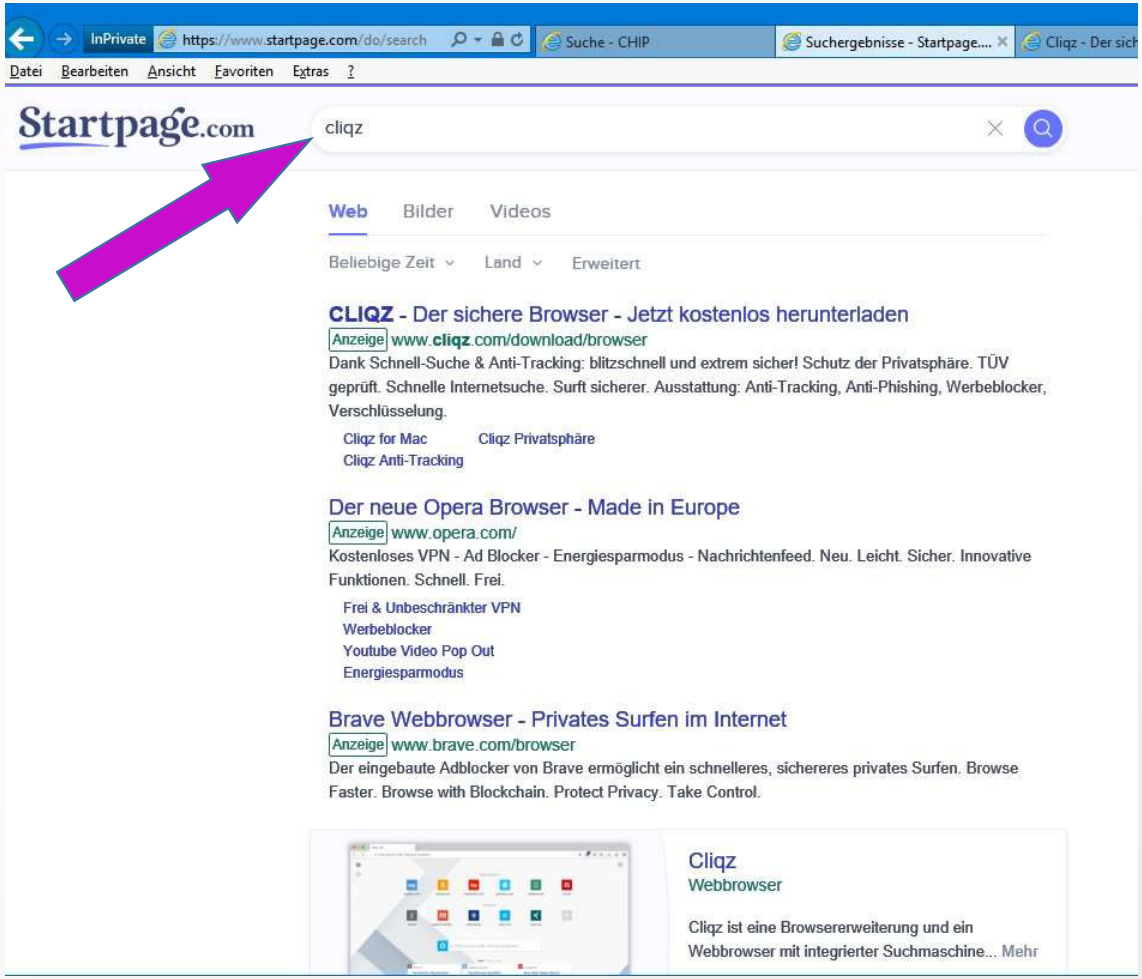
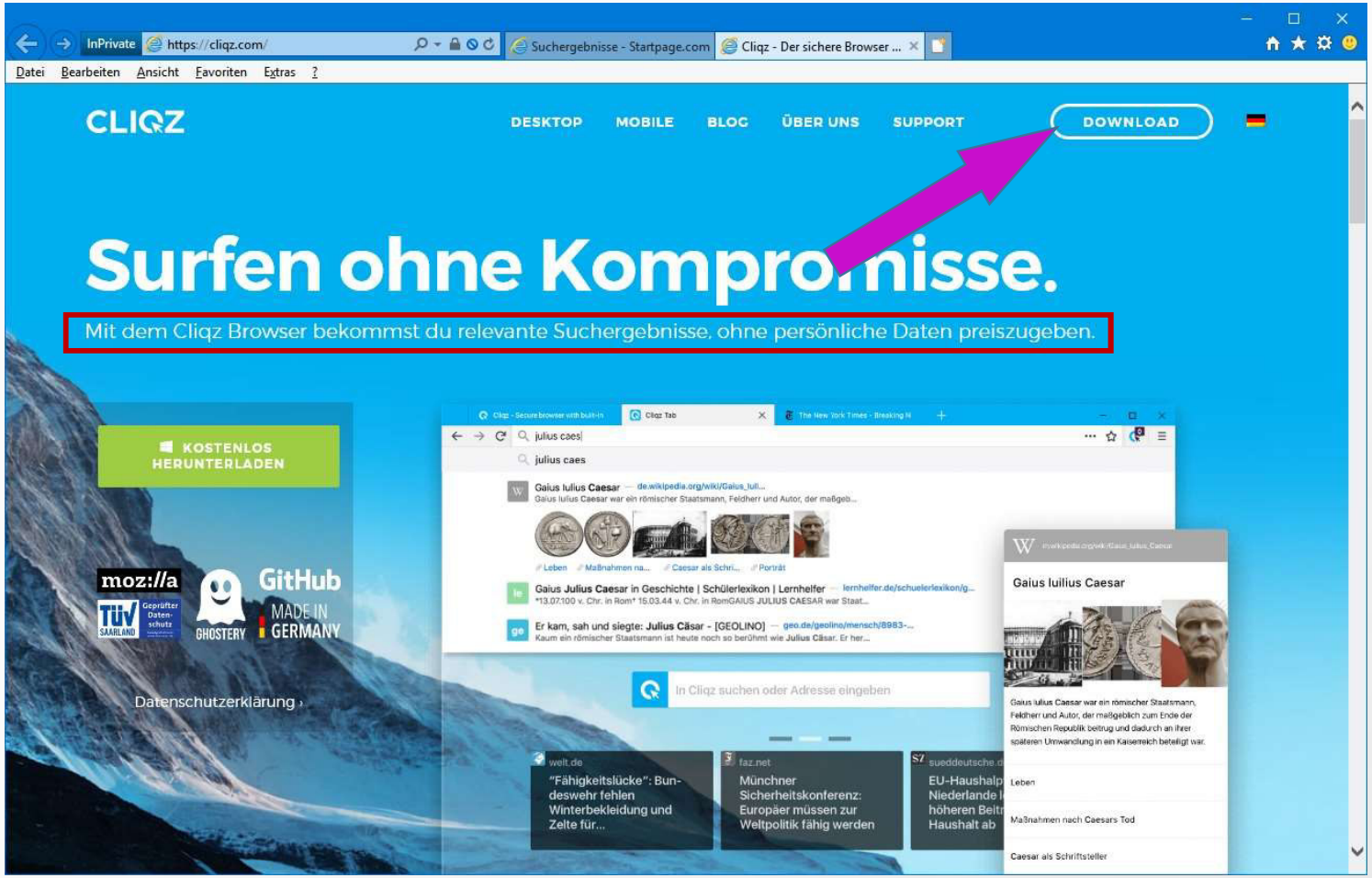
hi-senior

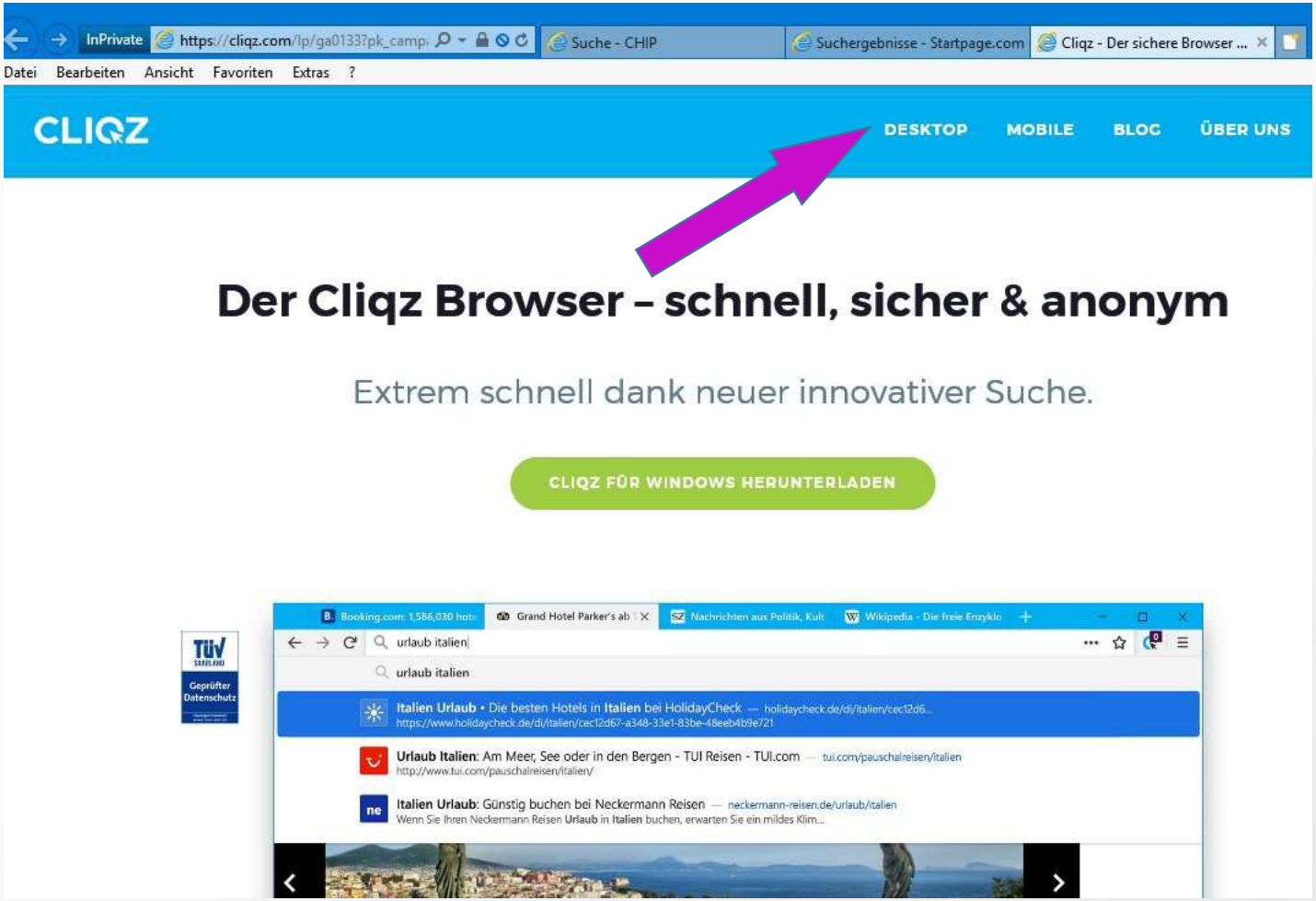
VHS-Club: Senioren @ns Netz

Cliqz-Browser

Cliqz


InPrivate
https://www.startpage.com/do/search
Suche - CHIP
Suchergebnisse - Startpage....
Cliqz - Der sich
Datei Bearbeiten Ansicht Favoriten Extras ?
Startpage.com
cliqz
Web Bilder Videos
Beliebige Zeit
Land
Erweitert
CLIQZ - Der sichere Browser - Jetzt kostenlos herunterladen
Anzeige www.cliqz.com/download/browser
Dank Schnell-Suche & Anti-Tracking: blitzschnell und extrem sicher! Schutz der Privatsphäre. TÜV geprüft. Schnelle Internetsuche. Surft sicherer. Ausstattung: Anti-Tracking, Anti-Phishing, Werbeblocker, Verschlüsselung.
Cliqz for Mac
Cliqz Privatsphäre
Cliqz Anti-Tracking
Der neue Opera Browser - Made in Europe
Anzeige www.opera.com/
Kostenloses VPN - Ad Blocker - Energiesparmodus - Nachrichtenfeed. Neu. Leicht. Sicher. Innovative Funktionen. Schnell. Frei.
Frei & Unbeschränkter VPN
Werbeblocker
Youtube Video Pop Out
Energiesparmodus
Brave Webbrowser - Privates Surfen im Internet
Anzeige www.brave.com/browser
Der eingebaute Adblocker von Brave ermöglicht ein schnelleres, sichereres privates Surfen. Browse Faster. Browse with Blockchain. Protect Privacy. Take Control.
Cliqz
Webbrowser
Cliqz ist eine Browsererweiterung und ein Webbrowser mit integrierter Suchmaschine... Mehr


InPrivate
https://cliqz.com/
Suchergebnisse - Startpage.com
Cliqz - Der sichere Browser ...
Datei Bearbeiten Ansicht Favoriten Extras ?
CLIQZ
DESKTOP
MOBILE
BLOG
ÜBER UNS
SUPPORT
DOWNLOAD
Surfen ohne Kompromisse.
Mit dem Cliqz Browser bekommst du relevante Suchergebnisse, ohne persönliche Daten preiszugeben.
KOSTENLOS HERUNTERLADEN
moz://a
GHOSTERY
GitHub
MADE IN GERMANY
Datenschutzerklärung ›
julius caes
Gaius Iulius Caesar
Gaius Julius Caesar in Geschichte | Schülerlexikon | Lernhelfer
Er kam, sah und siegte: Julius Cäsar - [GEOLINO]
In Cliqz suchen oder Adresse eingeben
welt.de
"Fähigkeitslücke": Bundeswehr fehlen Winterbekleidung und Zelte für...
faz.net
Münchner Sicherheitskonferenz: Europäer müssen zur Weltpolitik fähig werden
Leben
Maßnahmen nach Caesars Tod
Caesar als Schriftsteller


InPrivate
https://cliqz.com/lp/ga0133?pk_camp
Suche - CHIP
Suchergebnisse - Startpage.com
Cliqz - Der sichere Browser ...
Datei Bearbeiten Ansicht Favoriten Extras ?
CLIQZ
DESKTOP
MOBILE
BLOG
ÜBER UNS
Der Cliqz Browser – schnell, sicher & anonym
Extrem schnell dank neuer innovativer Suche.
CLIQZ FÜR WINDOWS HERUNTERLADEN
Geprüfter Datenschutz
urlaub italien
urlaub italien
Italien Urlaub • Die besten Hotels in Italien bei HolidayCheck
https://www.holidaycheck.de/di/italien/cec12d67-a348-33e1-83be-48eeb4b9e721
Urlaub Italien: Am Meer, See oder in den Bergen - TUI Reisen - TUI.com
http://www.tui.com/pauschalreisen/italien/
Italien Urlaub: Günstig buchen bei Neckermann Reisen
Wenn Sie Ihren Neckermann Reisen Urlaub in Italien buchen, erwarten Sie ein mildes Klim...

BROWSER

Cliqz versteht sich als **Datenschutz-Browser**. Mit einem eingebauten Tracking-Schutz und Suchergebnissen direkt in der Adresszeile stellt er sich gegen *Google*. Der US-Konzern ist nämlich nicht nur der weltgrößte Suchmaschinen-betreiber, mit seinem Werbenetzwerk sammelt er auch quer über das Internet verteilt mehr Userdaten als jedes andere Unternehmen.

Hinter dem Browser aus München steht als Mehrheitseigentümer die *Burda-Mediengruppe*. Diese gilt nicht gerade als ein Freund von *Google*. Seit Jahren schwelt zwischen den beiden Konzernen ein Streit um das Leistungsschutz-recht. Bei dieser medienrechtlichen Frage steht *Burda* vereinfacht gesagt auf dem Standpunkt, dass *Google* von fremden Inhalten profitiert und daher Inhaltsanbieter – also beispielsweise die Medien des *Burda*-Verlags – bezahlen müsste.

Cliqz setzt auf Datenschutz, aber auch die Benutzerfreundlichkeit überzeugt.

Burdas Unterstützung des *Cliqz*-Browsers, der sich gegen die Marktmacht von *Google* im Bereich der Online-Wer-bung stellt, ist also medienpolitisch motiviert. Für den Anwender bedeutet das: *Cliqz* verhindert, dass *Google* zu viele Daten über ihn sammelt. Denn *Googles* Marktmacht beruht vor allem auf seiner umfassenden Datensamm--lung, die dem Konzern ermöglicht, **personalisierte Werbung** an User auszuspielen.

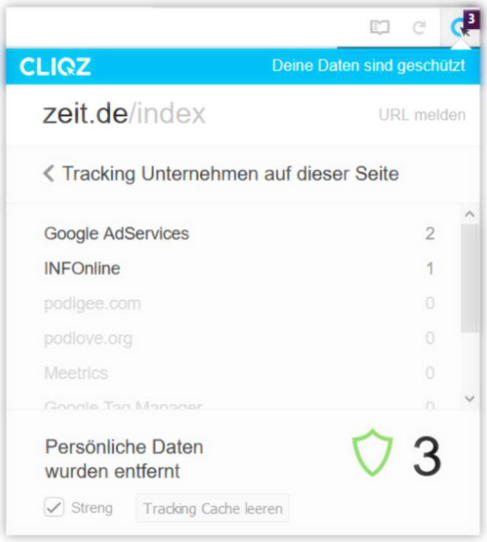
Cliqz Browser hat eine integrierte Anti-Tracking-Funktion: Was steckt dahinter?

Fast alle Websites integrieren Tracking-Dienste, die alle Aktivitäten ihrer Besucher aufzeichnen. Wo die eigenen Nutzerdaten überall hingehen, ist meist nicht mehr zu durchschauen. Denn in der Regel verfolgen zahlreiche Tracker die Internetnutzer auf Schritt und Tritt, auch websiteübergreifend.

Einer Cliqz-Studie zufolge erheben Tracker – beabsichtigt oder nicht – bei über drei Vierteln der Web-seiten-Aufrufe unsichere Daten. Als unsicher definieren wir Daten, anhand derer einzelne Nutzer identifiziert und durchs Web verfolgt werden könnten.

Du hast die Kontrolle!

Wenn du eine Website besuchst, zeigt Cliqz dir im Browser eine Auflistung von Trackern, die möglicherweise deine Privatsphäre verletzen.



In dem Info-Fenster (Control Center) hinter dem blauen Symbol rechts oben siehst du eine Darstel-lung, wie sich Tracker bei deinem Besuch einer Webseite verhalten. In dem Beispiel-Bild oben siehst du neben dem Namen der Tracking-Betreiber Zahlen die auflisten, wie viele unsichere Daten ein Tracker-Betreiber angefordert hat. Solche Daten werden von Cliqz überschrieben, sodass die Privat-sphäre unserer Nutzer geschützt ist.

Cliqz Anti-Tracking unterbindet auch dann die Übertragung unsicherer Daten, wenn du den jeweiligen Betreibern z.B. durch Zustimmung in AGBs oder in entsprechenden Hinweisen auf Webseiten (die du vielleicht liest, vielleicht auch nicht) „Erlaubnis“ gegeben hast. Mit der Datenübermittlung blockiert Cliqz Anti-Tracking zugleich Services und Funktionen, sowie die Einspeisung von Werbeanzeigen, die mit unsicheren Tracking-Daten arbeiten.
Du kannst Cliqz Anti-Tracking komplett oder für die jeweilige Website ausschalten. Dann erhalten die Tracker auf der jeweiligen Webseite Daten, anhand derer du identifiziert werden könntest.

Nur die unsicheren Daten werden entfernt

Die Anti-Tracking-Funktion blockiert, anders als andere Anti-Tracking-Systeme, die Signale nicht vollständig, sondern unterbindet nur das Abgreifen nutzerbezogener Daten. Website-Betreiber kön-nen sichere Daten erheben und z.B. die Anzahl der Besuche korrekt berechnen. Dies ist das “Stan-dard”-Verhalten dieser Funktion. Auf Wunsch können jedoch auch alle Daten blockiert werden. Dazu wählst du im Control Center unter “Persönliche Daten wurden entfernt” die Option “strikt” oder „streng“ aus. Cliqz Anti-Tracking arbeitet dank unserer Statistiken aus dem Human Web sehr präzise. Es erkennt mehr unsichere Daten als viele andere Anti-Tracking-Technologien. So kommt es kaum vor, dass Cliqz nützliche Webseiten-Funktionen fälschlicherweise blockiert.

Unsichere Tracking-Daten – ein ganz konkretes Risiko für deine Privatsphäre

Angenommen ein Nutzer besucht nacheinander mehrere Webseiten, in die Tracker desselben Betreibers eingebunden sind. Das können Online-Shops und Nachrichten sein, aber auch Seiten mit Informationen zu Suchtkrankheiten oder zum Thema Privatinsolvenz. So laufen höchst private Informatio-nen in den Datenbanken der Tracker auf, die nicht nur Rückschlüsse auf die finanzielle Situation, Interessen und Kaufabsichten, sondern z.B. auch auf die sexuelle Orientierung, Gesundheit oder die politische und religiöse Einstellung erlauben. Loggt sich der Nutzer dann z.B. auf seine persönliche Seite bei dem beliebten Dienst about.me ein, können ihm die zutiefst intimen Informationen aus vorhe-rigen Seitenbesuchen zugeordnet werden.

Wir wissen nicht, was die unzähligen Tracking-Betreiber mit den Daten machen

Wer Zugriff auf die Daten hat, mit welchen Geschäftspartnern sie diese Daten teilen und wofür die Tracking-Betreiber die Daten konkret nutzen, bleibt oft im Dunkeln. Der US-Geheimdienst NSA oder die Justizbehörden können US-Anbieter verpflichten, Daten über deutsche Nutzer herauszugeben. Hacker könnten sich Zugriff auf Tracking-Daten verschaffen. Es besteht zumindest das Risiko der Aus-spähung einzelner Menschen und von Datenlecks. Deshalb schützen wir unsere Nutzer mit einer neu entwickelten Technik davor, ungewollt persönliche Daten an Tracker zu übermitteln. Wie Web-Tracking im Detail funktioniert und wie Cliqz Anti-Tracking davor schützt, erklären wir in zwei Techblog-Artikeln

Cliqz Werbeblocker

Mit Online-Werbung ist es so eine Sache: Einerseits ermöglichen es die Einnahmen aus Anzeigen, dir Inhalte, Apps und Services wie zum Beispiel eine Suchmaschine kostenlos anzubieten. Auch wir selbst wollen in naher Zukunft unsere Cliqz-Produkte mit Werbung finanzieren.

Anderseits stört aggressive Werbung das Web-Erlebnis. Auch die Datensammel-Wut mancher Akteure aus der Werbeindustrie ist bedenklich.

Vor diesem Hintergrund haben uns viele User unseres Desktop-Browsers nach einer Funktion zum Blockieren von Werbung gefragt. Bei uns kommt der User immer an erster Stelle und wir haben uns beeilt, diesem Wunsch nachzukommen. Eine Lösung gegen verfolgende Werbung (Re-Targeting) gibt es mit der Cliqz Anti-Tracking-Funktion ja bereits. Mit dem Cliqz Ad Blocker kannst du nun auch andere Anzeigen „ausschalten“.

Unser Ziel ist es, dir mittelfristig eine Möglichkeit zu geben, nur die Werbung abzuschalten, die störend und aggressiv ist. Wir halten das Akzeptieren von „fairer“ Werbung für den besten Ausgleich zwischen den Interessen der Websitebetreiber, der Werbewirtschaft und der Nutzer.

Momentan geht das aber noch nicht. Du kannst in dieser vorläufigen Version Werbung nur komplett abschalten, und sie dann auf bestimmten Websites wieder erlauben (zum Beispiel auf Websites, die verantwortungsvoll mit Werbung umgehen). Wir bieten die „unfertige“ Version unseres Ad Blockers jetzt schon an, um Erfahrungen für die Entwicklung der endgültigen Version sammeln zu können.

In der künftigen, endgültigen Version des Cliqz Ad Blocker wird die Grundeinstellung sein, „faire“ Werbung zuzulassen. Was „fair“ ist und was nicht, müssen wir selbst noch definieren. Einer unserer Leitgedanken, nämlich „den User immer so direkt wie möglich zum Ziel bringen“ gibt die Richtung vor: Stellt sich Werbung dem User in den Weg, kann sie nicht mehr als „fair“ gelten. Bei der Definition von fairer Werbung lassen wir uns nicht bestechen – im Unterschied zu anderen Ad Blockern, die sich de facto von der Werbewirtschaft für „Ausnahmen“ bezahlen lassen.

Basis-Einstellungen:

Optimiert: Nur faire Werbung zulassen (noch nicht verfügbar)
Alle: Alle Anzeigen blockieren
Keine: Keine Anzeigen blockieren

Es wird auch möglich sein, eigene Regeln bzw. Ausnahmen zu definieren.
Unser Ziel: Cliqz Ad Blocker wird dir die volle Kontrolle geben. Du entscheidest!

Welche Funktionen und Einstellmöglichkeiten wünschst du dir vom Cliqz Ad Blocker?

Was ist für dich „faire“ Werbung? Was hältst du für „unfair“?

Sag es uns hier cliqz.com/support

Anti-Phishing

Cliqz Anti-Phishing schützt dich vor Betrügern, die es auf deine Passwörter und Kontodaten abgesehen haben.

Im Netz sind Phishing-Betrüger unterwegs, die mit gefälschten Nachrichten und Websites deine Passwort-, Konto-, Kreditkarten- oder sonstige kritische Daten abgreifen wollen. Der Cliqz Browser und die Browser-Erweiterung Cliqz for Firefox enthalten eine eingebaute Sicherheitsfunktion, die dich besser vor Identitätsdiebstahl schützt. Die neuartige, von Cliqz selbst entwickelte Technologie erkennt solche gefährlichen Websites besonders frühzeitig und zuverlässig. Wenn du eine Website besuchst, die Cliqz als Fälschung identifiziert, zeigt dir unser Browser einen Warnhinweis. Um einen möglichst umfassenden Schutz sicherzustellen, setzen wir ergänzend Googles Safe Browsing Service ein. Er verhindert zusätzlich den Download und die heimliche Installation von Schadprogrammen, die über unsichere Websites verbreitet werden. Einen hundertprozentigen Schutz gegen Phishing und Malware gibt es aber nicht. Lass also weiterhin Vorsicht walten!

Hinweis für nicht-deutsche Nutzer: Aufgrund unserer Konzentration auf den deutschen Markt funktioniert Cliqz Anti-Phishing nur in Deutschland vollständig.

Warum ist der Schutz vor Phishing so wichtig?

Phishing-Betrüger senden E-Mails, SMS oder andere Nachrichten, die aussehen als kämen sie von einem seriösen Absender. Die Adressaten werden aufgefordert, einen Weblink anzuklicken, um auf der dahinter liegenden, ebenfalls gefälschten Website ihre Daten einzugeben. Dieser Identitätsdiebstahl kann böse Folgen haben – so könnten sich etwa Kriminelle an deinem Bankkonto vergreifen.

Wie funktioniert Cliqz Anti-Phishing?

Anti-Phishing-Technologien nutzen verschiedene Methoden, um gefälschte Nachrichten oder Websites zu erkennen. Die Cliqz-Technologie setzt an der Erkennung von Websites an. Cliqz Anti-Phishing untersucht neue Websites und prüft, ob sie Daten-Eingabefelder enthalten und verdächtige Merkmale aufweisen. „Neu“ sind für Cliqz Anti-Phishing jene Websites, die erstmals von Teilnehmern von Human Web besucht wurden.

Human Web

Human Web ist eine Software, die in die Browser bzw. Browsererweiterungen von Cliqz und Ghostery eingebaut ist. Der Zweck ist der Aufbau von Statistiken, die wir als Treibstoff für unsere Produkte nutzen. Mit den kollektiv zusammengetragenen Statistiken finden wir heraus, welche Websites am besten zu Suchanfragen passen und decken gefälschte Websites und Tracker auf. So machen die Human-Web-Nutzer das Internet als Gemeinschaft zu einem besseren Ort. Die Teilnahme am Human Web ist freiwillig, du kannst es auch abschalten (Opt-out). Die Privacy-by-

Design-Architektur der Human-Web-Technologie stellt sicher, dass sich in den Statistiken keinerlei Daten über einzelne Nutzer befinden. Die Anonymität der Nutzer ist stets vollständig gewährleistet und Tracking ausgeschlossen. Das ist nachprüfbar, denn der Softwarecode von Human Web ist öffentlich (Open Source).

Check das!

Wir von Cliqz versprechen dir mehr Kontrolle über deine Daten. Dazu gehört, dass du nachprüfen kannst, was mit deinen Daten passiert.

Viele Firmen verschleiern ganz bewusst, wie, welche und wofür sie Daten sammeln. Aus gutem Grund. Wenn du wüsstest, was sie über dich wissen, wärest du schockiert. Wir dagegen versprechen: Cliqz sammelt überhaupt keine persönlichen Daten über dich. Hmmm…kann ja jeder behaupten, wirst du dir vielleicht sagen. Eine gesunde Skepsis ist im Internet ja auch durchaus angebracht. Darum machen wir überprüfbar, wie wir mit Daten umgehen.

Der TÜV hat unsere Architektur, hinsichtlich Datenschutz abgesegnet. Und im Cliqz Browser für Desktop gibt es ein Transparenz Cockpit, auf dem du “live” siehst, welche Daten dein Browser an uns sendet und was mit ihnen geschieht. Der Cliqz Browser und alle integrierten Cliqz-Funktionen sind Open Source, das heißt der Softwarecode ist für jedermann einsehbar. Und bei Fragen zum Datenschutz hat unser Support immer ein offenes Ohr für dich. Mehr Transparenz geht nicht.

Auch bei unserem Geschäftsmodell steht der Schutz der Privatsphäre unserer Nutzer im Vordergrund. MyOffrz bringt erstmals Zielgerichtete Angebote mit konsequentem Datenschutz in Einklang. Es zeigt dir passende Angebote im richtigen Moment an und berücksichtigt dabei deine Interessen, ohne deine Privatsphäre zu gefährden. Hier erfährst du mehr.

Persönliche Daten auf Cliqz Servern gespeichert.

“Privacy by Design” bedeutet, dass keine persönlichen Daten auf unseren Servern gespeichert werden. Wir versprechen das nicht nur. Mithilfe des CliqzTransparenz Dashboards kannst du das jederzeit überprüfen.

Pro

Sehr sichere Default-Konfiguration
Schutz vor Trackern
Suchergebnisse in der Adresszeile
Eingebauter Werbeblocker
SSL-Verschlüsselung als Standard

Kontra

Themes beschränken sich auf Hintergrundbilder
Synchronisation nur eingeschränkt möglich
Nutzer erhalten Werbeangebote

Fazit

Cliqz ist eine gute Alternative für Menschen, die einen Browser suchen, der ihre Privatsphäre schützt. Er ist bereits ab Werk für maximalen Datenschutz konfiguriert. Dass Cliqz selbst dem Nutzer mit MyOffrz Werbeangebote unterbreitet, lässt sich zum Glück deaktivieren.

Cliqz versteht sich als Datenschutz-Browser. Mit einem eingebauten Tracking-Schutz und Suchergebnissen direkt in der Adresszeile stellt er sich gegen Google. Der US-Konzern ist nämlich nicht nur der weltgrößte Suchmaschinenbetreiber, mit seinem Werbenetzwerk sammelt er auch quer über das Internet verteilt mehr Userdaten als jedes andere Unternehmen.

Hinter dem Browser aus München steht als Mehrheitseigentümer die Burda-Mediengruppe. Diese gilt nicht gerade als ein Freund von Google. Seit Jahren schwelt zwischen den beiden Konzernen ein Streit um das Leistungsschutzrecht. Bei dieser medienrechtlichen Frage steht Burda vereinfacht gesagt auf dem Standpunkt, dass Google von fremden Inhalten profitiert und daher Inhaltsanbieter – also beispielsweise die Medien des Burda-Verlags – bezahlen müsste.

Cliqz setzt auf Datenschutz, aber auch die Benutzerfreundlichkeit überzeugt.

Burdas Unterstützung des Cliqz-Browsers, der sich gegen die Marktmacht von Google im Bereich der Online-Werbung stellt, ist also medienpolitisch motiviert. Für den Anwender bedeutet das: Cliqz verhindert, dass Google zu viele Daten über ihn sammelt. Denn Googles Marktmacht beruht vor allem auf seiner umfassenden Datensammlung, die dem Konzern ermöglicht, personalisierte Werbung an User auszuspielen.

Ein abgesicherter Firefox

Technisch besteht Cliqz aus dem Open-Source-Browser Mozilla Firefox mit einigen Modifikationen. Die Anti-Tracking-Technologie von Cliqz verhindert, dass Nutzer im Web eindeutig identifiziert werden können, und mit der eigenen Suchtechnologie direkt in die Adresszeile holt Cliqz die User ab, bevor sie überhaupt auf die Idee kommen, eine Suchanfrage bei Google einzugeben.

Cliqz positioniert sich nicht grundsätzlich gegen Werbung im Internet. Im Gegenteil, mit MyOffrz bespielt der Browser seine Nutzer sogar selbst mit Werbung, was diese allerdings sehr einfach abschalten können. MyOffrz sind personalisierte Angebote – im Unterschied zu anderen Werbenetzwerken werden dabei allerdings keine persönlichen Daten von Usern zentral gespeichert. Die Personalisierung findet im Browser statt. Cliqz verfolgt also einen dezentralen Ansatz: für Funktionen, die sonst vom Server ausgeführt werden, ist hier der Client zuständig.

Theoretisch zeigt Cliqz an dieser Stelle Werbung – das war jedoch im Testzeitraum nie der Fall.

Die Grundfunktionen von Cliqz unterscheiden sich nicht von Firefox. Cliqz bemüht sich um Aktualität, neue Firefox-Versionen werden übernommen. Somit beruht der Browser jetzt auf dem grundlegend erneuerten Firefox Quantum mit allen seinen Vorzügen, oder zumindest mit fast allen. Funktionen, die Sever-Dienste verwenden, auch die von Mozilla selbst, hat Cliqz nämlich nicht übernommen. Der Leselisten-Dienst Pocket und die überaus gelungene Screenshot-Funktion fehlen also, während die Leseansicht erhalten bleibt. Auch die Synchronisation, für die ein Firefox-Konto nötig ist, steht in Cliqz nicht zur Verfügung. Allerdings können Anwender die Desktop- mit der Mobilversion verknüpfen. Mehr dazu im Abschnitt „Synchronisation“.

Abgesehen von den Datenschutzerweiterungen und der Suchfunktion in der Adresszeile, auf die wir in den entsprechenden Abschnitten näher eingehen, hat Cliqz den Firefox-Code auch um einen Video-Downloader erweitert, mit dem Anwender Videos von Seiten wie YouTube und Vimeo lokal speichern können.

Das wirkt fast wie eine Stichelei gegen Google, den Eigentümer von YouTube. Das Videoportal selbst unterstützt den Video-Download nämlich nicht. Entsprechende Erweiterungen wurden auch aus Googles Chrome Store entfernt. Wer YouTube-Videos herunterlädt, statt sie online zu sehen, beansprucht Bandbreite, hinterlässt aber kaum Benutzerdaten und ist nur schlecht durch Werbung erreichbar. Das kann nicht im Interesse von Google sein.

Die Benutzeroberfläche macht sofort klar, dass Cliqz auf Firefox basiert. Im Großen und Ganzen sehen die beiden Browser gleich aus. Dass die Entwickler hier nur wenig geändert haben, ist kein Nachteil. Im Gegenteil, Firefox zeichnet sich durch hohe Benutzerfreundlichkeit aus, dennoch lässt sich sein Design gut an persönliche Vorstellungen anpassen. Das trifft auf Cliqz genauso zu.

Eine maßgebliche Änderung gibt es allerdings: Cliqz unterstützt aus Sicherheitsgründen keine Themes. Das Ändern des Hintergrundbilds für neue Tabs ist jedoch möglich. Bei der Titelleiste und den Schaltfläche müssen Anwender allerding bei Grau und Hellblau bleiben. Diese wirkt sehr klar und freundlich, der ein oder andere Nutzer könnte sich allerdings an dem kräftigen Hellblau der Titelleiste stören. Eine dezenter gefärbte Oberfläche wäre zumindest als Option wünschenswert.

Firefox und somit auch Cliqz hat eine Option zum Einstellen der Dichte der Oberfläche. Damit wird der Abstand zwischen den Bedienelementen reguliert. Während Firefox dafür drei Stufen anbietet, „Kompakt“, „Normal“ und „Touch“, sind es bei Cliqz nur zwei, nämlich „Normal“ und „Touch“. Wider Erwarten fehlt allerdings nicht die kompakte Ansicht von Firefox, sondern die Touchscreen-Ansicht. Die normale Ansicht bei Cliqz entspricht der kompakten bei Firefox und die Touchscreen-Ansicht der normalen. Das ist durchaus sinnvoll, fällt doch schon die normale Ansicht relativ groß aus. Firefox-Nutzer müssen auf „Kompakt“ umstellen, wenn sie wollen, dass die Bedienelemente des Browsers genauso wenig Platz einnehmen wie bei Google Chrome.

Hier fehlt etwas! Der Anwender kann die Menüleiste von Cliqz genauso wie bei Firefox anpassen, allerdings unterstützt der Datenschutz-Browser keine Themes. Auch für die Dichte der Oberfläche gibt es weniger Optionen.

Die Integration der Suche direkt in die Adresszeile ist sehr gelungen. Bei einfachen Suchanfragen spart sich der Anwender dadurch den Besuch einer Suchmaschine und somit Zeit. Die Suchanfrage „wetter berlin“ zeigt beispielsweise eine Wetterprognose für die nächsten Tage direkt in der Adresszeile und auch „btc in eur“ serviert sofort den aktuellen Bitcoin-Kurs. Im Unterschied zu anderen Browsern, die nur Suchvorschläge anzeigen, listet Cliqz gleich drei Treffer auf, die der User mit den Cursortasten auswählen kann. Zur besseren visuellen Orientierung werden auch die Website-Icons (Favicons) der Treffer angezeigt.

Eiseskälte und klarer Himmel in Berlin; das weiß Cliqz, ohne überhaupt eine Website zu öffnen.

Die Suchergebnisse in der Adresszeile sind eine Innovation, die viele Anwender wahrscheinlich intuitiv nutzen werden, ohne überhaupt bewusst wahrzunehmen, dass sich etwas geändert hat. Das Ganze wirkt durchaus zukunftsweisend und könnte bald Standard bei Browsern werden.

Aus Sicherheits- und Datenschutzgründen hat man sich bei Cliqz gegen Erweiterungen entschieden. Viele davon sammeln nämlich unbemerkt Benutzerdaten. Für den Anwender ist es nicht ersichtlich, was genau einzelne Erweiterungen alles über ihn in Erfahrung bringen. Das widerspricht naturgemäß dem Konzept eines Browsers wie Cliqz, der seinen Nutzern so viel Kontrolle wie möglich über ihre Daten geben möchte.

Statt eines offenen Erweiterungsverzeichnisses integriert Cliqz einen Ad-Blocker, die Technologie von HTTPS Everywhere, das sichere SSL-Verbindungen zur Default-Einstellung macht, sowie den Trackingschutz und die Cliqz-Suche direkt in den Browser. Zwei zusätzliche Erweiterungen kann der Anwender direkt in den Einstellungen von Cliqz installieren, nämlich den Tracking-Filter Ghostery und den Passwortmanager LastPass.

Der sichere Browser ohne Add-ons: Das war schön gedacht, aber Cliqz hat die Rechnung ohne die Nutzer gemacht. Diese wollen ihren Browser einfach mit neuen Funktionen erweitern. Das haben die Entwickler schließlich auch eingesehen. Seit Dezember 2018 unterstützt Cliqz nun Firefox-Add-ons, die sich hier genauso einfach wie im Mozilla-Browser installieren lassen.

Eine klassische Synchronisationsfunktion gibt es bei Cliqz nicht. Stattdessen ist eine Funktion namens Connect integriert.

Connect verknüpft auf einfache Weise Desktop- und Mobilversion von Cliqz. Der Desktop-Browser zeigt einen QR-Code, der auf dem Smartphone mit der Mobilversion gescannt wird. Daraufhin sind die beiden Geräte miteinander gekoppelt. Der Anwender kann Tabs von einem Gerät auf das andere senden und mit dem Video-Cliqz Connect

Vergrößern

Eine richtige Synchronisation fehlt, aber dank Connect stellt Cliqz sehr einfach und schnell eine Verbindung zum Smartphone her.

Noch mehr als Firefox schützt Cliqz Privatsphäre und Sicherheit seiner Nutzer. Firefox lässt sich mit diversen Erweiterungen zwar auch so konfigurieren, dass sein Sicherheitsstandard ähnlich hoch wie bei Cliqz ist, dafür ist allerdings ein gewisses Maß an technischem Wissen und Interesse notwendig. Cliqz hingegen ist schon in der Standardkonfiguration darauf ausgelegt, die Weitergabe von personenbezogenen Daten zu gut wie möglich zu vermeiden. Dafür wurde der Firefox-Code in einigen Punkten angepasst:

- Die HTTPS-Everywhere-Integration sorgt für SSL-Verschlüsselung, sofern der Server das unterstützt.
- Eine eigene Anti-Tracking-Funktion verhindert die Weitergabe persönlicher Daten an Tracker.
- Die optionale Erweiterung Ghostery bringt zusätzlichen Schutz vor Trackern.
- Der Ad-Blocker unterbindet das Anzeigen von Werbung.
- Eine Suchfunktion in der Adressleiste speichert im Gegensatz zu Suchmaschinen wie Google und Bing keine personenbezogenen Daten.
- Passwörter werden auf Wunsch beim Online-Dienst LastPass gespeichert.
- Erweiterungen, die immer ein Risiko für die Sicherheit und die Privatsphäre darstellen, sind generell deaktiviert.

Wo sich Datenschutz, Sicherheit und Benutzerfreundlichkeit treffen

Datenschutz und Sicherheit stehen oft der Benutzerfreundlichkeit entgegen. So ist der Tor Browser – momentan wahrscheinlich der Browser, der im Bereich Sicherheit und Datenschutz am konsequentesten ist – nicht besonders benutzerfreundlich. Jedenfalls dann nicht, wenn der Anwender tatsächlich vollständig anonym bleiben will.

Die Entwickler von Cliqz gehen einen anderen Weg. Das Ziel ist nicht, vollständige Anonymität zu erreichen, sondern die Datenspur, die jeder Anwender hinterlässt, möglichst schmal zu halten, ohne gleichzeitig die Benutzerfreundlichkeit spürbar einzuschränken.

Diese Philosophie wird beispielsweise beim Tracking-Schutz deutlich. Er blockiert Tracker nicht vollständig. Dadurch würden nämlich einige Websites nicht richtig funktionieren. Stattdessen verhindert er, dass Tracker Nutzer eindeutig identifizieren können, indem er nur einen Teil der Daten weitergibt und diese nötigenfalls verändert. Wenn beispielsweise ein Anwender eine ungewöhnliche Bildschirmauflösung verwendet, die ihn in Kombination mit einigen anderen Daten identifizierbar machen würde, sendet Cliqz eine unauffällige Standardauflösung an den Tracker.

Um zu gewährleisten, dass der Tracking-Schutz funktioniert, und auch für die Optimierung der Suchergebnisse muss Cliqz selbst Benutzereingaben verarbeiten. Damit hat der Browser das Potential zur Datenkrake. Das will der Software-Anbieter naturgemäß vermeiden, weshalb er Vorkehrungen trifft, um keine personenbezogenen Daten zu speichern. Das Unternehmen spricht von „Privacy by Design“. Cliqz erhebt nur anonymisierte statistische Daten.

Cliqz behandelt Suchanfragen streng getrennt von Besuchsstatistiken und überträgt die Daten über Seitenbesuche auch einzeln und um mindestens eine Stunde zeitversetzt – so lassen sich keine Browsersitzungen rekonstruieren, sollten die Daten auf legalem (Behörden) oder illegalem (Hacker) Weg Dritten in die Hände fallen. Viel Datenverarbeitung geschieht bereits im Client, also auf dem Rechner des Benutzers, so dass die Server von Cliqz erst gar keine Daten erhalten, die zu viel verraten. Da der Code des Browsers Open-Source ist, ist der sorgsame Umgang mit Benutzerdaten keine Vertrauensfrage, denn jeder mit entsprechenden Kenntnissen kann im Programmcode nachprüfen, ob sich das Programm tatsächlich so verhält, wie der Hersteller behauptet.

Auf dem Desktop ist Cliqz für Windows, Mac und Linux erhältlich. Die Linux-Version wird allerdings nicht beworben; sie ist als experimentell gekennzeichnet. Anwender finden sie nur, wenn sie direkt danach in Suchmaschinen forschen. Die Windows-Version benötigt mindestens Windows 7, die Mac-Version ist ab OS X 10.9 lauffähig.

Die Hardware-Voraussetzungen sind niedrig und dieselben wie für Firefox: Ein Pentium-4-Prozessor mit SSE2-Befehlssatz unter Windows beziehungsweise ein Mac mit Intel-Prozessor, 512 Megabyte Arbeitsspeicher und 200 Megabyte Speicherplatz. Auf unserem Testrechner belegt Cliqz rund 144 Megabyte Speicherplatz.

Die Performance-Werte liegen sehr nahe an denen von Firefox, was dadurch zu erklären ist, dass die beiden Browser zu einem großen Teil dieselbe Code-Basis verwenden. Cliqz ist, wie auch Firefox, sicher nicht der schnellste Webbrowser, aber schnell genug. Die Unterschiede zum Geschwindigkeitssieger Chrome sind gering und fallen im Alltag nicht auf.

Lediglich für den Programmstart ließ sich Cliqz deutlich mehr Zeit als Firefox. Er brauchte 0,66 Sekunden dafür, so lange wie kein anderer Browser im Test. Das wird allerdings dadurch relativiert, dass Cliqz im Prinzip Firefox mit einigen vorinstallierten Erweiterungen ist. Auch alle anderen Browser brauchen länger für den Start, wenn mehr Erweiterungen installiert sind. Die Arbeitsspeicherbelegung war um eine Spur (weniger als 100 Megabyte mit 20 geöffneten Websites) größer als bei Firefox, was sich ebenso mit den vorinstallierten Erweiterungen erklären lässt.

Lohnt es sich, Cliqz zu verwenden? Zum einen bietet der Browser nicht die beinahe vollständige Anonymität, die der Tor Browser verspricht, zum anderen lässt sich Firefox mit Erweiterungen genauso gut absichern wie Cliqz. Erfahrene User sind also schnell versucht, Cliqz als unnötig zu disqualifizieren.

Was Cliqz allerdings leistet, ist die Messlatte dafür, was ein Alltagsbrowser defaultmäßig an Sicherheit und Datenschutz bieten kann, deutlich höher zu legen. Davon profitieren alle Anwender, auch solche, die nicht über das technische Wissen verfügen oder sich nicht die Mühe machen würden, einen anderen Browser entsprechend anzupassen. Ein Highlight ist die Suche direkt in der Adresszeile, die zeigt, dass Benutzerfreundlichkeit und Privatsphäre sich nicht zwangsläufig ausschließen.

Der Wechsel auf Cliqz kann jedem Anwender empfohlen werden, der seine Browsersicherheit auf einfache Weise deutlich erhöhen möchte. Wer einen Browser ohne Erweiterungsmöglichkeit zu eingeschränkt findet und genau weiß, was er tut, kann immer noch Firefox installieren und ihn selbst absichern – auf die praktische Suchfunktion und den Tracking-Schutz von Cliqz muss er dank der Cliqz-Erweiterung trotzdem nicht verzichten.