Quarks & Co Sicher durch die Datenwelt

Autoren: Carsten Binsack, Cordula Echterhoff, Dirk Gilson, Peter Gotzner, Daniel Münter, Mike Schäfer
Redaktion: Monika Grebe
Assistenz: Uta Reeb

Das Internet ist ein fester Bestandteil unseres Alltags geworden. Doch den wenigsten Menschen ist bewusst, was sie alles über sich preisgeben, wenn sie im Netz unterwegs sind. Quarks & Co zeigt, welche Spuren wir mit jedem Besuch in der virtuellen Welt hinterlassen, welche Gefahren das birgt und wie man seine Daten besser schützen kann.

Ich weiß, was du gestern getan hast ▸ *Wie viel das Internet über einen verrät*
Mehr als 30 Millionen Menschen sind in Deutschland auf Seiten wie MySpace, SchülerVZ und Facebook angemeldet und tauschen sich dort mit ihren Bekannten und Freunden aus. Häufig lesen da auch Fremde mit! Jeder Klick hinterlässt eine digitale Spur. Wer das alles zusammenträgt, kann sehr viel über einen eigentlich fremden Menschen erfahren, heißt es. Quarks & Co hat getestet, ob das wirklich so einfach geht.

Niemals alleine ▸ *Was Werbefirmen über Sie herausfinden, wenn Sie im Internet surfen*
Informationen im Internet finden, online einkaufen, Videos angucken: Die virtuelle Welt des WWW steckt voller Annehmlichkeiten. Doch man bleibt in der Regel nicht allein. Jeder einzelne Klick wird registriert. Mithilfe von sogenannten Cookies verfolgen Werbevermarkter unsere digitalen Spuren im Netz. Welche Folgen das hat, zeigt Quarks & Co an einem alltäglichen Beispiel.

Die Fallen der sozialen Netzwerke ▸ *Facebook – die fast perfekte Marketingmaschinerie*
Rund 18 Millionen Menschen sind in Deutschland bei Facebook aktiv, dem größten sozialen Netzwerk der Welt. Auf den ersten Blick eine geniale Erfindung. Doch wir bezahlen mit einer kostbaren Währung: mit unseren Daten. Quarks & Co zeigt, wie die Nutzer von Facebook mit ihren Daten eine fast perfekte Marketingmaschinerie füttern.

Wer ist auf diesem Bild zu sehen? ▸ *Wie weit die automatische Gesichtserkennung entwickelt ist*
Die automatische Erkennung von Gesichtern ist längst Stand der Technik. Es ist nur eine Frage der Zeit, bis das auch im Internet angeboten wird. Dann ist praktisch jedes Gesicht auf einem Foto in Sekundenschnelle einer Person zuzuordnen. Machbar ist das längst. Das zeigt uns Professor Volker Blanz von der Uni Siegen.

Wenn die eigenen Daten fremdgehen ▸ *Wie bekomme ich meine Daten zurück?*
Das Internet vergisst nie: weder die Fotos der letzten Party, noch den hämischen Kommentar auf der Homepage des gegnerischen Fußballvereins. Doch was, wenn es passiert ist. Wenn Peinliches oder Gemeines über einen im Netz steht. Dann hilft manchmal nur noch der Fachmann, um den guten Ruf zu retten.

Wie Cyberkriminelle Kontodaten stehlen ▸ *Vorsicht vor Trojanern im Netz!*
Es ist schon bedenklich, was Unternehmen wie Google, Apple oder Facebook über uns wissen. Doch richtig bedrohlich wird es, wenn Kriminelle Zugriff auf unsere Daten bekommen. Wenn sie unsere Bankdaten ausspionieren und uns ausrauben. Dazu nutzen sie sogenannte "Trojaner"-Programme. Der Cybercrime-Spezialist Mirko Manske vom Bundeskriminalamt zeigt Quarks & Co, mit welchen Tricks Kriminelle an unsere Daten kommen und was sie damit anfangen können.

Sicher durch die Datenwelt ▸ *Wie man Cookies löscht – und andere Tipps zur Datensicherheit*
Mit nur fünf einfachen Regeln zur Datensicherheit surfen Sie deutlich sicherer im Netz. Quarks & Co stellt sie vor und erklärt am Beispiel der sogenannten „Cookies“ ganz konkret, wie Sie dagegen vorgehen.

Ich weiß, was du gestern getan hast

Wie viel das Internet über einen verrät

Mehr als 30 Millionen Menschen sind in Deutschland auf Seiten wie MySpace, SchülerVZ und Facebook angemeldet und tauschen sich dort mit ihren Bekannten und Freunden aus. Gerade für junge Menschen sind diese Netzwerke ein wichtiger Teil ihres Soziallebens. Doch häufig können auch Fremde mitlesen! Mit jedem Klick hinterlassen wir eine digitale Spur. Wer das alles zusammenträgt, kann sehr viel über einen eigentlich fremden Menschen erfahren, heißt es.

Ob das wirklich so einfach geht, wollten wir selbst ausprobieren: Sechs mutige Quarks-Zuschauer stellen sich unserem Internet-Experiment. Die Spielregel: Internet-Experte Boris Kartheäuser soll zeigen, was er in kurzer Zeit mit normalen Suchmaschinen über unsere Kandidaten herausfinden kann, wenn er nur deren Namen und Geburtsdatum kennt. Was er herausbekommen konnte und was nicht, das sehen Sie im Quarks-Film. Jetzt angucken auf www.quarks.de.

Autor: Mike Schaefer

Niemals alleine

Was Werbefirmen über Sie herausfinden, wenn Sie im Internet surfen

Informationen im Internet finden, online einkaufen, Videos angucken: Die virtuelle Welt des WWW steckt voller Annehmlichkeiten. Doch man bleibt in der Regel nicht alleine, wenn man im Internet „unterwegs“ ist. Wer auf der Webseite eines Buchshops surft, klickt diesen und jenen Titel an und kauft vielleicht auch eines der Bücher. Jeder einzelne Schritt wird dabei registriert. Mithilfe von sogenannten Cookies verfolgen Werbevermarkter unsere digitalen Spuren im Netz. Das ermöglicht ihnen mit der Zeit, ein ziemlich exaktes Profil über uns zu erstellen. Das ist auch der Grund dafür, dass Werbung, die beim Besuch von Webseiten eingeblendet wird, oft überraschend gut auf unsere Person zugeschnitten ist.

Sehen Sie im Film auf www.quarks.de, warum Sarah, die vor kurzem ein paar Bücher im Internet gekauft hat, heute einen Fahrradhelm bestellt.

Autoren: Peter Gotzner, Ulrich Grünewald

Die Fallen der sozialen Netzwerke

Facebook – die fast perfekte Marketingmaschinerie

Rund 18 Millionen Menschen sind in Deutschland bei Facebook registriertaktiv, dem größten sozialen Netzwerk der Welt. Auf den ersten Blick eine geniale Erfindung – und darüber hinaus auch kostenlos. Doch wir bezahlen mit einer kostbaren Währung: mit unseren Daten. Das beginnt schon bei der Registrierung. Die Macher von Facebook fordern uns nachdrücklich auf, möglichst viel von uns zu verraten: Alter, Wohnort, Beziehungsstatus, Konsumvorlieben, religiöse Ansichten. Auch über Arbeitgeber und Kollegen, Schulbildung und politische Einstellung sollen wir Auskunft geben. Pflicht ist dies nicht. Doch viele User präsentieren sich gern ihren Freunden. Ein Traum für Facebook und seine Werbepartner. Denn jeder Nutzer hat für das Unternehmen Facebook einen Wert von rund 100 Dollar (zurzeit etwa 70 Euro). Und das nur durch unsere Daten, mit denen wir „bezahlen", damit unsere Freunde und Bekannten nur ein paar Mausklicks entfernt sind.

Quarks & Co zeigt, wie die Nutzer von Facebook mit ihren Daten eine fast perfekte Marketing-maschinerie füttern – und was der in Deutschland für Facebook zuständige Datenschutzbeauftragte Professor Johannes Caspar aus Hamburg dazu meint. Jetzt angucken auf www.quarks.de.

Autor: Daniel Münter

Wer ist auf diesem Bild zu sehen?

Wie weit die automatische Gesichtserkennung entwickelt ist

Das Internet quillt über vor Bildern. Auf Foto-Portalen haben Nutzer Milliarden von Schnappschüssen eingestellt, um sie mit ihren Freunden zu teilen. Auch sehr private Bilder sind häufig für jedermann im Netz sichtbar – beispielsweise auch für den Personalchef der Firma, bei der man sich für einen Job bewirbt. In einer Studie des Bundesverbraucherschutzministeriums gab ein Viertel der befragten Unternehmen an, sie würden bei der Auswahl von Bewerbern gezielt Informationen aus dem Internet benutzen. Wenn da das Foto der letzten exzessiven Party auftaucht, ist das kein Pluspunkt.

Doch bislang findet man Fotos zu einer bestimmten Person nur, wenn die Bildunterschrift die Namen der Fotografierten verrät. Doch seit einiger Zeit arbeiten kommerzielle Anbieter daran, Gesichter automatisch zu erkennen und so auffindbar zu machen. Einer der führenden Experten für Gesichtserkennung in Deutschland ist Professor Volker Blanz von der Universität Siegen. Er arbeitet schon seit Jahren an der Perfektionierung dieser Technik und zeigt am Beispiel von Rangas Facebook-Foto, was die neue Technik schon alles kann – auf www.quarks.de.

Autor: Daniel Münter

Wenn die eigenen Daten fremdgehen

Wie bekomme ich meine Daten zurück?

Quarks & Co erzählt die Geschichte eines Kölner Jazz-Musikers, dessen eigene Daten im Netz benutzt werden, um ihn zu diffamieren. Bilder über sich, die er selber auf seiner Homepage eingestellt hat, werden verfremdet: Er wird lächerlich gemacht und beschimpft – und das auf unzähligen Seiten im Internet. Schließlich weiß er keinen anderen Rat mehr und wendet sich an eine Firma, die darauf spezialisiert ist, Daten aus dem Netz löschen zu lassen. Wird sie es schaffen, dass die verunglimpfenden Bilder wirklich aus dem Netz verschwinden? Sehen Sie den Film auf www.quarks.de.

Autor: Carsten Binsack

Wie Cyberkriminelle Kontodaten stehlen

Vorsicht vor Trojanern im Netz!

Es ist schon bedenklich, was Unternehmen wie Google, Apple oder Facebook über uns wissen. Doch richtig bedrohlich wird es, wenn Kriminelle Zugriff auf unsere Daten bekommen. Wenn sie unsere Bankdaten ausspionieren und uns ausrauben. Dazu nutzen sie sogenannte „Trojaner"-Programme.

Der Cybercrime-Spezialist Mirko Manske vom Bundeskriminalamt zeigt Quarks & Co, wie Kriminelle an unsere Daten kommen. Dabei geht es nicht „nur" um die Login-Daten für den persönlichen E-Mail-Account. Mirko Manske zeigt, wie schnell man alle wichtigen Daten sammeln kann, um eine ganze Identität zu stehlen. Damit kauft er erstmal eine neue Kamera – online natürlich. Sehen Sie jetzt, wie erschreckend einfach man auch selber Opfer eines solchen Identitätsdiebstahls sein kann. Der ganze Film zum anschaun auf www.quarks.de.

Autor: Mike Schaefer

Sicher durch die Datenwelt

Wie man Cookies löscht – und andere Tipps zur Datensicherheit

Cookies – ursprünglich eine geniale Idee

Manche Cookies sind „gutartig" und helfen zum Beispiel beim Einkauf im Internet. Doch nutzen Werbevermarkter Cookies auch, um maßgeschneiderte Werbung präsentieren zu können

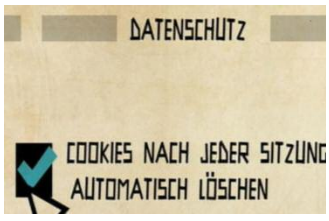
Cookies sind kleine Textdateien, die von Webseiten auf unserem Computer abgelegt werden. Cookies speichern persönliche Daten. Oft ist das sehr nützlich: beispielsweise, wenn Artikel im Warenkorb zwischengespeichert werden oder wenn auf der Wetter-Seite der Heimatort gespeichert bleibt, so dass beim nächsten Aufruf der Seite direkt die richtige Wettervorhersage angezeigt wird. Manchmal enthalten sie auch Informationen, die einen Nutzer mit einer Kennung identifizieren, damit eine Internetseite ihn wiedererkennt. In den kleinen, helfenden Textdateien auf unserem Computer hinterlegen Webseiten über den Browser Informationen, auf die sie bei einem späteren Besuch zurückgreifen können. Cookies sind im Internet sehr weit verbreitet. Bei einem normalen Nutzer sammeln sich jeden Tag Hunderte von Cookies an.

Peilsender der Werbeindustrie

Mit Hilfe von Cookies erstellen Werbevermarkter Nutzerprofile, wenn wir uns im Internet bewegen

Cookies sollten dem Internet ursprünglich eine Art Gedächtnis verleihen. Heute sind sie aber zu kleinen Peilsendern verkommen, die das „Aushorchen" von Surfern ermöglichen. Werbevermarktern dienen sie dazu, Nutzer zu identifizieren; ja sogar, um sie im Internet von Seite zu Seite zu verfolgen. Vorlieben ausspähen und den Computernutzer immer wieder mit der gleichen Art von Werbung bombardieren – dank engmaschiger Werbenetzwerke ist das kein Problem. Die Grundvoraussetzung dafür: zweckentfremdete Cookies, die nicht der angesteuerten Internetseite gehören, sondern von fremden Seiten kommen und dem User überhaupt nicht nutzen. In keinem Medium vor dem Internet ließ sich der einzelne Nutzer und potenzielle Konsument einfacher in eine Schublade stecken, kategorisieren und maßgeschneidert bewerben. Nutzerprofile oder komplizierte Marktanalysen helfen dabei, den möglichen Kundenstamm bis auf den letzten User mit vielversprechenden, genau platzierten Werbebotschaften zu erreichen.

Datenschutzeinstellung des Browsers anpassen



Einstellungen zum Datenschutz erlauben es, Cookies regelmäßig automatisch zu löschen

Die meisten Browser lassen sich so einstellen, dass sogenannte „3rd-Party-Cookies", also Cookies die von Dritten und fremden Webseiten erzeugt werden, nicht akzeptiert werden. Hinter ihnen verstecken sich oft Werbevermarkter. Die setzen beim Ansteuern von Internetseiten zusätzlich zu den Cookies der Seitenbetreiber ihre eigenen zu Werbezwecken ab. Durch das Ausschließen dieser Cookies im eigenen Browser werden sie daran gehindert. Die Cookies der angesteuerten Webseiten, die nützliche Informationen speichern, nimmt der Browser aber weiterhin an.

Zusätzlich ist es sinnvoll, alle Cookies, die sich auf dem Computer angesammelt haben regelmäßig zu löschen. Zwar gibt es heutzutage sogenannte Zombie-Cookies, die nach dem Löschen „wiederauferstehen" und sich selbst wiederherstellen. Die sind aber eher die Ausnahme. Mit dem Löschen von Cookies gelingt es oft, hartnäckige Verfolger endgültig abzuschütteln. Da das von Hand eine mühsame Angelegenheit ist, bieten Browser in den Einstellungen eine Funktion an, die dies automatisch übernimmt. Sobald der Benutzer das Programm schließt, wird jedes Mal die Festplatte automatisch von Cookies bereinigt.

Kleine Datenspur erschwert das Spionieren

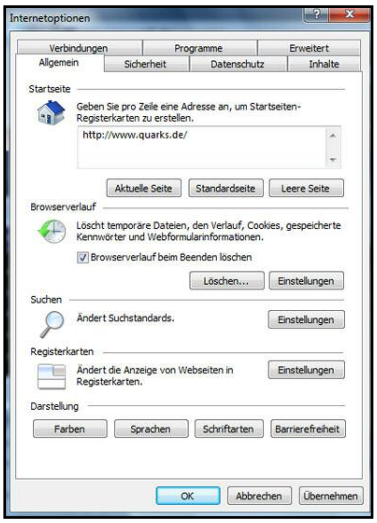
Ein Monate umfassendes, ausführliches Nutzerprofil und die Horrorvision des gläsernen und berechenbaren Kunden wird mit diesen angepassten Einstellungen verhindert. Das Ausspionieren wird mühsamer für die Werbeindustrie. Der einzige Nachteil dabei: Beispielsweise der Wohnort auf der Wetter-Seite oder der gespeicherte Einkaufswagen beim Online-Versand werden ebenfalls gelöscht. Doch diese Daten können in den meisten Fällen mit wenig Zeitaufwand beim nächsten Aufruf der Seite wieder eingeben werden.

Autor: Peter Gotzner

Wie Sie Ihren Browser einstellen müssen, um der lästigen Verfolgung durch Cookies im Internet zu entgehen, können Sie hier nachlesen.

Windows *Internet-Explorer*

Unter „Internetoptionen“ lässt sich der Umgang des Browsers mit Cookies bestimmen.



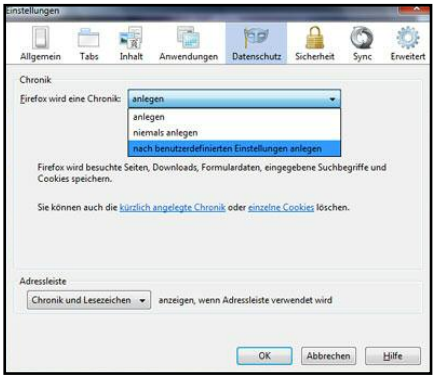
Um Cookies nach jedem Surfen automatisch zu löschen, muss im Register „Allgemein“ die Box bei „Browserverlauf beim Beenden löschen“ aktiviert sein.

Welche Cookies der Browser überhaupt akzeptieren soll, lässt sich im Register „Datenschutz“ durch Klick auf den Button „Erweitert“ einstellen.

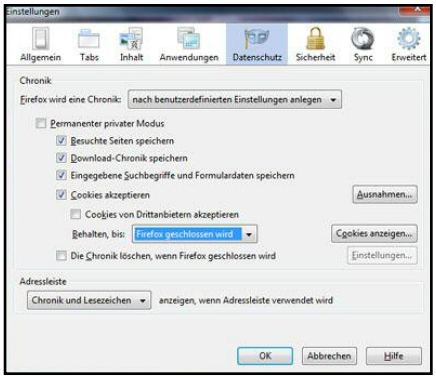
Nachdem man die „Automatische Cookiebehandlung“ in einer Box deaktiviert hat, schließt man 3rd-Party-Cookies von fremden Webseiten und Werbevermarktern mit einem Klick auf „Blocken“ aus.

Windows *Firefox*

Über das Firefox-Menü öffnet man durch Klick direkt das Einstellungsfenster. In älteren Firefox-Versionen ist das im Menü „Extras“ und dort unter „Einstellungen“ zu finden.



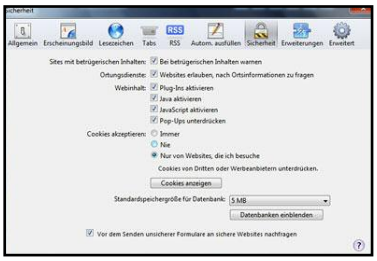
Im Register „Datenschutz“ kann man die „Chronik“, die Firefox anlegt, nach seinen Bedürfnissen anpassen. Darunter ist auch der Umgang des Browsers mit Cookies zu finden.



Um fremde 3rd -Party-Cookies von Werbevermarktern zu blockieren, muss die Box neben „Cookies von Drittanbietern akzeptieren“ deaktiviert sein. Das automatische Löschen von Cookies nach jeder Sitzung, steuert die Auswahl neben „Behalten, bis“. Mit einem Klick auf „Firefox geschlossen wird“ bereinigt der Browser den Computer von allen gespeicherten Cookies, sobald das Programm geschlossen wird.

Windows *Safari*

Beim Safari-Brwoser gelangt man durch Klick auf das Zahnrad am rechten, oberen Bildschirmrand und den Menüpunkt „Einstellungen“ zu den Cookie-Einstellungen.

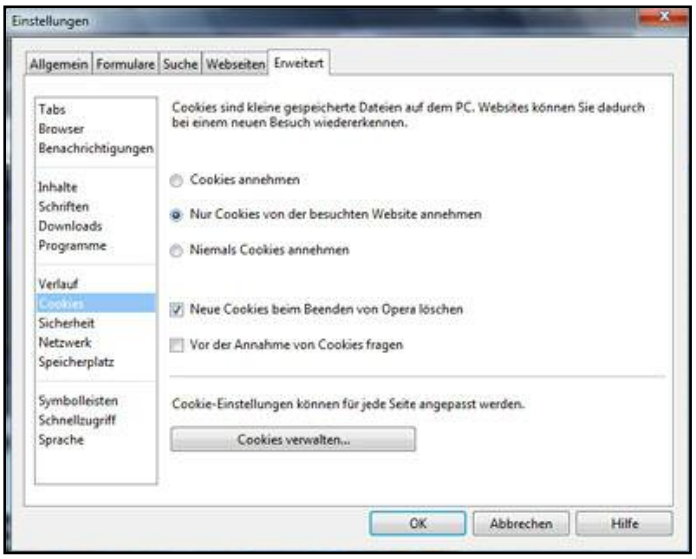


Im Register „Sicherheit“ kann man angeben, welche Cookies vom Browser akzeptiert werden sollen. Durch das Auswählen von „Nur von Websites, die ich besuche“ werden die 3rd-Party-Cookies der Werbevermarkter ausgeschlossen.

Leider bietet Safari standardmäßig keine Einstellung zum automatischen Löschen von Cookies nach Programmende an. Dies kann man entweder manuell erledigen durch den Menüpunkt „Safari zurücksetzen...“. Oder man verzichtet vollkommen auf Cookies: Im Einstellungsmodus „Privates Surfen...“ legt Safari keine Cookies an.

Windows *Opera*

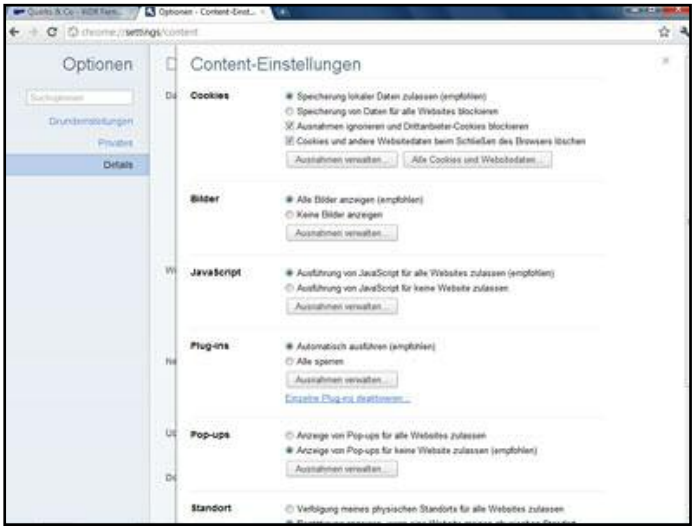
Im Menü von Opera findet sich die Cookie-Verwaltung unter „Einstellungen“ und noch mal „Einstellungen ...“.



Im Register „Erweitert“ unter dem seitlichen angezeigten Unterpunkt „Cookies“ lässt sich auswählen, dass „nur Cookies von der besuchten Website“ angenommen werden. Zusätzlich kann man mit einem Klick auf die Box neben „Neue Cookies beim Beenden von Opera löschen“ dafür sorgen, dass ab diesem Zeitpunkt keine dauerhaften, neuen Cookies angelegt werden. Vorhandene Cookies sind aber von dem Löschvorgang ausgeschlossen. Daher empfiehlt es sich, vor dem Aktivieren dieser Einstellung alle vorhandenen Cookies zu löschen. Die kann man durch Klick auf „Internetspuren löschen ...“ im Hauptmenü erledigen.

Windows *Chrome*

Durch Klick auf den Schraubenschlüssel im rechten, oberen Teil des Fensters erreicht man bei Chrome den Menüpunkt „Optionen“, hinter dem sich auch die Cookie-Einstellungen verbergen.



Über „Details“ im linken Bildrand gelangt man zum Punkt „Datenschutz“. Durch Klick auf „Content-Einstellungen“ (im Bereich „Datenschutz“) öffnet sich ein neues Fenster. Hier sollte man im oberen Teil neben „Cookies“ aktivieren: „Ausnahmen ignorieren und Drittanbieter-Cookies blockieren“. Dies verhindert die Speicherung von Werbevermarkter-Cookies. Zudem lassen sich alle Cookies automatisch nach Programmende löschen, wenn man die Box neben „Cookies und andere Websitedaten beim Schließen des Browsers löschen“ aktiviert.

MacOS *Firefox*

Über das Menü „Firefox“ öffnet man durch Klick auf „Einstellungen“ direkt das Einstellungsfenster

Im Register „Datenschutz“ kann man die „Chronik“, die Firefox anlegt, nach seinen Bedürfnissen anpassen. Darunter ist auch der Umgang des Browsers mit Cookies zu finden.

Um fremde 3rd -Party-Cookies von Werbevermarktern zu blockieren, muss die Box neben „Cookies von Drittanbietern akzeptieren“ deaktiviert sein. Das automatische Löschen von Cookies nach jeder Sitzung, steuert die Auswahl neben „Behalten, bis“. Mit einem Klick auf „Firefox geschlossen wird“ bereinigt der Browser den Computer von allen gespeicherten Cookies, sobald das Programm geschlossen wird.

MacOS *Safari*

Über das Menü „Safari“ gelangt man zu „Einstellungen“, hinter denen sich die Optionen des Browsers zum Umgang mit Cookies verbergen.

Im Register „Sicherheit“ kann man angeben, welche Cookies vom Browser akzeptiert werden sollen. Durch das Auswählen von „Nur von Websites, die ich besuche“ werden die 3rd-Party-Cookies der Werbevermarkter ausgeschlossen.

Leider bietet Safari standardmäßig keine Einstellung zum automatischen Löschen von Cookies nach Programmende an. Dies kann man entweder manuell erledigen durch den Menüpunkt „Safari zurücksetzen...“. Oder man verzichtet vollkommen auf Cookies: Im Einstellungsmodus „Privates Surfen...“ legt Safari keine Cookies an.

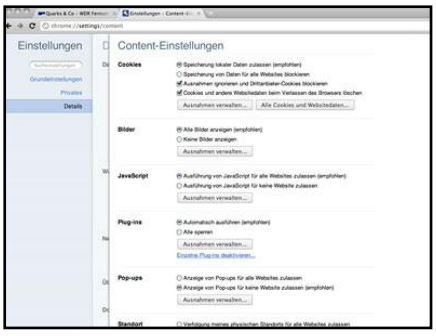
MacOS *Opera*

Über das Menü „Opera“ gelangt man durch Klick auf „Einstellungen“ zu den Einstellungsoptionen.

Im Register „Erweitert“ unter dem seitlichen angezeigten Unterpunkt „Cookies“ lässt sich auswählen, dass „nur Cookies von der besuchten Website“ angenommen werden. Zusätzlich kann man mit einem Klick auf die Box neben „Neue Cookies beim Beenden von Opera löschen“ dafür sorgen, dass ab diesem Zeitpunkt keine dauerhaften, neuen Cookies angelegt werden. Vorhandene Cookies sind aber von dem Löschvorgang ausgeschlossen. Daher empfiehlt es sich, vor dem Aktivieren dieser Einstellung alle vorhandenen Cookies zu löschen. Die kann man durch Klick auf „Internetspuren löschen ...“ im Hauptmenü erledigen.

MacOS *Chrome*

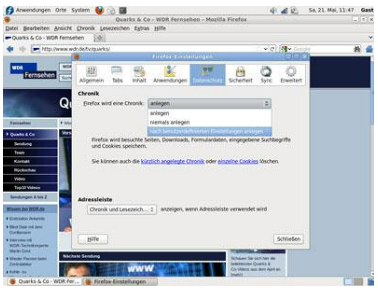
Über das Menü „Chrome“ gelangt man zu dem Unterpunkt „Einstellungen“, hinter denen sich die Optionen des Browsers zum Umgang mit Cookies verbergen.



Über „Details“ im linken Bildrand gelangt man zum Punkt „Datenschutz“. Durch Klick auf „Content-Einstellungen“ (im Bereich „Datenschutz“) öffnet sich ein neues Fenster. Hier sollte man im oberen Teil neben „Cookies“ aktivieren: „Ausnahmen ignorieren und Drittanbieter-Cookies blockieren“. Dies verhindert die Speicherung von Werbevermarkter-Cookies. Zudem lassen sich alle Cookies automatisch nach Programmende löschen, wenn man die Box neben „Cookies und andere Websitedaten beim Schließen des Browsers löschen“ aktiviert.

Linux *Firefox*

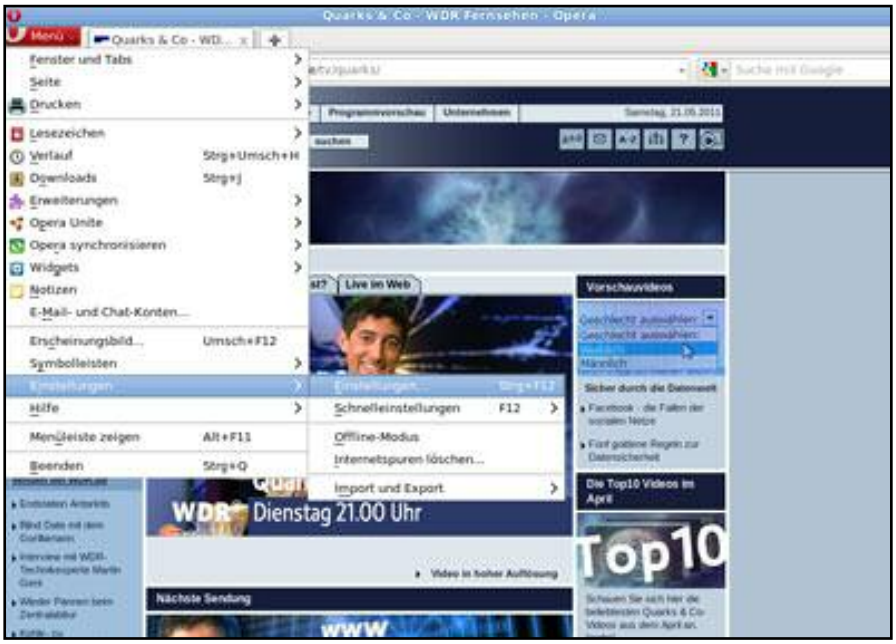
Das Einstellungsfenster bei Firefox öffnet man durch Klick auf das Menü „Bearbeiten“ und den Unterpunkt „Einstellungen“.



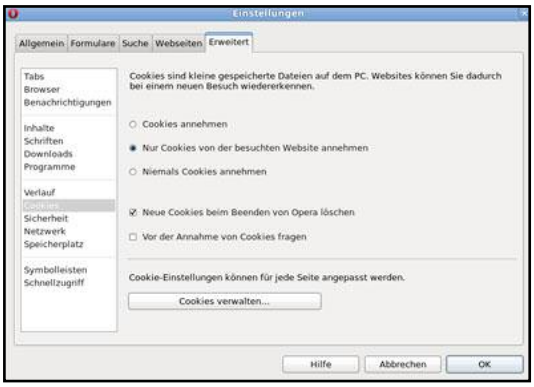
Im Register „Datenschutz“ kann man die „Chronik“, die Firefox anlegt, nach seinen Bedürfnissen anpassen. Darunter ist auch der Umgang des Browsers mit Cookies zu finden.

Um fremde 3rd -Party-Cookies von Werbevermarktern zu blockieren, muss die Box neben „Cookies von Drittanbietern akzeptieren“ deaktiviert sein. Das automatische Löschen von Cookies nach jeder Sitzung, steuert die Auswahl neben „Behalten, bis“. Mit einem Klick auf „Firefox geschlossen wird“ bereinigt der Browser den Computer von allen gespeicherten Cookies, sobald das Programm geschlossen wird.

Linux *Opera*



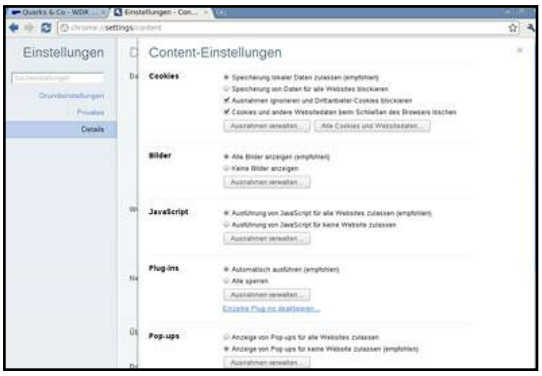
Im Menü von Opera findet sich die Cookie-Verwaltung unter „Einstellungen“ und noch mal „Einstellungen ...“.



Im Register „Erweitert“ unter dem seitlichen angezeigten Unterpunkt „Cookies“ lässt sich auswählen, dass „nur Cookies von der besuchten Website“ angenommen werden. Zusätzlich kann man mit einem Klick auf die Box neben „Neue Cookies beim Beenden von Opera löschen“ dafür sorgen, dass ab diesem Zeitpunkt keine dauerhaften, neuen Cookies angelegt werden. Vorhandene Cookies sind aber von dem Löschvorgang ausgeschlossen. Daher empfiehlt es sich, vor dem Aktivieren dieser Einstellung alle vorhandenen Cookies zu löschen. Die kann man durch Klick auf „Internetspuren löschen ...“ im Hauptmenü erledigen.

Linux *Chrome*

Durch Klick auf den Schraubenschlüssel im rechten, oberen Teil des Fensters erreicht man bei Chrome den Menüpunkt „Optionen“, hinter dem sich auch die Cookie-Einstellungen verbergen.



Über „Details“ im linken Bildrand gelangt man zum Punkt „Datenschutz“. Durch Klick auf „Content-Einstellungen“ (im Bereich „Datenschutz“) öffnet sich ein neues Fenster. Hier sollte man im oberen Teil neben „Cookies“ aktivieren: „Ausnahmen ignorieren und Drittanbieter-Cookies blockieren“. Dies verhindert die Speicherung von Werbevermarkter-Cookies. Zudem lassen sich alle Cookies automatisch nach Programmende löschen, wenn man die Box neben „Cookies und andere Websitedaten beim Schließen des Browsers löschen“ aktiviert.

Lesetipps

Die Facebook-Falle: Wie das soziale Netzwerk unser Leben verkauft

Autor: Sascha Adamek
Verlagsangaben: Heyne Verlag, 2011
ISBN-10: 3453601807
ISBN-13: 978-3453601802
Sonstiges: 352 Seiten, 16,99 Euro

Der WDR-Journalist Sascha Adamek beschreibt anschaulich und unterhaltsam, wie das Unternehmen Facebook uns mittlerweile in allen Bereichen des Internets über die Schulter schaut und welche negativen Konsequenzen dies haben kann.

Linktipps

Tipps zum Umgang mit Computer und Internet
http://www.verbraucher-sicher-online.de
Auf einer übersichtlich und freundlich gestalteten Website gibt die Technische Universität Berlin ausführliche Tipps zum Umgang mit Computern und dem Internet. Leicht verständlich und dennoch umfassend erklärt die vom Verbraucherschutzministerium gefördert Internetseite dabei Themen wie Datensicherheit und Grundwissen rund um den Computer.

Tipps für den Datenschutz
http://www.verbraucher-sicher-online.de/thema/soziale-netzwerke
Das Verbraucherschutzportal „Verbraucher Sicher Online", das vom Bundesministerium für Verbraucherschutz gefördert wird, gibt konkrete Tipps für den Datenschutz in sozialen Netzwerken.

Direktlink zum Löschen des Facebook-Profils
https://www.facebook.com/help/contact.php?show_form=delete_account
Wer sein Facebook-Profil löschen möchte, muss meist lange suchen, wo das geht. Mit diesem Link ist es ganz einfach: Klicken Sie auf den Link, loggen Sie sich dann bei Facebook ein und bestätigen per Mausklick, dass Ihr Facebook-Profil gelöscht werden soll.

Facebook allein macht nicht glücklich
http://www.uzh.ch/news/articles/2009/facebook-allein-macht-nicht-gluecklich.html
Zusammenfassung der Studie des Psychologischen Instituts der Universität Zürich zur Frage: Welche Persönlichkeiten nutzen Facebook und sind sie zufriedener als Nicht-Nutzer?

Wenn Facebook, dann richtig
http://www.einslive.de/multimedia/service/2010/11/facebook_privatsphaere.jsp
EinsLive erklärt ausführlich, welche Einstellungen man bei Facebook vornehmen sollte, um seine Privatsphäre zu schützen.

Lehrstuhl Medieninformatik der Universität Siegen
http://mi.informatik.uni-siegen.de/
Hompage des Lehrstuhls Medieninformatik der Universität Siegen, dem Professor Volker Blanz vorsteht. Verschiedene Projekte zur Gesichtserkennung und Modellierung von Gesichtern werden vorgestellt.

Ein Experte des Bundeskriminalamtes zum Thema Cyberkriminalität
http://www.teltarif.de/internet-handy-smartphone-sicherheit/news/40359.html
Interview mit Mirko Manske, Internetexperte beim Bundeskriminalamt, über neue Strategien von Cyberkriminellen, sich private Daten von Computernutzern zu verschaffen. Auch das Ausspähen von Smartphones durch Kriminelle könnte demnach zu einem wachsenden Risiko werden.

Tyrannei der Intimität? Über die Geschichte des Privaten im Öffentlichen
http://www.medienheft.ch/uploads/media/
12_13_ZOOM_KM_10_Kurt_Imhof_Tyrannei_der_Intimitaet.pdf
Seit den 1950er-Jahren bis Anfang 2000. Eine Untersuchung anhand der schweizerischen Medien. (PDF, 10 Seiten)

Impressum:

Herausgegeben
vom Westdeutschen Rundfunk Köln

Verantwortlich:
Quarks & Co
Claudia Heiss

Redaktion:
Monika Grebe

Gestaltung:
Designbureau Kremer & Mahler