**IT - News im März 2015**

# Sicherer Surfen mit den richtigen Einstellungen für Ihren Browser

**Browser sind beliebte Ziele für Angriffe. Ob Chrome, Safari, Firefox oder Internet Explorer - mit diesen Tipps bewegen Sie sich sicherer im Netz.**

Ähnlich wie bei einem Betriebssystem oder der Antivirus-Software sind Updates auch bei Browsern Pflicht. Falls ein Hersteller Sicherheitsaktualisierungen herausgibt, sollten diese immer sofort installiert werden. Aktivieren Sie wenn möglichst die automatischen Updates.

**So geht das bei den gängigsten Browsern:**

- **Firefox:** «Extras / Einstellungen / Erweitert / Update / Updates automatisch aktualisieren» Unter dem Menüpunkt «Hilfe / Über Firefox» kann jederzeit überprüft werden, ob die aktuellste Version des Browsers installiert ist.
- **Chrome:** Automatische Updates sind Standard. Chrome wird jedes Mal aktualisiert, wenn eine neue Version des Browsers verfügbar ist. Manuelle Suche nach Aktualisierungen ist möglich: Im Hauptmenü wählen Sie «Über Google Chrome» aus. Um die neue Version zu installieren, klicken Sie auf «Neu starten
- **Internet Explorer:** Aktualisiert sich selbst, wenn das automatische Update von Windows aktiviert ist. Ansonsten können Sie im Internet Explorer auf «Extras / Windows Update» oder in der Menüleiste auf «? / Info» klicken.
- **Safari:** Auch bei Safari werden Updates automatisch vorgenommen, wenn die Softwareaktualisierung unter Mac OS X aktiviert ist. Windows-Benutzer sollten Safari nicht mehr verwenden, da der Apple-Browser für Windows nicht mehr weiterentwickelt wird.

### Schutz vor Angriffen

Die meisten Browser enthalten Schutzfilter, um Phishing- und Malwareattacken abzuwehren. In den Sicherheitseinstellungen legen Sie auch fest, ob Passwörter gespeichert werden sollen. Natürlich ist es komfortabel, Passwörter nicht jedes Mal eintippen zu müssen. Wir empfehlen aber, Passwörter im Browser nie zu speichern.

- **Firefox:** Die Einstellungen sind unter «Extras / Einstellungen» aufgelistet. Setzen Sie unter «Sicherheit» alle drei Häckchen bei den Kontrollkästchen, damit der Browser Sie vor gefährlichen Seiten warnt. In den Einstellungen legen Sie ausserdem fest, ob Firefox-Passwörter speichert.
- **Internet Explorer:** Den Filter aktivieren Sie in den Internetoptionen auf dem Seitenreiter «Datenschutz». Wählen Sie dort die Option «Ein für SmartScreen». Unter «Inhalte

/ Einstellungen» lässt sich einstellen, dass Internet Explorer vor dem Speichern von Passwörtern nachfragt.

- **Chrome:** Im Hauptmenü klicken Sie auf «Erweiterte Einstellungen anzeigen» und gehen Sie zum Bereich «Datenschutz». Aktivieren Sie das Kontrollkästchen «Phishing- und Malware-Schutz aktivieren». Im Abschnitt Passwörter und Formulare befindet sich auch die Option «Speicherung Ihrer Web-Passwörter anbieten».
- **Safari:** In die Einstellungen gelangt man via «Sicherheit». Wie bei Firefox warnt der Browser vor Seiten mit betrügerischen Inhalten. In den Einstellungen befindet sich ein Seitenreiter «Kennwörter». Falls Sie Passwörter nicht speichern wollen, entfernen Sie hier die Häkchen «Benutzernamen und Kennwörter automatisch ausfüllen» bzw. «Autom. ausfüllen auch für Websites erlauben, die verlangen, Kennwörter nicht zu sichern.»

## Cookies löschen

Viele Webseiten, platzieren Cookies, um Benutzer wiederzuerkennen. Diese können missbraucht werden, um Ihr Surfverhalten zu verfolgen. Am sichersten sind Sie, wenn Sie Cookies nach jeder Sitzung automatisch löschen.

- Cookies von Drittanbietern, die durch Werbebanner oder PopUps eingeschleust werden, sollten generell nicht zugelassen werden. Vertrauenswürdigen Anbieter, sollten als Ausnahmen hinzugefügt werden. Browser bieten die Möglichkeit, einer Website mitzuteilen, dass man nicht verfolgt werden möchte.

## So verwalten Sie Cookies

- **Firefox:** «Unter Extras / Einstellungen / Datenschutz / Verfolgung von Nutzeraktivitäten / Websites mitteilen, meine Aktivitäten nicht zu verfolgen» anwählen. «Unter Chronik / Firefox wird eine Chronik / nach benutzerdefinierten Einstellungen anlegen». Bei «Cookies von Drittanbietern akzeptieren» wählen Sie «nie». Unter «Ausnahmen» vertrauenswürdige Sites hinzufügen. Im Dropdown «Behalten, bis» wählen Sie «Firefox geschlossen wird».
- **Chrome:** Unter «Hauptmenü / Einstellungen / Erweiterte Einstellungen anzeigen / Datenschutz / Inhaltseinstellungen», aktivieren Sie das Kontrollkästchen «Drittanbieter-Cookies und Website-Daten blockieren». Unter «Ausnahmen verwalten» können jeweilige festgelegt werden.
- **Internet Explorer**: Unter «Extras / Internetoptionen / Datenschutz / Einstellungen» die Werte «mittelhoch» oder «hoch» aus, um Cookies von Drittanbietern auszuschliessen. Unter «Sites» können Sie Datenschutz-Einstellungen für einzelne Seiten vornehmen.
- **Safari:** Bei «Einstellungen / Datenschutz / Cookies und andere Website-Daten unterdrücken» wählen Sie «Von Dritten oder Werbeanbietern».

## Add-ons auf Aktualität prüfen

Was für den Browser gilt, ist auch für installierte Add-ons (Erweiterungen) relevant. Diese speziell für den Browser entwickelten Programme rüsten diesen mit Zusatzfunktionen aus. Eine Übersicht über populäre Add-ons gibt es für Firefox, Chrome, Internet Explorer und Safari.

- **Firefox:** Infos zu installierten Add-ons finden Sie unter «Extras / Add-ons». Unter dem Zahnrädchen klicken Sie «Auf Updates überprüfen», die alle installierten Add-ons auf Aktualität prüft.
- **Chrome:** Im Hauptmenü «Über Google Chrome» klicken Sie auf «Erweiterungen». Wenn ein Update für eine Erweiterung vorhanden ist, erscheint «Aktualisieren».
- **Internet Explorer:** Unter «Extras / Add-Ons verwalten» werden Sie fündig. Klicken Sie unter «Anzeigen» auf «Alle Add-Ons», danach wählen Sie beim Add-On «ActiveX aktualisieren», um das Add-on mit der aktuellen Version zu ersetzen. Diese Option ist nicht für alle Add-ons verfügbar.
- **Safari:** Die Erweiterungen sind unter dem Menüpunkt «Safari / Einstellungen» aufgelistet. Sie können Updates manuell installieren und die Option für das automatische Aktualisieren jederzeit wieder einschalten.

Quelle: Bluewin