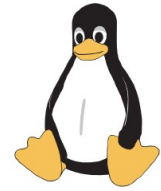




Sicherer und privater im Netz bewegen


Surfen im Netz mit Add-Ons zum Browser Firefox




Add-Ons sind kleine Programme, mit der die Arbeitsweise und -umfang des Webbrowsers Firefox erweitert werden kann. Sie finden sich in der Menu-Leiste von Firefox unter Extras (oder hinter den drei Balken, die rechts oben zu sehen sind). Man muss sich aber der Tatsache bewusst sein, daß alle Maßnahmen, die das Browsen sicherer und privater machen, dazu führen können, dass Webseiten langsamer geladen werden und evtl. nicht mehr vollständig angezeigt werden. Für diese Seiten muss man dann u.U. auf den Schutz verzichten.

 Eine alltägliche Erfahrung beim Browsen im Internet ist, daß **Werbung** eingeblendet wird, die teilweise sehr störend ist oder sogar sich dauerhaft in den Browser einnistet. Ein Mittel dagegen ist das Add-On uBlock.

 Nicht so direkt zu erkennen ist, dass mit kleinen Datenkrümeln (sog. cookies) versucht wird zu verfolgen, welche Seiten im Internet besucht werden, dass der Nutzer verfolgt wird. Aus dem Englischen wird der Begriff **getrackt** (von track = die Spur) verwendet. Damit sollen Informationen abgegriffen werden, um z.B. als harmloseste Variante auf die Person bezogene Werbung zu erzeugen. Mit dem Add-On **Privacy-Badger** kann man das beschränken oder teilweise ganz verhindern.

 Ein wichtiges Werkzeug, um sicherer im Internet zu browsen, ist die Verwendung von **verschlüsselten Verbindungen**, die man daran erkennt, dass statt http https (das >s< steht für sicher=secure) angezeigt wird. Webseiten bieten oft den Zugang über eine unverschlüsselte und eine verschlüsselte Verbindung an. Das Add-On **https-everywhere** sorgt dafür, dass immer die verschlüsselte Verbindung verwendet wird, wenn eine angeboten wird.

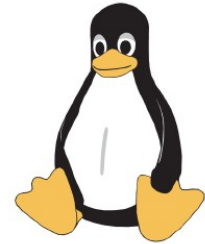
 Auf Internet-Seiten finden sich oft kleine Programme, sogenannte Skripte, die für die Funktionalität oft wichtig sind, aber auch Einfallstor für Viren und anderes Nachteiliges sind. Die Ausführung kann gesteuert werden mit dem Add-On **noscript**. Die Verwendung ist nur sehr erfahrenen Usern oder denen empfohlen, die bereit sind, für ihre Sicherheit und Privatheit eine Zeitlang große und auf Dauer kleinere Unannehmlichkeiten auf sich zu nehmen.

Unbeobachtet im Netz suchen mit Startpage

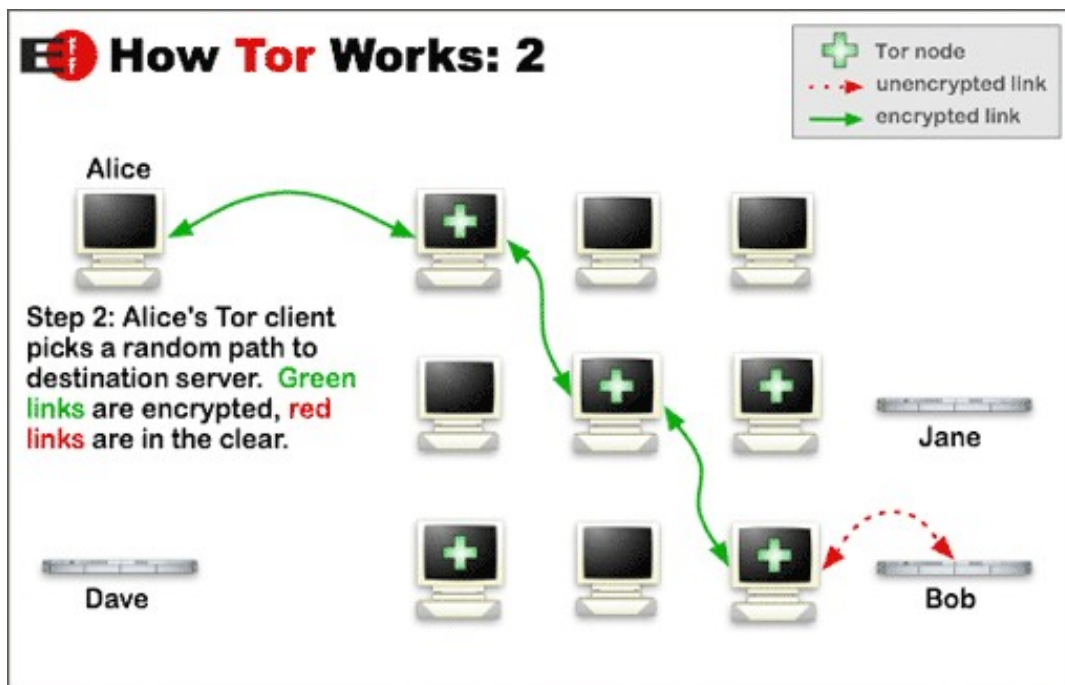
Die Suchmaschine von google wird so häufig und selbstverständlich verwendet, dass „googeln“ zu einem Synonym für „Suchen im Internet“ geworden ist. Leider sammelt google aber eine Fülle von Daten über das Suchverhalten der Nutzer. Es gibt aber Suchmaschinen, die die Privatheit der Nutzer respektieren.

startpage Eine davon ist **Startpage**, die unter <https://startpage.com/deu/> zu finden ist. Sie sollten **Startpage als Startseite** von Firefox unter Einstellungen / Allgemein einstellen.

Anonym surfen mit dem TOR-Browser, der auf Firefox aufbaut



Eine Möglichkeit, die Verfolgung Ihrer Aktivitäten im WWW zu erschweren, ist die Verwendung des TOR-Browsers, der eine Weiterentwicklung des Webbrowsers Firefox ist, mit der man das TOR-Netzwerk nutzen kann. Das TOR-Netzwerk ermöglicht anonymes Surfen im Internet, indem die Internet-Verbindung über mehrere Server aufgebaut werden, die jeweils nur wissen, woher die Anfrage kommt und an welchen Server sie weiter geleitet werden muss, wie es die folgende Grafik veranschaulicht.



Sie finden weitere Information unter: <https://www.torproject.org/about/overview.html.en>
Dort können Sie auch TOR herunterladen.

Beachten Sie aber, dass TOR in erster Linie ein Anonymisierungswerkzeug und kein Verschlüsselungswerkzeug ist. Um sich weitestgehend sicher und unbeobachtet im Internet bewegen zu können, müssen Sie weitere Maßnahmen ergreifen.