eBlocker GmbH

21.11.2017 – 09:45 Uhr

Keine Angst vor dem Internet: Sieben Tipps, mit denen Sie viel sicherer surfen

---

Weitere Informationen
http://ots.de/Ql7li

Hamburg (ots) -

- Querverweis: Bildmaterial ist abrufbar unter
http://www.presseportal.de/pm/128614/3793571 -

Sieben Tipps zum sorglosen Surfen im Internet Schutz vor Trickbetrügern und Hackern: Dank dieser Ratschläge sind Sie sicher online unterwegs

Begleitet Sie beim Surfen im Internet nicht auch immer so ein merkwürdiges Gefühl der Angst? Die Angst davor, was man überhaupt noch anklicken darf. Denn auf fast jeder Internetseite lauern Viren und andere Schädlinge - und man erhält E-Mails, vermeintlich von der eigenen Bank mit der Aufforderungen, die PIN zu ändern oder sogar TANs herauszugeben. Zudem wird man überall von störenden Werbebannern verfolgt. Nur ein Beispiel: Wenn Sie nach Mitteln gegen Haarausfall suchen, zeigt Ihnen Ihr Internetbrowser kurze Zeit später häufig Werbung rund um Treppenlifte und Potenzmittel. Doch das ist nur das offensichtliche und oberflächliche Problem. Denn wenn Sie sich nicht schützen, lassen Sie bei jedem Ausflug ins Internet sprichwörtlich die Datenhose herunter. Und gefährlich ist es obendrein.

Spionage bei jedem Internet-Besuch

Was nur Experten wissen: Beim Surfen werden Sie unauffällig und permanent auf Schritt-und-Tritt verfolgt. Zahlreiche Datensammler (sog. Tracker) beobachten jede Aktion auf jeder von Ihnen besuchten Seite - egal, welches Gerät Sie verwenden. Wie Detektive, die Sie überall hin verfolgen, Ihnen über die Schulter lugen und alles haarklein aufschreiben - von der Bewegung der Maus bis hin zu Eingaben in Online-Formularen. Diese Mini-Schnüffler tragen allerdings keinen Trenchcoat, sondern verstecken sich in unsichtbaren Bildern im Hintergrund. Ihr Auftrag lautet, Sie auszuspionieren und fleißig Informationen an Datensammler zu liefern. Denn die verdienen mit Ihren Daten bares Geld: Zwischenhändler sammeln Nutzerprofile, reichern sie an, schnüren sie zu großen Paketen und verkaufen sie weiter. Sei es Ihr finanzieller Status, wie es um Ihre Gesundheit bestellt ist oder welche Partei Sie wählen: All diese persönlichen und sensiblen Daten landen in Ihrem Nutzerprofil.

Die besten 7 Tipps für mehr Privatsphäre im Web

Die gute Nachricht: Sie können sich schützen. Wenige Maßnahmen genügen, um schnüffelnden Unternehmen einen Strich durch die Rechnung zu machen, Ihre Privatsphäre zu schützen und Gefahren generell abzuwehren. eBlocker gibt die besten Tipps, damit Sie sorgenfrei im Internet unterwegs sind:

Tipp 1: Mehrere Internetbrowser einsetzen

Verwenden Sie für Ihre täglichen Ausflüge und Suche im Internet unterschiedliche Internetbrowser. Browser sind Computerprogramme zur Darstellung von Webseiten im Internet. Den einen Browser nutzen Sie am besten für Dinge, für den Sie Ihren echten Namen verwenden müssen, also zum Beispiel zum Einkaufen im Internet, Online-Banking, Cloud-Dienste und soziale Netzwerke. Der andere kommt dann für anonyme Aufgaben, wie auf Seiten stöbern und Web-Recherchen, zum Einsatz. Auf diese Weise entkoppeln Sie eine große Datenmenge von Ihrer Person auf einen Browser und machen Datensammlern das Leben viel schwerer. Legen Sie sich dazu in beiden Browsern am besten Lesezeichen für die jeweiligen Seiten an und zwar auf allen Geräten, mit denen Sie ins Internet gehen. Nach einer kurzen Eingewöhnungsphase haben Sie sich schnell an das duale System gewöhnt.

Tipp 2: Auf die richtigen Browser setzen

Immer mehr Internet-Nutzer nutzen den Internetbrowser Chrome, wenn es um Ausflüge ins weltweite Datennetz geht. Aus Datenschutzsicht ist dieser Browser allerdings mit Vorsicht zu genießen. Denn Google legt ein Surfprofil des Chrome-Nutzers an, wenn dieser ein Google-Konto in Chrome verwendet, zum Beispiel zur Aktivierung eines Android-Gerätes. Schließlich besteht Googles Geschäftsmodell nun einmal darin, Nutzerdaten zu sammeln und daraus Profit zu schlagen. Es gibt aber Alternativen: Zum Beispiel den Browser Firefox. Hinter dem steckt - im Gegensatz zu Chrome und Microsofts Edge - eine gemeinnützige Organisation und kein profitorientiertes Unternehmen, das scharf auf Nutzerdaten ist. Obendrein hat der Browser in letzter Zeit technisch aufgeholt. Und mit Version 57, die in Kürze erscheint, peilen die Entwickler einen weiteren großen Schritt hin zu mehr Geschwindigkeit und besserer Bedienung an. Besseren Datenschutz als Chrome bietet überdies "Chromium", ein von Google-Diensten befreiter Chrome-Klon.

Tipp 3: Google-Suche verbannen

Es muss nicht immer Google sein. Es gibt schließlich zahlreiche Suchdienste, die die Suchbegriffe ihrer Nutzer nicht speichern und auswerten. Gute Empfehlungen sind zum Beispiel www.startpage.de und www.metager.de. Startpage liefert beispielsweise genauso gute Treffer wie Google, übermittelt dabei nicht Ihre persönlichen Nutzerdaten. Auch die Suchmaschine www.DuckDuckGo.com setzt auf verschiedene Maßnahmen, um Ihre Privatsphäre im Internet zu wahren. So verspricht der Dienst, komplett aufs Sammeln von persönlichen Nutzerdaten zu verzichten, weder Cookies noch Standortdaten zu erfassen und Suchbegriffe nicht an die Seitenbetreiber weiterzugeben. Dadurch soll es für angeklickte Seiten nicht möglich sein, herauszubekommen, nach was Sie gesucht haben. DuckDuckGo können Sie in Firefox sogar als Standardsuchmaschine einsetzen: Klicken Sie dazu in Firefox oben rechts auf und dann auf Suche. Klicken Sie im Abschnitt "Standardsuche" auf Google und dann im Aufklappmenü auf DuckDuckGo.

Tipp 4: Schützen Sie sich vor gefährlichen E-Mails

Vermeintliche Gewinne, Mahnungen für Rechnungen oder Erinnerungen, das Passwort zu ändern: Solche E-Mails bringen Ihr Postfach zum Überquellen und kommen in der Regel von Trickbetrügern. Die Ideen der sog. "Phishing-Mafia" kennen dabei keine Grenzen. Mit Phishing-Mails wollen Online-Diebe wortwörtlich Ihre Anmeldedaten "angeln", etwa vom Online-Bankkonto. Das Gefährliche hierbei: Sie lassen sich von "echten" Nachrichten kaum noch unterscheiden. Dazu versenden die Kriminellen gefälschte E-Mails, die so aussehen, als kämen sie etwa direkt von Ihrer Bank oder einem Bezahldienst, wie beispielsweise PayPal. Darin versuchen die Betrüger, Sie auf gefälschte Internetseiten zu locken, auf denen Sie dann "zur Überprüfung" Kontonummern, Passwörter, PINs oder Transaktionsnummern (TANs) eintippen sollen. Tappen Sie in die Falle, räumen die Betrüger das Konto ab oder gehen damit auf Shopping-Tour. Tipp: Gehen Sie einfach davon aus, dass Banken, Bezahldienste und andere Unternehmen schlicht und ergreifend niemals nach Passwörter, Anmeldedaten oder anderen persönlichen Daten per E-Mail fragen. Klicken Sie daher niemals auf die dort hinterlegten Links oder antworten auf die E-Mails. Löschen Sie solche Nachrichten stattdessen schnellstens und schieben Sie diese erst gar nicht in den Papierkorb.

Tipp 5: Wählen Sie einmalige, lange Kennwörter

Es ist zwar sehr bequem: Aber Passwörter im Browser zu speichern, ist aus Sicherheitsgründen keine gute Idee. Angreifer können diese Informationen mit Schadprogrammen auslesen, da die Kennwörter hier nicht ausreichend geschützt sind. Ebenso tabu sind "schwache" Kennwörter wie "123456". Illegale Spezialprogramme knacken solche Kombinationen in Sekunden. Betrachten Sie Zugangsdaten am besten als Ihre persönlichen Tresorschlüssel zu Ihren Internet-Safe, den Sie auch nicht an Fremde weitergeben: Sie schützen Ihr E-Mail-Postfach, das Konto im Lieblings-Online-Shop und Ihr Online-Bankkonto vor unbefugtem Zugriff. Für Hacker sind sie deshalb ein lohnenswertes Ziel. Erneuern Sie daher jetzt Ihre unsicheren Passwörter für alle Ihre Internet-Konten. Oder lassen Sie auch stets die Haustüre offen? Für jedes Konto richten Sie ein neues, einmaliges Passwort mit mindestens acht Stellen ein - besser mehr. Tabu sind dabei neben einfachen Zahlenfolgen und Allerweltsbegriffen auch Namen von Angehörigen, Bekannten, Haustieren, Prominenten sowie die eigene Adresse. Experten empfehlen, sehr lange Passwörter zu erstellen und ganze Sätze, die keinen Sinn ergeben oder auch noch Falschschreibung enthalten, zum Beispiel ist "ElefantenSchielenAufDemEis" besser als Passwort geeignet als h&2KQ@1.

Tipp 6: Den richtigen Adblocker installieren

Übertriebene Online-Werbung ist nicht nur nervig, bremst den Seitenaufbau und erzeugt unnötigen Datenverkehr, darüber hinaus ist sie gefährlich. Denn Werbeeinblendungen kommen nur selten direkt vom Server des Seitenbetreibers, sondern aus ganz anderen Ecken des Internets. Dementsprechend unterliegen sie nicht der redaktionellen Kontrolle des Internetseiten-Betreibers. Diesen Umstand machen sich Cyber-Kriminelle und Datensammler zu nutzen und bauen in die Werbung Schädlinge beziehungsweise Tracker ein. Adblocker versprechen Abhilfe. Die kleinen Browser-Zusatzprogramme klinken sich auf Wunsch in den Browser ein und filtern die Werbung zuverlässig heraus, so das Versprechen der Anbieter. Aber Adblocker ist nicht gleich Adblocker. Das weit verbreitete "Adblock Plus" macht etwa Ausnahmen für zahlungskräftige Firmen. Die bessere Alternative ist daher "uBlock Origin". Der quelloffene Code macht das Programm vollkommen transparent - Hintertüren gibt es also keine. Die Installation in Firefox ist schnell erledigt: In Firefox klicken Sie oben rechts in der Ecke auf , Add-ons und Add-ons suchen. Über das Suchfenster oben rechts suchen Sie nach Ublock Origin und drücken die Enter-Taste. In der Trefferliste klicken Sie rechts vom richtigen Add-On auf Installieren. Nach wenigen Sekunden ist der Werbeblocker einsatzbereit, ein Neustart von Firefox ist nicht nötig.

Tipp 7: Sicheres Surfen leicht gemacht

Die einfache Lösung, um sich gegen all diese Gefahren, die im Internet lauern, zu schützen, ist der eBlocker. Dank dieses kleinen Geräts müssen Sie kein Experte sein, um nervige Werbung, Schädlinge und betrügerische E-Mails effektiv abzublocken. Der eBlocker übernimmt diese Aufgaben für Sie. Dazu schließen Sie das kleine Gerät einfach per Kabel am Router an und versorgen diese mit Strom - fertig. Sofort verhindert der eBlocker wirkungsvoll das Sammeln Ihrer persönlichen Nutzerdaten und die Erstellung von Nutzerprofilen, blockt verlässlich jegliche Form von Internet-Werbung und schützt Sie vor Angriffen über Internetbrowser. Den betrügerischen Versuchen, über gefälschte Internetseiten an die Eingabe persönlicher Daten, wie Passwörter, zu gelangen "Phishing", schiebt der eBlocker dank des innovativen "Browser-Schutzes" ebenfalls einen Riegel vor. Dieser Schutz funktioniert auf allen an den Internetrouter angeschlossenen Geräten, sodass Sie nicht umständlich Software installieren müssen. Mithilfe von wenigen Klicks sind Sie sicher im Internet unterwegs.

Über die eBlocker GmbH

Nach zweijähriger Vorbereitung im Verborgenen ging 2015 die eBlocker GmbH mit Sitz in Hamburg an den Start. Deren Produkte eBlocker Pro und eBlocker Family geben Privatpersonen die Kontrolle über ihre ungewollt während des Surfens im Internet preisgegebenen Informationen zurück. So erhalten die Nutzer wieder die Hoheit und volle Kontrolle über Ihre Daten. Der eBlocker Family verfügt zusätzlich über Jugendschutzfunktionen, über die sich unter anderem Web-Inhalte und Surfdauer beschränken

lassen. Unmittelbar nach Anschluss des eBlockers blockiert er effektiv sämtliche Tracker und datensammelnde Werbung, anonymisiert die IP-Adresse und lässt alle Nutzer vollkommen anonym surfen. Der eBlocker schützt dabei sämtliche Geräte im Heimnetz per Plug&Play, ohne zusätzliche Softwareinstallation. Dank einfachem Anschluss, automatischer Konfigurierung und täglichen Software-Updates ist der eBlocker auch für technisch unerfahrene Nutzer schnell und unkompliziert einsetzbar.
www.eBlocker.com

Kontakt:

Griffel & Co. Kommunikation GmbH
Forsmannstraße 8b
22303 Hamburg, Germany
Email: de-press@eblocker.com
Telefon: +49 40 6094586 00