AGF Arbeitsgemeinschaft der deutschen Familienorganisationen e.V.

Die Einstellung macht's:

Werbung und Privatsphäre im Internet

November 2012

Mit freundlicher Genehmigung der Confederation of Family Organisations in the European Union (COFACE) dient ihr Aufsatz „Behavioural advertising and privacy: browsers can help“, verfasst von Martin Schmalzried, als Basis für diese Broschüre.

Herausgeberin:
Arbeitsgemeinschaft der deutschen Familienorganisationen e.V. (AGF)

Redaktion:
Sven Iversen (Leitung), Lars Vogelsang, Silka Riedel, Ariann Weinmann

Bildnachweise:
@pete pahham - Fotolia.com
@contrast werkstatt - Fotolia.com
@rubysoho - Fotolia.com

Layout & Satz:
manuka.p.r

Die Einstellung macht´s: Werbung und Privatsphäre im Internet

Viele Internetnutzer(innen) empfinden Online-Werbung als störend und haben gelernt, herkömmliche Anzeigen und Banner zu ignorieren. Umso mehr versucht der Werbemarkt sicherzustellen, dass seine Botschaften ankommen. Kostenlose und frei zugängliche Inhalte wie Videos, Wettervorhersagen oder Zeitschriftenartikel werden den Konsument(inn)en zunehmend erst nach einer „Werbepause" zur Verfügung gestellt.

Online-Werbung hat in den letzten Jahren stark zugenommen und ist allein 2010 um 15,3 % gestiegen. In Europa wurden dafür 17,7 Milliarden Euro ausgegeben (Quelle: IAB Europe).

Zudem wird die Online-Werbung an das Verhalten der einzelnen Nutzer(innen) angepasst. Produkte können so zielgerichtet beworben werden, während die Internetnutzer(innen) gleichzeitig weniger belästigt werden. Bedenkt man jedoch den Umfang an privaten Informationen, der gesammelt werden muss, um Personen gezielt mit Werbung zu erreichen, erscheint dieses individualisierte Marketing weniger positiv.

Wie werden persönliche Informationen gesammelt?

Tracking (d.h. Nutzer(innen)verfolgung im Internet) mit Hilfe von Cookies: Cookies sind Dateien, die von Websites automatisch auf dem Computer der Nutzer(innen) abgelegt werden. Sie können dazu dienen, Bewegungen und Klicks aufzuzeichnen, um so das Besucher(innen)verhalten zu verfolgen.

Über soziale Netzwerke wie z. B. Facebook können Unternehmen viele private Informationen für gezielte Werbung nutzen: Name, Alter, Aufenthaltsort, Freunde, Interessen und Vorlieben.

Kinder im Visier

Individualisierte und verhaltensbezogene Werbung kann weitere Nachteile haben. Oft werden Computer von mehreren Familienmitgliedern genutzt. Wenn nicht jedes Familienmitglied ein separates Benutzerkonto hat, werden Cookies und die Liste der besuchten Seiten (Browserverlauf) automatisch gemeinsam aufgezeichnet. So erhalten Kinder die Werbung, die für ihre Eltern gedacht ist.

Trotz vieler Bemühungen, jüngere Kinder von sozialen Netzwerken fernzuhalten, zeigt sich, dass immer mehr Kinder dieser Altersgruppe eigene Konten haben. Die Praxis der Werbeindustrie, die Online-Aktivitäten von Kindern zu verfolgen und Daten über sie zu sammeln, wirft ernste Fragen zur Ethik und Privatsphäre auf.

Wenn soziale Netzwerke erklären, dass keine persönlichen Informationen über die Nutzer(innen) weitergegeben werden, wird meist der umgekehrte Weg gegangen. Die werbenden Unternehmen liefern eine Beschreibung ihrer Zielgruppe (Alter, Geschlecht, Interessen, Ort etc.) an die sozialen Netzwerke, die die Werbung an das entsprechende Publikum weiterleiten.

Infolgedessen wird ein Kind, das z. B. eine bestimmte Schokoladensorte mag, der Werbung mit Produkten genau dieser Firma ausgesetzt - maßgeschneidert nach Alter, Geschlecht, Ort etc. Ein Kind, das Informationen über die eigenen Interessen bereitstellt, liefert die Basis für gezielte Werbung.

Weniger Werbung? Lösungen!

Im Folgenden werden Möglichkeiten vorgestellt, wie sich Internetnutzer(innen) vor Tracking schützen und Werbung blockieren können. Diese Informationen erleichtern interessierten Eltern die Wahl und Nutzung der entsprechenden Funktionen. Alle hier beschriebenen Werkzeuge sind frei erhältlich.

Die Wege, die schnell umsetzbar sind, schränken die Nutzung des Internets oft deutlich ein. Passgenauere Maßnahmen hingegen bedeuten oft einen erheblichen Mehraufwand wie z. B. ein Zusatzprogramm zu installieren oder die Listen gesperrter Seiten ständig zu aktualisieren. Die perfekte Lösung gibt es nicht. Somit müssen Eltern abwägen, welche Vorgehensweise aus ihrer Sicht die beste ist.

Die meisten Einstellungen in den Browsern erfolgen im Menü unter „Einstellungen", „Optionen" oder „Extras", die in vielen neuen Browsern oft nur mit Symbolen wie  oder  gekennzeichnet sind.

Der folgende Überblick umfasst die am häufigsten genutzten Browser: Mozilla Firefox, Internet Explorer, Google Chrome sowie Safari.

Anonymes Surfen

Hierbei wird ein spezieller „Proxy-Server" zwischengeschaltet, der als Vermittler zu den besuchten Websites fungiert und die Weitergabe individueller Daten unterbindet. Nachteile bestehen in einer gewissen Zeitverzögerung sowie in Einschränkungen bei solchen Internetpräsenzen, die Cookies z. B. zum Einloggen erfordern. Kostenlose Beispiele hierfür sind Anonymouse.org oder Proxify.com. Eine anonyme Suchmaschine auf Google-Basis bietet Startpage.com.

Ein weiterer Nachteil des anonymen Surfens liegt darin, dass die Nutzung oft vergessen wird. Insbesondere bei Kindern kann dies vorkommen, auch wenn im Browser eine Website für anonymes Surfen als Startseite festgelegt wurde. Es gibt keine Browsereinstellung, mit der sich verhindern lässt, dass ohne Anonymisierung gesurft wird.

Alle Webbrowser haben Einstellungsmöglichkeiten, die einen gewissen Schutz der Privatsphäre und somit vor individualisierter Werbung bieten. Allerdings schränken auch sie den Komfort beim Surfen oder die Funktionsweise mancher Internetseiten ein.

Festlegen der Startseite

Mozilla Firefox
Extras → Einstellungen → Allgemein

Internet Explorer
Extras → Internetoptionen → Allgemein

Google Chrome
Optionen → Grundeinstellungen

Safari
Einstellungen → Allgemein

Cookies ablehnen

Cookies sind kleine Datenpakete, die eine besuchte Website an den Browser sendet. Dieser speichert sie auf der Festplatte der Nutzerin oder des Nutzers. Es ist jedoch möglich, das Speichern von Cookies zu beeinflussen oder zu untersagen.

Ein Browser kann so eingestellt werden, dass er Cookies entweder ablehnt oder dass er fragt, ob er

Ablehnen von Cookies

Mozilla Firefox
Extras → Einstellungen → Datenschutz

Internet Explorer
Extras → Internetoptionen → Datenschutz → Einstellungen → Schieberegler verschieben → ok

Google Chrome
Einstellungen → Optionen → Details → Inhaltseinstellungen

Safari
Einstellungen → Datenschutz

sie ablehnen oder speichern soll. Auf diese Weise lernt der Browser, bei welchen Websites Cookies erlaubt sind. Bei einem erneuten Besuch der Seite fragt er nicht mehr nach. Zu beachten ist, dass manche Websites ohne Cookies nicht richtig funktionieren. Das gilt für alle Websites zum Einloggen: Online-Banking, Online-Shops und Auktionsplattformen, soziale Netzwerke sowie viele Diskussionsforen. Für solche Internetpräsenzen sollten Cookies zugelassen werden. Die meisten Cookies jedoch dienen nur dem Tracking.

Nur wenige Internetpräsenzen weisen ihre Besucher(innen) darauf hin, wenn ein abgelehntes Cookie für eine bestimmte Funktion nötig ist. Dann ist nicht ersichtlich, warum die Website nicht richtig funktioniert. Google Chrome bzw. Chromium zeigt in der Adressleiste ein entsprechendes Symbol an, wenn Cookies abgelehnt wurden. Per Klick auf das Symbol kann die Nutzerin oder der Nutzer angeben, dass diese Website künftig Cookies speichern darf. Mit einem ähnlichen Ansatz arbeiten einige kleine Zusatzprogramme (Add-ons) für Mozilla Firefox.

Eine weitere Option besteht darin, Cookies zwar zuzulassen, sie aber nur bis zum Ende der Computersitzung speichern zu lassen. Anschließend werden die Cookies automatisch gelöscht. Eine Website kann diesen Computer danach nicht mehr „wiedererkennen“. Hat die Nutzerin oder der Nutzer bestimmte Einstellungen vorgenommen, gehen diese zwar verloren; aber auch Trackingdienste haben es sehr viel schwerer, Informationen einem speziellen Nutzerprofil zuzuordnen. Fazit: Oft wird diese Option ein guter Kompromiss sein.

Privatmodus einschalten

Alle Browser bieten für das Surfen im Netz einen privaten Modus. Hier werden Cookies ebenfalls nicht permanent gespeichert. Die weiteren Eigenschaften des Privatmodus dienen hauptsächlich dazu, gegenüber anderen Nutzer(inne)n desselben Computers zu verbergen, welche Seiten besucht wurden.

Privatmodus aktivieren

Mozilla Firefox
Extras → Einstellungen → Datenschutz bzw.
Extras → Privaten Modus starten

Internet Explorer
Extras → Sicherheit → InPrivate-Browsen

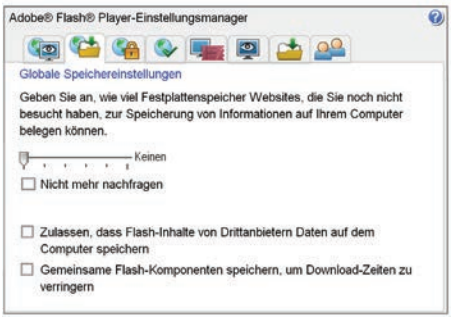
Google Chrome
Optionen → Inkognito

Safari
Einstellungen → Privates Surfen

Flash-Cookies abschalten

Flash-Cookies sind eine besondere Art von Cookies, die von dem Browser-Plug-in „Flash“ gespeichert werden, welches für Videofilme und Animationen benutzt wird. Zumindest bei Mozilla Firefox werden im Privatmodus auch keine Flash-Cookies gespeichert. Die eigene Flash-Cookies können unter folgenden Links verwaltet werden:

Globale Speichereinstellungen



- Ansehen und Löschen bereits bestehender Flash-Cookies: www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager07.html
- Ablehnen künftiger Flash-Cookies: www.macromedia.com/support/documentation/de/flashplayer/help/settings_manager03.html

Keine Grafiken zwischenspeichern

Neben den normalen Cookies und den Flash-Cookies werden auch kleine Grafikdateien als „Super-Cookies“ eingesetzt. Normalerweise speichert ein Computer die Grafiken der besuchten Internetpräsenzen für eine gewisse Zeit.

Wird dieselbe Website erneut besucht, erfolgt der Seitenaufbau dadurch schneller. Umgekehrt erkennt jedoch auch die Website den Computer wieder. Zu diesem Zweck werden für jede(n) Besucher(in) winzige individuelle Grafiken erzeugt und gespeichert. Solche Super-Cookies lassen sich vermeiden, indem im Browser der Zwischenspeicher für Grafiken abgeschaltet wird. Der Seitenaufbau ist dann etwas langsamer, aber die Verfolgung wird dadurch wirksam reduziert.

Google Chrome bietet diese Möglichkeit nicht an. Hier kann der Grafik-Cache nur manuell gelöscht werden.

Ablehnen der Zwischenspeicherung von Grafiken

Mozilla Firefox
Extras → Einstellungen → Erweitert → Netzwerk → Häkchen bei „Automatisches Cache Management ausschalten“ und (!) Cache auf 0 MB

Javascript abschalten

JavaScript ist eine einfache Programmiersprache, die von vielen Internetpräsenzen benutzt wird, insbesondere für interaktive Funktionen – einschließlich Tracking. Das Abschalten von JavaScript hilft wirkungsvoll gegen verhaltensbezogene Werbung, kann aber auch zu unerwünschten Funktionseinschränkungen einer Website führen. Erfreulicherweise erscheint zum Beispiel auf eBay ohne JavaScript keinerlei Werbung. Artikel können jedoch weiterhin ersteigert werden. Bei Facebook hingegen wird ohne JavaScript die Zeitlinie nicht angezeigt. Die Nutzerin oder der Nutzer erhält meist keinen Hinweis, dass etwas fehlt. Google Chrome zeigt dies mit einem kleinen Symbol in der Adressleiste an, mit dem JavaScript für diese spezielle Website oder allgemein wieder eingeschaltet werden kann. Der Browser merkt sich, für welche Websites JavaScript erlaubt ist. Mozilla Firefox bietet dafür das Zusatzprogramm NoScript an.

Fazit: Die Deaktivierung von JavaScript ist ein wirkungsvolles Mittel mit großen Nebenwirkungen, das beim Surfen ein überdurchschnittliches technisches Verständnis erfordert.

Deaktivierung von JavaScript

Mozilla Firefox
Extras → Einstellungen → Inhalt → kein Häkchen bei „JavaScript aktivieren“

Internet Explorer
Extras → Einstellungen → Inhalt → kein Häkchen bei „JavaScript aktivieren“

Google Chrome
Einstellungen → Optionen → Details → Inhaltseinstellungen

Safari
Einstellungen → Sicherheit

Browserspezifische Möglichkeiten

1. Mozilla Firefox

Mozilla Firefox war der erste Browser, der die Funktion „Do Not Track“ (DNT) optional bereitgestellt hat, die Tracking verhindern soll. Ist die DNT-Funktion aktiv, fordert der Browser alle besuchten Websites per Signal auf, Tracking von weiteren Websites (Third-Party Websites, z. B. Anzeigen) abzuschalten.

Diese Methode wird von der Kartellbehörde der USA gefördert und hat dadurch an Bedeutung gewonnen. Das System ist einfach und könnte in Zukunft ver-

DNT-Funktion aktivieren

Mozilla Firefox
Extras → Einstellungen → Datenschutz → Verfolgung → Häkchen bei „Websites mitteilen, dass ich nicht verfolgt werden möchte“

mehrt zu rechtlichen Konsequenzen für die Websites führen, die das DNT-Signal nicht respektieren.

Noch ignorieren die meisten Websites jedoch das DNT-Signal, seine Funktion ist daher abhängig vom Willen der Betreiber. Das DNT-System bietet somit gegenwärtig keinen umfassenden Schutz.

Zusatzprogramme (Add-ons und Extensionen)

Mozilla Firefox hat noch einen weiteren Pluspunkt: Zusatz- und Erweiterungsmöglichkeiten, die verhältnismäßig einfach in den Browser eingebaut werden können. „Adblock Plus“ ist z. B. eine häufig genutzte Erweiterung, um Werbung zu blocken.

Es gibt jedoch einen wichtigen Unterschied zwischen Adblock- und Tracking-Schutz: Werbeblocker können das Erscheinen von Werbung im eigenen Browser verhindern, nicht aber das Sammeln von Informationen.

Add-ons im Browser

Mozilla Firefox
Extras → Add-ons
Add-ons auf der Mozilla-Website: https://addons.mozilla.org/de/firefox/

2. Internet Explorer

Zusätzlich zum DNT-System bietet der Internet Explorer eine „Tracking Protection List“ zum Schutz vor Werbung und Verfolgung. Microsoft stellt dabei jedoch keine Liste zur Verfügung, sondern fordert dazu auf, entweder eine der Listen von der Microsoft Website zu wählen oder andernorts eine Liste zu suchen, die den eigenen Ansprüchen gerecht wird. Im Grunde könnte jeder so eine Liste selbst erstellen.

So ist z. B. die „EasyList“ sehr umfangreich und blockt die meisten Websites, während z. B. die „TRUSTe“ eine „Erlaubt-Liste“ ist, die in verschiedenen Bewertungen scharf kritisiert wurde.

Microsoft hat den Internet Explorer so konfiguriert, dass für den Fall, dass zwei Listen installiert wurden und eine Website nur in der einen Liste erlaubt ist, sich automatisch das „Erlaubt-Signal“ durchsetzt. Fazit: Der Umgang mit TPL erfordert ein gewisses Maß an Aufmerksamkeit und Fachkenntnis.

Track Protection List aktivieren

Internet Explorer
Extras → Sicherheit → Tracking-Schutz

3. Google Chrome

Google bietet zu seinem Browser eine Erweiterung (Plug-in) namens „Keep My Opt-Outs“, die ebenfalls mit einer „Block-List“ arbeitet. Dieses Programm bietet einfach und schnell Schutz und wirkt derzeit effektiver als das DNT-System, welches trotz Kritik der US-Kartellbehörden von Google selbst nicht unterstützt wird.

Allerdings beinhaltet die Liste dieser Erweiterung wesentlich weniger Einträge als beispielsweise die Listen, die von Adblock Plus bei Mozilla Firefox oder vom Internet Explorer für die Tracking Protection List genutzt werden.

Über weitere Zusatzprogramme (z. B. „Keep MORE Opt-Outs“) können die Nutzer(innen) den Schutz vergrößern und ihren eigenen Wünschen anpassen.

Überblick

Maßnahme	Aufwand
Anonym surfen	Evtl. Startseite im Browser einstellen, über eine andere Webseite (Proxyserver) surfen
DNT-Signal aktivieren	Browser-Funktion einschalten
Grafik-Zwischenspeicher abschalten	Browser-Funktion einschalten
Cookies nicht permanent speichern lassen (oder Privatmodus einschalten)	Browser-Funktion einschalten
Cookies manuell selektieren	Browser-Funktion einschalten und anfangs viele Fragen beantworten
Cookies immer ablehnen	Browser-Funktion einschalten
Javascript abschalten	Browser-Funktion einschalten und häufiges Ein- und Ausschalten
Add-on, Extension, Plugin oder TPL installieren	Zusatzprogramm/Blacklist installieren
Alternatives Flash-Plugin	Plugin installieren
Flash-Cookies verwalten	Einstellung vornehmen

Browser	Nachteil	Vorteil/Wirkung
alle	Verlangsamt das Surfen	Verhindert Tracking weitgehend
Firefox **Internet Explorer**	Derzeit kein umfangreicher Schutz	Kann zukünftig Tracking verhindern
Firefox **Internet Explorer**	Seitenaufbau langsamer	Stoppt jedes Tracking durch grafische Super-Cookies
alle	Websites merken sich keine Optionen (z.B. Sprachauswahl)	Erschwert langfristiges Tracking
alle	Funktionseinschränkung bei zu restriktiver Auswahl	Erschwert kurz- und langfristiges Tracking
alle	Funktionseinschränkung insbesondere bei Login-Seiten	Erschwert kurz- und langfristiges Tracking
alle	Funktionseinschränkung bei vielen Seiten	Erschwert kurz- und langfristiges Tracking
Firefox **Internet Explorer** **Chrome**	Auswahl bzw. Aktualisierung der Liste nötig	Stoppt Tracking durch Drittanbieter weitgehend
alle		Stoppt jedes Tracking durch Flash-Cookies
alle		Stoppt jedes Tracking durch Flash-Cookies

Obwohl die Maßnahmen effektiven Nutzen bringen, sollten deren Grenzen im Blick behalten werden:

1. Das DNT-System ist davon abhängig, dass alle Websites das Signal erkennen und respektieren. Es wird noch einige Zeit dauern, bis es sich umfangreich durchgesetzt hat.

2. Blockierungslisten müssen fortlaufend aktualisiert und geprüft werden. Außerdem muss sichergestellt sein, dass die gewählte Liste die richtige ist, denn einige Unternehmen stellen Listen zur Verfügung, die Tracking und Werbung ausdrücklich erlauben.

3. Die Signale zum Tracking-Schutz funktionieren nicht, wenn eine Website besucht wird, die direkt mit Tracking arbeitet wie z. B. Google oder Facebook. Der Schutz bezieht sich nur auf dritte Parteien (externe Websites).

4. Ein sehr restriktiver Tracking-Schutz limitiert gleichzeitig die Internet-Nutzungsmöglichkeiten. Soziale Netzwerke wie Facebook, Google+ oder Twitter verfolgen Internet-Aktivitäten über einen „like", „+1" oder „Tweet"-Button. Wird diese Möglichkeit deaktiviert, können Share-Funktionen bei Zeitschriften oder Videos nicht mehr wie bisher genutzt werden. Das Gleiche gilt für eingebaute Karten z. B. bei „Google Maps". Auch sie haben einen doppelten Zweck: Sie zeigen die Karten an und dienen gleichzeitig dem Tracking.

Zusammenfassung

Mozilla Firefox, Google Chrome und Internet Explorer bieten jeweils verschiedene Möglichkeiten, um Werbung zu blockieren und vor Tracking zu schützen.

Ein positiver Aspekt dabei ist, dass dadurch das Bewusstsein der Konsument(inn)en wesentlich steigt. Eltern, die sich um die Privatsphäre ihrer Kinder sorgen, sollten in ihrem Browser eine Startseite für anonymes Surfen einrichten, Cookies nur selektiv oder zeitlich begrenzt zulassen bzw. den Privatmodus aktivieren, den Zwischenspeicher für Grafiken abschalten und/oder Tracking-Schutz und Adblocking installieren. Sofern vorhanden, sollten DNT und gleichzeitig Blocklists/TPLs aktiviert sein, da sie gut zusammenarbeiten. Diese Maßnahmen sind insbesondere für jüngere Kinder wichtig, um sie vor immer aufdringlicherer Werbung und vor Tracking zu schützen.

Den achtsamen Blick und die Zuwendung der Eltern kann jedoch keine Technik ersetzen. Damit Kinder sich ein sicheres Internet-Verhalten aneignen und gute Erfahrungen mit diesem Medium machen können, ist es wichtig, kritische Denkweisen zu fördern und die Achtsamkeit für die eigene Privatsphäre zu schulen.

Weiterführende Links:

www.datenschutzzentrum.de
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (Anstalt des öffentlichen Rechts)

www.datenschutz.de/feature detail/?featid=8
Datenschutz bei Kindern (Virtuelles Datenschutzbüro des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein)

www.surfer-haben-rechte.de
Verbraucherzentrale Bundesverband

www.klicksafe.de
EU-Initiative für mehr Sicherheit im Netz

www.verbraucher-sicher-online.de
Projekt der TU Berlin, um Verbraucher(innen) u.a. über sichere Internetnutzung zu informieren

www.coface-eu.org/en/Policies/Education-ICT/Safer-Internet/
Informationen der Confederation of Family Organisations in the European Union (COFACE) zum Thema (auf Englisch).

AGF Arbeitsgemeinschaft der deutschen Familienorganisationen e.V.

Kontakt und Information:

AGF e.V.
Courbièrestr. 12
10787 Berlin
www.ag-familie.de

Fon: +49(0)30-21962-513
Fax: +49(0)30-21962-638
info@ag-familie.de

Die AGF wird gefördert vom

Bundesministerium für Familie, Senioren, Frauen und Jugend