Sicheres Surfen im Internet

Cookies und Tracking - ein paar Grundlagen

Cookies aus dem Internet krümeln nicht. Dafür können sie Informationen über den Nutzer einer Internetseite speichern. Das passiert, wenn die Seite, die den Cookie beim Benutzer speichern will, aufgerufen wird. Man ruft also nicht nur die Seite ab, sondern speichert unter Umständen auch gleichzeitig einen oder mehrere Cookies dazu ab.

Doch wozu dienen Cookies eigentlich? Cookies sind auf keinen Fall per se böse, denn sie erfüllen mitunter sinnvolle Aufgaben, ohne die der Besuch einer Webseite mitunter sehr unkomfortabel und mühselig wäre. Zum Beispiel speichern sie Benutzerdaten auf Seiten, bei denen man sich einloggen muss, wie sozialen Netzwerken. Oder sie enthalten den Inhalt des Warenkorbes bei Onlineshops. Ohne Cookies müsste man diese Informationen also ständig neu eingeben, weil der Browser selbst sie sich nicht merken kann. Auch Benutzereinstellungen, wie die Sprache oder das gewünschte Aussehen einer Seite, können in Cookies abgelegt werden.

Aber Cookies können auch dazu genutzt werden, das Surfverhalten von Nutzern zu verfolgen, den Nutzer also zu tracken. Das geschieht meist über sogenannte Drittanbieter-Cookies, also jene, die gar nicht vom eigenen Betreiber der Webseite kommen, sondern von Dritten, die beispielsweise einen Werbebanner auf der besuchten Seite platziert haben und so ihre Cookies an die Nutzer der Seite verteilen. Ist dieser Drittanbieter auf mehreren Seiten im Netz vertreten, merkt das Cookie, das den Nutzer bereits vom Besuch einer anderen Seite kennt, wenn dieser weitere Seiten betritt, auf denen der Drittanbieter vertreten ist. Das Cookie kann also dazu benutzt werden, die Wege des Nutzers im Netz nachzuverfolgen. Dann kann ermittelt werden, wofür er sich interessiert.

Willst Du nicht, dass unbekannte andere ausnutzen, wofür Du dich gerade interessierst oder was Du deiner Mutter zu Weihnachten schenkst bevor Du selbst es weißt? Im Folgenden sind ein paar Möglichkeiten beschrieben, wie man besser kontrollieren und nachvollziehen kann, welche Informationskrümel man für wen im Netz hinterlassen will. Außerdem werden Erweiterungen gezeigt, die das Surfen sicherer machen.

Cookie-Einstellungen

Auch ohne zusätzliche Tools hat man bereits die Möglichkeit, sich einen Überblick über gespeicherte Cookies zu verschaffen. Im Firefox-Browser kann man über das Menü „Einstellungen“ die Registerkarte „Datenschutz“ öffnen. Über den „Cookies anzeigen“ Button lassen sich alle gespeicherten Cookies auflisten und bei Bedarf einzeln löschen. Dort lässt sich auch einstellen, dass Cookies von Drittanbietern nicht akzeptiert werden.

Add-ons

Im Folgenden werden einige Firefox Add-ons aufgelistet, die beim Verhindern unerwünschter Cookies nützlich sind und andere positive Effekte auf die Privatsphäre beim Surfen im Internet haben. Bei der Installation der Add-ons ist das Vorgehen immer das gleiche: Klickt man auf Firefox – Add-ons bzw. Extras – Add-ons, öffnet sich ein Fenster zur Add-On-Verwaltung. Im Reiter Add-ons suchen können nun Add-ons gesucht sowie Details über Add-ons angezeigt werden. Will man direkt ein Add-on über den Namen finden, kann man diesen in das Suchfeld oben rechts eingeben. Die Installation erfolgt dann über den Installieren- bzw. Zu Firefox hinzufügen-Button. Nach der Installation muss Firefox in der Regel neu gestartet werden - nun ist das Add-on verfügbar!

HTTPS Everywhere

HTTPS Everywhere ist eine Firefox, Chrome und Opera-Erweiterung, die Ihre Kommunikation mit vielen großen Webseiten verschlüsselt, so dass das Surfen sicherer wird. Dieses Add-On sollte direkt nach der Installation mitinstalliert werden, um sicher zu gehen, dass Verschlüsselung immer genutzt wird, wenn Sie angeboten wird. Dieses Add-on ist nicht im Firefox Add-on Verzeichnis, sondern nur über folgende URL zu finden:

URL: https://www.eff.org/de/https-everywhere

Web of Trust (Add-On)

WOT setzt intuitive Ampelsymbole neben Suchergebnisse und URLs, damit Sie eine Entscheidung darüber treffen können, ob Sie eine Website besuchen möchten oder nicht. Die Bewertungen und Rezensionen von WOT basieren auf einer weltweiten Community aus Millionen von Nutzern, die Websites auf Grundlage ihrer persönlichen Erfahrungen bewertet haben.

URL: https://addons.mozilla.org/de/firefox/addon/wot-safe-browsing-tool

AdBlock Edge

Neben dem Effekt, dass Werbung unangenehm ist und beim Betrachten einer Website stört, werden durch ebenjene oftmals Cookies und Zählpixel auf eine Seite eingeschleust – ein Werbeblocker bietet hier einfache Hilfe! Das Internet wirkt dadurch wie aufgeräumt und man möchte nicht mehr ohne Webeblocker browsen.

URL: https://addons.mozilla.org/de/firefox/addon/adblock-edge/

Ghostery

Ghostery deckt versteckte Trackingmechanismen auf Webseiten auf (zum Beispiel Zählpixel) und zeigt dem Nutzer eine Liste der aktiven Trackingmechanismen an. Er kann sich dann dazu entschließen, welche er blockieren oder erlauben möchte. Außerdem stellt Ghostery bei Auswahl eines dem Programm bekannten Trackers zusätzliche Informationen zu dessen Herkunft bereit, wie zum Beispiel Abgaben zur Herkunftsfirma und deren Datensammlung.

URL: https://addons.mozilla.org/de/firefox/addon/ghostery/

Better Privacy

Better Privacy hilft dem Nutzer, Langzeitcookies zu löschen. Das sind Cookies, die nicht wie klassische Cookies ein Verfallsdatum haben, nach dem sie automatisch vom Browser entfernt werden, sondern die unbegrenzte Lebensdauer haben, weil sie in einem anderen Verzeichnis des Rechners von der Löschung unbehelligt bleiben.

URL: https://addons.mozilla.org/de/firefox/addon/betterprivacy/