegen Werbung im Netz ist an sich wenig einzuwenden: Sie ermöglicht, dass wir online kostenlos Musik hören, Videos sehen oder Nachrichten über den FC Bayern lesen können. Werbung finanziert viele Gratisportale. Sport1 etwa muss Redakteure und Techniker bezahlen, um die News über den FC Bayern an die Leser zu bringen.

Das Problem: Zur Personalisierung der Werbung werden Unmengen von Nutzerdaten abgegriffen. Der Surfer zahlt nicht mit Geld, sondern mit dem Verlust seiner Privatsphäre. Das Geschäft lohnt sich: Im Jahr 2015 sorgte Onlinewerbung weltweit für rund 130 Milliarden Euro Umsatz.

Im Verborgenen

Der Surfer bemerkt im Normalfall kaum etwas vom Tracking. Irgendwann hat ihm Sport1.de mal einen Hinweis zu den Cookies eingeblendet, die auf der Seite aktiv sind. Doch meist klicken Nutzer dann einfach schnell auf Okay. Kaum jemand liest die oft ellenlangen, komplizierten Erklärungen. Vom Ausmaß des Datenhungers der Tracker haben viele Menschen daher kaum eine Vorstellung.

Wie die Verfolgung funktioniert

Die Tracker können Surfer häufig über mehrere Internetbrowser und mehrere Geräte hinweg verfolgen – vom Smartphone über den PC bis hin zum Tablet. Die Verfolgung gelingt ihnen vor allem mit zwei Techniken: Cookies und Fingerprinting.

Cookies sind kleine, in Internetseiten eingebettete Dateien, die automatisch auf den Rechner des Nutzers übertragen werden, sobald er eine Seite erstmals aufruft. Sie weisen jedem Surfer eine individuelle Identifikationsnummer zu, um ihn bei späteren Besuchen oder auf anderen Seiten wiedererkennen zu können. Cookies bleiben oft jahrelang auf dem Computer.

Beim Fingerprinting speichern die Tracker einen digitalen „Fingerabdruck“ des Surfers. Sie erfassen etwa das Betriebssystem seines Rechners, die darauf installierten Schriftarten, die Speicherkapazität und

FOTO: THINKSTOCK

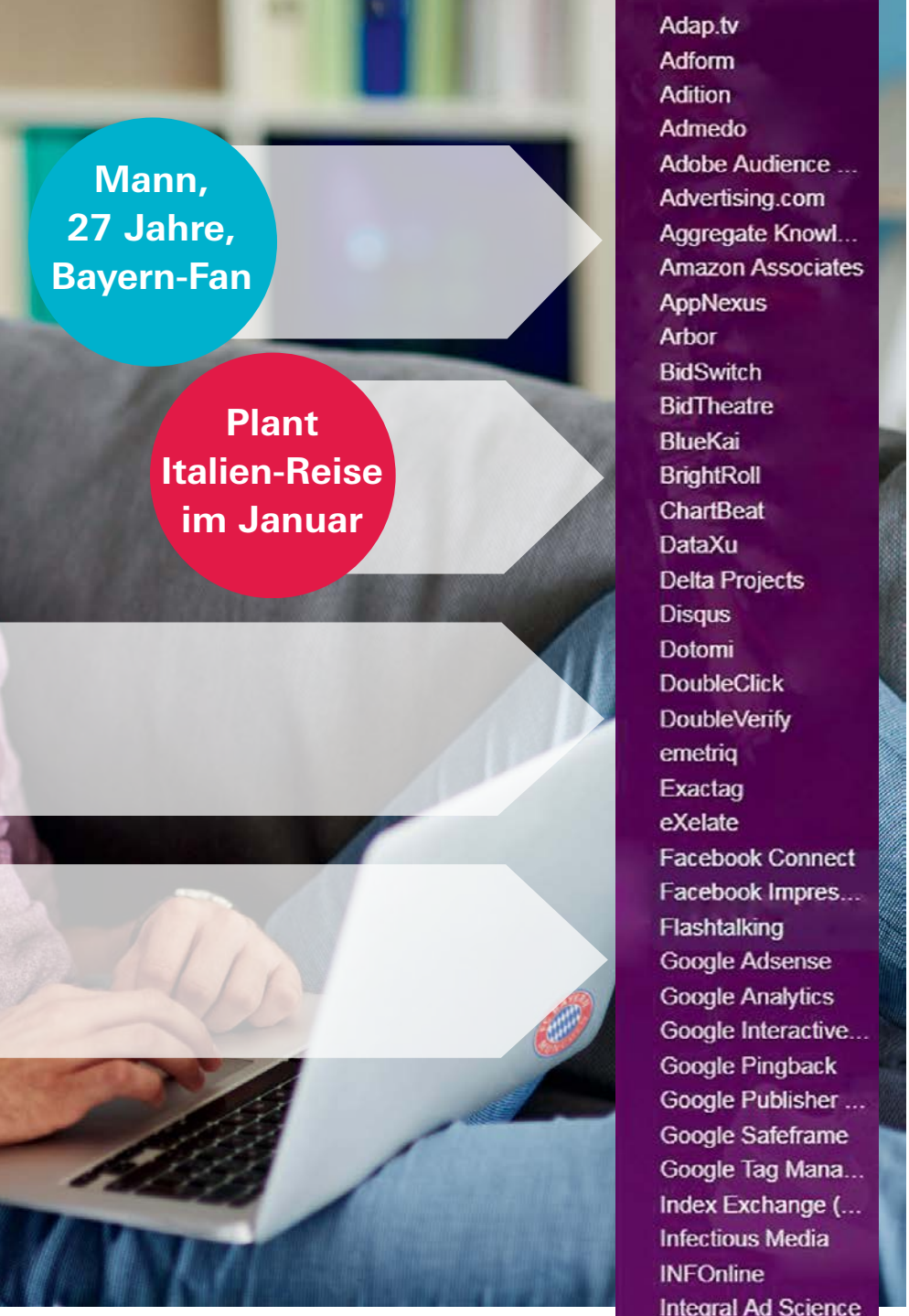


FOTO: THINKSTOCK

Tracking:

Firmen beobachten Surfer im Netz und erfahren intime Details.

die Auflösung des Displays. So erstellen sie ein möglichst individuelles Profil des verwendeten Geräts, um den Nutzer auch auf anderen Seiten identifizieren zu können.

Langsamer durchs Netz

Tracking hat nicht nur auf die Privatsphäre negative Auswirkungen. Es senkt auch die Surfgeschwindigkeit: Zusätzlich zur Internetseite müssen zahlreiche Tracking-Elemente geladen werden, die folglich die Datenmenge erhöhen. Außerdem verwenden einige Tracking-Methoden Programmiersprachen wie Javascript oder Flash, die als Einfallstore für Computerviren gelten.

Auf Bonität abgeklopft

Die Nutzerdaten dienen zwar primär, aber nicht ausschließlich zu Werbezwecken. Auch sogenannte Scoring-Unternehmen, die die Bonität von Verbrauchern bewerten, interessieren sich dafür. Ihre Urteile können zum Beispiel darüber entscheiden, ob jemand einen Kredit erhält oder nicht. Zusätzlich wäre auch Preisdiskriminierung möglich: Als zahlungskräftig eingestufte Kunden könnten online für das gleiche Produkt mehr bezahlen müssen als andere Käufer, die als weniger wohlhabend gelten.

Viele solcher Scoring-Dienste sind kaum einem Verbraucher bekannt. Ihre Urteilsfindung ist oft intransparent und es gibt keine Garantie, dass sie Nutzern Auskunft über die von ihnen erfassten Daten erteilen. Scoring-Firmen außerhalb der EU müssen sich nicht einmal an europäische Datenschutzbestimmungen halten.

Albtraum Datendiebstahl

Das wohl beunruhigendste Szenario im Zusammenhang mit Tracking ist ein Datendiebstahl. Täter kann beispielsweise ein frustrierter, neugieriger Mitarbeiter einer Trackingfirma sein – oder ein Hacker, dem es gelingt, die Server eines solchen Unternehmens zu knacken und die dort gespeicherten Nutzerdaten zu erbeuten.

Je nach Art der entwendeten Daten lässt sich alles Mögliche damit anfangen: Erpressung mit kompromittierenden Informationen etwa – oder eine Überwachung täglicher Routinen, um den besten Zeitpunkt für Einbrüche zu bestimmen.

Bei den digitalen Eindringlingen kann es sich auch um staatliche Hacker handeln. Spätestens seit den Enthüllungen von Edward Snowden ist bekannt, dass Geheimdienste Sicherheitslücken ausnutzen, um Bürger auszuspähen.

Die gute Nachricht: Tracking lässt sich einschränken. Auf den folgenden Seiten steht, wie Surfer ihre Privatsphäre mithilfe von Tracking-Blockern schützen können. ■ ▶▶

Zehn Tracking-Blocker im Test. Wie effektiv sie die Verfolger abschütteln, lesen Sie ab Seite 40.

Spuren verwischen

Tracking-Blocker Mit speziellen Programmen können Surfer ihre Verfolger abschütteln. Im Test mussten zehn Blocker beweisen, wie gut sie die Privatsphäre schützen.

Was gibts Neues vom 27-jährigen Bayern-Fan mit dem Fußfetischismus? Diese Frage stellen Tracker regelmäßig (siehe S. 38). Solche auf Internetseiten versteckten Schnüffelprogramme verfolgen sein Surfverhalten. Der Bayern-Fan hat jedoch an einem fußballfreien Abend einen Tracking-Blocker installiert. Nicht mal eine Minute hat das gedauert. Geringer Aufwand, hoher Ertrag: Der Blocker schränkt die Fähigkeit von Firmen ein, ihn auszuspionieren. Aus dem Datenstrom wird ein Rinnsal. Zudem freut den jungen Mann, dass sich seine Lieblingsportale nun etwas schneller aufrufen lassen, da sie viele Tracking-Elemente im Hintergrund nicht mehr laden müssen.

Gekostet hat ihn das Ganze nichts. Die Basisversionen aller zehn Programme im Test sind gratis. Die meisten sind auch für Nutzer mit durchschnittlichen Computerkenntnissen leicht zu handhaben. Rund die Hälfte bietet detaillierte Einstellungsmöglichkeiten und Zusatzfunktionen.

Wie effektiv die Werkzeuge das Ausspähen des Nutzers verhindern, war das wichtigste Prüfkriterium. Die Resultate unterscheiden sich deutlich (siehe Kommentare S. 42/43). Für alle Blocker gilt aber: Ihr Einsatz lohnt sich auf jeden Fall. Egal für welches Programm sich der Anwender entscheidet – allein durch die ruckzuck erledigte Installation dieses Schutzschilds stärkt er seine Privatsphäre schon.

Tipp: Wichtig ist, dass Sie jeden Rechner und jeden Internetbrowser, auf dem Sie Tracking verhindern wollen, mit einem Blocker ausstatten. Sie können auch mehrere Blocker parallel verwenden.

PCs leichter zu schützen als Handys

Im Test haben wir uns aufs Surfen per Computer konzentriert. Smartphones und Tablets haben wir ausgeklammert, da sich Tracking dort deutlich schwerer unterbinden lässt. Mobil kommen anstelle des Browsers oft Apps zum Einsatz – in Apps können Nutzer aber keine Tracking-Blocker einbinden. Auf Computern werden die Blocker als Erweiterungen – auch Add-ons genannt – direkt in den Internetbrowser integriert.

Wir haben sechs Erweiterungen mit dem Browser Chrome und drei mit Firefox auf einem Windows-PC geprüft. Der Grund: Diese Software-Kombinationen sind unter deutschen Internetnutzern am stärksten verbreitet. Es gibt die Blocker aber oft auch für andere Browser sowie für Mac-Rechner.

Tipp: Wie Sie die Erweiterungen in Ihren Internetbrowser einbinden können, zeigen die Anleitungen auf Seite 44.

Unser Rat

Installieren Sie einen oder mehrere Tracking-Blocker! Am besten auf jedem Rechner und in jedem Browser. **Egal welchen Blocker** Sie wählen: Ihre Privatsphäre ist damit auf jeden Fall besser geschützt als ohne. Die besten Erfahrungen machten wir in unserem Test mit **uBlock Origin.** Das Programm bietet eine gute Balance aus Schutzfunktionen und geringen Surf-Einschränkungen.

Sonderfall Cliqz-Browser

Zusätzlich zu den neun Erweiterungen haben wir den Internetbrowser Cliqz getestet. Dessen Anbieter wirbt für die voreingestellten Funktionen, mit denen Cliqz das Tracking behindert. Bei anderen Browsern lassen sich solche Schutzmethoden zwar teilweise auch aktivieren, der Nutzer muss sich aber selbst darum kümmern – und das kann kompliziert sein.

FOTO: THINKSTOCK

Blocker:

Sie schränken Tracking ein und verwischen die Spuren im Netz.

Zu viel blockieren kann schaden

Um die Effektivität der Tracking-Blocker zu beurteilen, untersuchten wir zunächst auf zwölf beliebten Internetportalen, wie viele Tracker die Seiten einsetzen. Anschließend prüften wir, wie viele Schnüffler sie noch mit Daten versorgen, nachdem wir den jeweiligen Blocker aktiviert hatten.

Mit den Grundeinstellungen senkte das Programm Scriptsafe die Anzahl der Tracker um 85 Prozent – der höchste Wert im Test. Ghostery und das Cliqz-Add-on kamen nur auf 3 Prozent. Der Nutzer kann die Einstellungen aber nach Belieben verändern, sodass anfangs zaghafte Programme schärfer blockieren und aggressive Erweiterungen sich etwas zurückhalten. Viel blockieren ist zwar grundsätzlich sinnvoll, doch es gibt auch Grenzen: Zu harsches Vorgehen wie bei Scriptsafe oder NoScript kann zu massiven Funktionsverlusten führen: Bilder oder Videos verschwinden von der Oberfläche, Texte zerbröckeln, Seiten werden unbenutzbar. In solchen Fällen ist es ratsam, die Intensität des Blockens in den Programmeinstellungen abzumildern.

Tipp: Tritt auf einer Seite ein Defekt auf, können Sie in einem zweiten Browser ohne integrierten Blocker ausprobieren, ob Ihr Blocker den Defekt verursacht hat.

Sanft anfangen, dann hochschalten

Vorsichtiges Blockieren, wie es etwa Ghostery in den Grundeinstellungen praktiziert, verfolgt einen anderen Ansatz: Sobald der Surfer eine Internetseite aufruft, zeigt ihm das Programm eine Liste der Firmen an, die im Hintergrund seine Daten abgreifen. Durch diesen „Bildungseffekt“ kann er dann selbst entscheiden, wie scharf er die Blockierfunktion ausrichten möchte.

Wie so oft geht es um den goldenen Mittelweg: Je stärker die Programme blockieren, desto mehr Einschränkungen treten auf. Schwache Einstellungen ermöglichen bequemes Surfen, verbessern den Schutz der Privatsphäre aber nur geringfügig.

Was Tracking-Blocker zeigen

Die Blocker erscheinen meist als Symbol rechts oben im Browser, direkt neben der Adresszeile. Surft der Nutzer eine Seite an, zeigt das Symbol, wie viele Tracking-Elemente der Blocker entdeckt hat. Klickt der Nutzer auf das Symbol, folgen weitere Infos – zum Beispiel die Namen der Tracker, ihr Einsatzzweck oder Links, die Erläuterungen zum jeweiligen Spion liefern.

Die geprüften Programme arbeiten mit unterschiedlichen Methoden: Adblock Plus und uBlock Origin etwa verwenden „schwarze Listen“ mit bekannten Trackern. Erkennen sie einen solchen auf einer Seite, blocken sie dessen Anfragen. Scriptsafe und No-Script stoppen die Ausführung sogenannter Skripte – das sind Programme auf Internetseiten, die Aktionen auf dem Rechner des Nutzers ausführen und so Daten auslesen wollen.

Der Cliqz-Browser unterbindet nicht generell Anfragen von Trackern, sondern beschränkt deren Datenerfassung auf nicht-individuelle Infos, um die Anonymität des Nutzers zu wahren.

Ohne Vertrauen geht es nicht

Tracking-Blocker schützen die Privatsphäre und kosten nichts – das klingt fast zu schön, um wahr zu sein. Tatsächlich gibt es einen Pferdefuß: Theoretisch könnten ▶

FOTO: THINKSTOCK

die Anbieter der Blocker all jene Daten, die sie vor Trackern abschirmen, selbst abgreifen und im schlimmsten Fall verkaufen. Es ist nicht möglich, das von außen zu prüfen. Deshalb ist letztlich Vertrauen gefragt.

Arbeiten die Anbieter sauber, profitiert der Nutzer auf jeden Fall von den Programmen. Aber selbst wenn sie die Daten verkaufen sollten: Schlimmer als ohne Blocker ist der Nutzer auch dann nicht dran. Hat er keinen Blocker installiert, bekommen definitiv zahlreiche Firmen seine Daten.

Wie die Macher Geld verdienen

Da die Blocker kostenlos sind, stellt sich die Frage, wie die Programmierer ihre Arbeit refinanzieren. Ein typisches Beispiel ist Adblock Plus. Der Anbieter führt „weiße Listen", mit denen er definiert, welche Arten von nichtinvasiver Werbung durchgelassen werden. Für diese Türöffnerfunktion verlangt er Geld von werbenden Firmen.

Manche Blocker brauchen keine Einnahmen zu generieren. Privacy Badger etwa stammt von der US-Datenschutzorganisation „Electronic Frontier Foundation". Sie verfolgt ein rein politisches Ziel: den Schutz der Privatsphäre im Internet.

Wenn Blocker blockiert werden

Immer mehr Internetseiten gelingt es, den Einsatz von Tracking-Blockern zu erkennen. Einige Portale blenden dann ihre eigentlichen Inhalte aus und verlangen, dass der Nutzer den Blocker abschaltet. Oft reicht es aber schon, in den Einstellungen des Blockers eine Ausnahme für die jeweilige Seite festzulegen. Oder der Surfer probiert es mal mit einem anderen Blocker.

Gute Werbung, schlechte Werbung

Tracking-Blocker stoppen oft nicht nur die Datensammelei von Schnüffelfirmen, sie blenden auch Werbeanzeigen aus. Während der Kampf gegen die Spione sinnvoll ist, sollten Nutzer sich überlegen, wie viel Werbung sie blockieren. Viele Gratisdienste könnten ohne Werbung ihre Kosten nicht decken. Sie müssten Nutzungsgebühren erheben – oder den Betrieb einstellen.

Wer gern kostenlose Onlineangebote nutzt, sollte gegen Tracking vorgehen, Werbung aber in Maßen zulassen. Besonders leicht klappt das bei uBlock Origin, mit dem Nutzer gezielt einzelne Seitenelemente abschalten können. Bei anderen Blockern lassen sich in den Einstellungen Ausnahmen für die eigenen Lieblingsseiten definieren. Die Programme merken sie sich für jeden weiteren Besuch. ■ ▶▶

Zusatzprogramme für Internetbrowser

Adblock Plus
(geprüft mit Chrome)

Verringerung der Tracker-Anzahl: 48 %

Handhabung für Normalnutzer: gut

Optionen für Erfahrene: befriedigend

Gegen Werbung und Tracking. Das kostenlose Zusatzprogramm für den Browser stoppt nervende Werbung und bietet Trackingschutz. Es lässt nur Werbung zu, die bestimmten Bedingungen entspricht: Zum Beispiel sollten die Anzeigen nicht zu viel Raum einnehmen und klar als Werbung zu erkennen sein. Der Blocker ist einfach zu bedienen. Nutzungsbedingungen und Datenschutzerklärung auf Deutsch vorhanden. Programm verfügbar für Chrome, Edge, Firefox, Internet Explorer, Opera, Safari.

Better Privacy
(geprüft mit Firefox)

Verringerung der Tracker-Anzahl: 17 %

Handhabung für Normalnutzer: befriedigend

Optionen für Erfahrene: befriedigend

Gegen Supercookies, auf Englisch. Löscht sogenannte Supercookies, die für Nutzer manuell nur schwer zu entfernen sind. Supercookies verwenden die überholte Flash-Technik. Sie wird von vielen Browsern nicht mehr gestattet, da sie als unsicher gilt. Das kostenlose Programm ist sinnvoll für Nutzer, die Flash weiterhin brauchen – ansonsten reicht es, auf die Installation von Flash zu verzichten. Das Menü der Browser-Erweiterung ist schwer zu finden. Blocker nur auf Englisch erhältlich. Keine Nutzungsbedingungen oder Datenschutzerklärung in deutscher Sprache vorhanden. Programm verfügbar für Firefox.

NoScript
(geprüft mit Firefox)

Verringerung der Tracker-Anzahl: 81 %

Handhabung für Normalnutzer: ausreichend

Optionen für Erfahrene: gut

Kompliziert zu steuern. Das kostenlose Programm blockiert Javascript und andere aktive Elemente, die dem Tracking dienen und als Einfallstore für Schädlinge gelten. Arbeitet so aggressiv, dass einige Seiten nicht mehr richtig nutzbar sind. Steuerung für Nutzer mit durchschnittlichen Computerkenntnissen ziemlich kompliziert.*) Keine Nutzungsbedingungen oder Datenschutzerklärung in deutscher Sprache vorhanden. Programm verfügbar für Firefox.

*) Korrigiert am 7.9.2017.

Privacy Badger
(geprüft mit Chrome)

Verringerung der Tracker-Anzahl: 21 %

Handhabung für Normalnutzer: gut

Optionen für Erfahrene: befriedigend

Einige Schwächen. Kostenloser Tracking-Blocker der amerikanischen Datenschutzorganisation „Electronic Frontier Foundation". Das Programm offenbart einige Schwächen: Das Menü-Design ist verbesserungswürdig, Erläuterungen zu den geblockten Trackern liefert Privacy Badger kaum. Keine Nutzungsbedingungen oder Datenschutzerklärung in deutscher Sprache vorhanden. Programm verfügbar für Chrome, Firefox, Opera.

Cliqz Add-on
(geprüft mit Firefox)

Verringerung der Tracker-Anzahl:
3 %

Handhabung für Normalnutzer: sehr gut

Optionen für Erfahrene: sehr gut

Sehr leicht zu bedienen. Kostenlose Erweiterung für den Internetbrowser Firefox als Alternative zum separaten Cliqz-Browser. Mit den Grundeinstellungen blockiert Cliqz nicht die Tracker an sich, sondern die Übertragung personenidentifizierbarer Daten an die Tracker. Mit diesen Grundeinstellungen blockiert das Cliqz-Add-on wenig. Auch für Normalnutzer ist es sehr leicht zu bedienen, zugleich bietet es erfreulich viele Einstellungsmöglichkeiten für erfahrene Nutzer. Datenschutzerklärung auf Deutsch, aber keine Nutzungsbedingungen vorhanden. Programm verfügbar für Firefox.

Disconnect
(geprüft mit Chrome)

Verringerung der Tracker-Anzahl:
63 %

Handhabung für Normalnutzer: gut

Optionen für Erfahrene: befriedigend

Gegen Tracking, auf Englisch. Die Basis-Version des Programms ist kostenlos. Es ist vor allem gegen Tracking gerichtet – Blockieren von Werbung als Nebeneffekt. Einfach zu bedienen. Das Programm ist nur auf Englisch erhältlich. Die Datenschutzbestimmungen gibt es auf Deutsch, es sind aber keine Nutzungsbedingungen vorhanden. Programm verfügbar für Chrome, Firefox, Opera, Safari.

Ghostery
(geprüft mit Chrome)

Verringerung der Tracker-Anzahl:
3 %

Handhabung für Normalnutzer: gut

Optionen für Erfahrene: sehr gut

Bildungseffekt steht im Vordergrund. Mit den Grundeinstellungen blockiert Ghostery wenig. Stattdessen klärt es den Nutzer auf, welche Dienste gerade seine Daten abgreifen. Leichte Bedienung für Normalnutzer, erfreulich viele Einstellungsmöglichkeiten für erfahrene Nutzer. Anders als die meisten Tracking-Blocker erhöht Ghostery die Datenmenge etwas – dadurch kann der Seitenaufbau minimal länger dauern. Lizenzvertrag und Datenschutzerklärung auf Deutsch vorhanden. Kostenloses Programm. Verfügbar für Chrome, Edge, Firefox, Internet Explorer, Opera, Safari.

Scriptsafe
(geprüft mit Chrome)

Verringerung der Tracker-Anzahl:
85 %

Handhabung für Normalnutzer: ausreichend

Optionen für Erfahrene: sehr gut

Kompliziert zu steuern. Das kostenlose Programm blockiert vor allem Javascript – eine Technologie, die dem Tracking dient und als Einfallstor für Schädlinge gilt. Es arbeitet so aggressiv, dass einige Seiten nicht mehr richtig nutzbar sind. Für Nutzer mit durchschnittlichen Computerkenntnissen ziemlich kompliziert zu steuern. Erfreulich viele Einstellungsmöglichkeiten für erfahrene Nutzer. Keine Nutzungsbedingungen oder Datenschutzerklärung in deutscher Sprache vorhanden. Programm verfügbar für Chrome.

uBlock Origin
(geprüft mit Chrome)

Verringerung der Tracker-Anzahl:
77 %

Handhabung für Normalnutzer: sehr gut

Optionen für Erfahrene: sehr gut

Sehr variabel. Allround-Schutz gegen Tracking, Schädlinge und Werbung. Das kostenlose Programm vermindert die Zahl der Tracker intensiv, zugleich führt es kaum zu Funktionsverlusten auf Internetseiten. Der Nutzer kann per Mausklick Elemente auswählen, die er von Seiten entfernen möchte. Sehr viele Einstellungsmöglichkeiten für erfahrene Nutzer, dennoch auch für Normalnutzer sehr leicht zu bedienen. Keine Nutzungsbedingungen oder Datenschutzerklärung in deutscher Sprache vorhanden. Programm verfügbar für Chrome, Edge, Firefox, Safari.

Internetbrowser

Cliqz-Browser

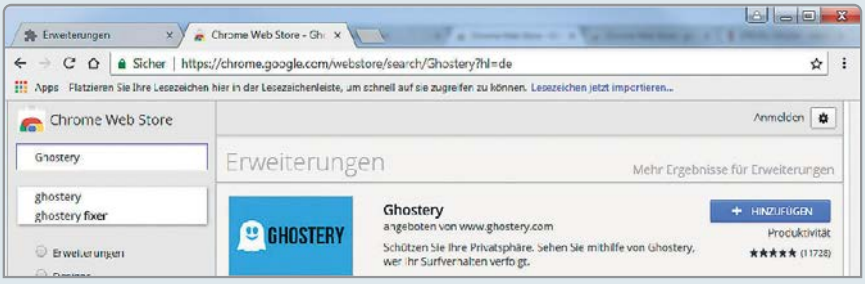
Verringerung der Tracker-Anzahl:
16 %

Handhabung für Normalnutzer: sehr gut

Optionen für Erfahrene: gut

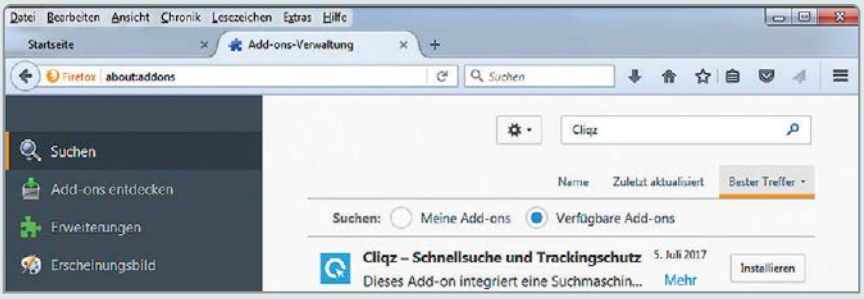
Sehr leicht zu bedienen. Browser mit Tracking-Blockerfunktionen – baut auf Firefox auf. Mit den Grundeinstellungen blockiert Cliqz nicht die Tracker an sich, sondern die Übertragung personenidentifizierbarer Daten an die Tracker. Mit diesen Grundeinstellungen blockiert der kostenlose Browser relativ wenig. Bedienung sehr leicht. Anders als die meisten Tools im Test erhöht der Browser die Datenmenge etwas – daher kann der Seitenaufbau minimal länger dauern. Datenschutzerklärung auf Deutsch, aber keine Nutzungsbedingungen vorhanden.

Wie Sie Blocker installieren und mit Daten geizen



Installation der Blocker im Internetbrowser Chrome:

▸ **Rechts oben im Browser auf das Drei-Punkte-Symbol klicken** ▸ **Dann auf „Weitere Tools“** ▸ **„Erweiterungen“** ▸ **„Mehr Erweiterungen herunterladen“** ▸ **Namen des gewünschten Tracking-Blockers eingeben** ▸ **„Hinzufügen“**



Installation der Blocker im Internetbrowser Firefox:

▸ **Rechts oben im Browser auf das Drei-Balken-Symbol klicken** ▸ **Dann „Add-ons“** ▸ **„Erweiterungen“** ▸ **Namen des gewünschten Trackers eingeben** ▸ **„Installieren“**

Die Installation von Tracking-Blockern (siehe links) ist nur eine Option, um Datenjäger zu stoppen. Die folgenden Tipps helfen ebenfalls, Ihre Privatsphäre zu schützen.

Ohne Login surfen. Auch wenn es unbequem ist: Melden Sie sich lieber jedes Mal separat an, wenn Sie online einen Dienst verwenden wollen. Sind Sie immer eingeloggt, erleichtert das Trackern die Arbeit.

Daten streuen. Nutzen Sie nicht zu viele Dienste aus einer Hand, etwa von Apple oder Google. Verteilen Sie Ihre Daten, indem Sie auf andere Browser, E-Mail-Anbieter (test 10/2016 oder test.de) und alternative Suchmaschinen wie Metager.de, Ixquick.com oder Duckduckgo.com zugreifen.

Mehr Tipps. Noch mehr praktische Kniffe haben wir auf test.de/datenspar sam versammelt. Dort lesen Sie unter anderem, wie Sie Cookies löschen, Ihre IP-Adresse ändern und den anonymen Modus Ihres Browsers verwenden können.

So haben wir getestet

Im Test: Wir prüften auf einem Computer mit dem Betriebssystem Windows 10 exemplarisch neun aktuelle, kostenlose und verbreitete Add-ons für die Browser Chrome und Firefox, die Trackingmethoden und Werbung behindern. Zusätzlich prüften wir den Cliqz-Browser – einen separaten Browser, der Trackingblockerfunktionen verwendet.

Prüfzeitraum: März bis Mai 2017.

Untersuchungen: Mittels eines transparenten Proxy-Servers und einer Man-in-the-Middle-Attacke überprüften wir auf zwölf populären Internetseiten, die mit gängigen Trackingmethoden arbeiten, in welchem Umfang der Einsatz der geprüften Blocker zu einer **Verringerung der Tracker-Anzahl** führt und ob durch die verwendeten Blocker Einschränkungen beim Surfen auftreten.

Mit drei Experten prüften und bewerteten wir die Installation, die Konfiguration und den täglichen Gebrauch der Programme. Dabei prüften wir auch, wie einfach die **Handhabung für Normalnutzer** mit durchschnittlichen Computerkenntnissen ist. Weiterhin bewerteten wir, welche zusätzlichen **Optionen für Erfahrene** die Programme bieten – zum Beispiel: Ausnahmen für bestimmte Seiten, Medientypen und Techniken wie Flash oder Javascript. Zusätzlich überprüften wir die Veränderung der übertragenen Datenmengen beim Einsatz der Blocker.

Tracking auf test.de

Was wir erfassen. Auch die Stiftung Warentest setzt Tracking ein, allerdings nur in geringem Maße. Da wir in unseren Publikationen – so auch auf test.de – keinerlei Werbung von anderen Firmen zulassen, besteht für uns keine Notwendigkeit, größere Mengen von Nutzerdaten auszulesen. Wir legen aber auf dem Rechner jedes test.de-Besuchers einen Cookie ab. Diese Datei dient unter anderem dazu, registrierten Nutzern das Einloggen zu ermöglichen, ihre Bestellungen zu speichern und die gekauften Produkte an sie zu liefern.

Wie wir es analysieren. Wir ermitteln in anonymisierter Form, welche Onlineartikel auf test.de von einem Computer abgerufen werden, von welchen Internetseiten die Nutzer zu test.de kommen und wie viele Surfer die einzelnen Onlineartikel lesen.

Mehr Infos. Auf test.de/stiwa-tracking erfahren Sie weitere Details zu unseren Tracking-Methoden.