

WACHSAM IM INTERNET SURFEN: WIR MOTZEN GEMEINSAM IHREN BROWSER AUF

Beim Surfen im Internet drohen alle möglichen Gefahren: Einmal falsch geklickt können Schadprogramme heruntergeladen oder sensible Daten preisgegeben werden. Auch hinterlassen wir beim Surfen Daten, mit denen Werbenetzwerke Nutzerprofile erstellen. Die Rede ist hier häufig vom sogenannten Tracking, dem „Verfolgen“ bzw. Ausspähen von Nutzerinnen und Nutzern über mehrere Webseiten hinweg. Diese Daten sind nicht nur für Marketingzwecke attraktiv, sondern auch für Kriminelle. Betrüger können solche Informationen beispielsweise nutzen, um sich leichter Zugriff auf Online-Konten zu verschaffen, in Ihrem Namen Waren zu bestellen oder mit Hilfe Ihrer gestohlenen Identität Straftaten zu begehen.

Welche Maßnahmen Sie treffen können, damit Sie sich sicherer im Netz bewegen, zeigen wir Ihnen hier.



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

Beauftragt vom

Ministerium für Wirtschaft, Innovation,
Digitalisierung und Energie
des Landes Nordrhein-Westfalen





ANTWORTEN AUF DIE WICHTIGSTEN FRAGEN



WARUM DEN BROWSER STÄHLEN?

Die Privatsphäre von Internetnutzenden wird durch Tracking aktiv verletzt.

- Cookies und Werbenetzwerke machen uns auch über mehrere Endgeräte hinweg nachverfolgbar.
- Was mit Informationen über Sie im Detail passiert, ist unklar.

Angezeigte Werbung auf Webseiten wird von zentralen Werbeservern verteilt.

- Diese besitzen mehr Informationen über die Besucher einer Webseite als die Webseite selbst.

WARUM DEN BROWSER STÄHLEN?

Über Websites können schadhafte Inhalte auf einen PC geladen werden.

Manche Webseiten können trotz SSL- oder TLS-Verschlüsselung ohne Verschlüsselung aufgerufen werden.

- Besuchte Webseiten und ggf. Informationen können von Hackern abgegriffen werden.

Der Browser wird häufig genutzt, um Passwörter zu Online-Diensten zu speichern.

- Hacker bekommen dadurch aber leichteren Zugriff auf gespeicherte Passwörter.



DEN BROWSER ABSICHERN – DIE WICHTIGSTEN SCHRITTE

SCHRITT 1 - EINSTELLUNGEN

Passwörter, Adressdaten und Zahlungsinformationen sollten nicht im Browser gespeichert werden.

Die entsprechenden Funktionen, die das Speichern dieser Daten und das automatische Ausfüllen anbieten, sollten deaktiviert werden.

SCHRITT 2 – ADD-ONS INSTALLIEREN

Erweiterungen für den Browser, sogenannte Add-Ons, helfen beim Schutz vor Gefahren und vor Brüchen der Privatsphäre. Sie können die Sicherheit der Endgeräte während des Surfs erhöhen. Folgende Add-Ons helfen dabei:

1. HTTPS EVERYWHERE

Erzwingt den Aufruf einer verschlüsselten Verbindung zur jeweiligen Webseite, sofern die Website dies anbietet (fast immer).

2. UBLOCK ORIGIN

Blockiert Werbung und Tracker.

- Werbung kann mit Viren belastet sein und wird damit blockiert.
- Tracker verletzen die Privatsphäre und ermöglichen eine Nachverfolgung des Benutzers im gesamten Internet.

3. PRIVACY BADGER

Blockiert Cookies und Tracker von Betreibern, die Besucher über mehrere Webseiten hinweg verfolgen.

SICHERER BROWSER – EIN MUSS FÜR JEDEN!

Ein abgesicherter und „gestählter“ Browser ist wichtig, wenn es um das Surfen im Web geht. Dieser ist auf jedem PC / Laptop installiert, wird tagtäglich aktiv genutzt und ist gerade deshalb vielen unterschiedlichen Bedrohungen ausgesetzt.

Wie Sie Ihren Browser gegen Bedrohungen absichern, zeigen wir Ihnen Schritt für Schritt in unserer Videoanleitung, die Sie über den QR-Code erreichen!



**DIGITAL
SICHER
NRW**

Kompetenzzentrum für
Cybersicherheit in der Wirtschaft

Beauftragt vom

Ministerium für Wirtschaft, Innovation,
Digitalisierung und Energie
des Landes Nordrhein-Westfalen



Erklärvideos Browser