# Drive-By-Download

**Das alleinige Aufrufen einer infizierten Webseite genügt, um Ihr Gerät zu infizieren. Vielfach beinhalten die betroffenen Webseiten seriöse Angebote und sind zwecks Verteilung der Malware kompromittiert worden. Doch man kann sich schützen.**

**Schützen Sie sich vor Drive-By-Downloads, indem Sie:**

- immer die aktuellen Versionen des Browsers sowie dessen Plug-Ins (Adobe Flash Player, Java etc.) verwenden.
- das Betriebssystem sowie alle installierten Programme (Office, Adobe Acrobat Reader etc.) aktuell halten.
- stets den Virenscanner aktualisieren und regelmässig die Festplatte auf Viren überprüfen.

## Gefahr durch Drive-By-Downloads

Webseiten werden teilweise durch Hacker gezielt manipuliert, indem diese Schwachstellen ausnützen. Die Betreiber der Webseite merken davon oft über längere Zeit nichts.

Die nachfolgenden Punkte zeigen auf, was ein Drive-By-Download so gefährlich und unberechenbar macht:

1. Ein Gerät wird alleine durch den Besuch einer verseuchten Webseite mit Schadcode infiziert, d.h. der Besucher braucht keinen Download zu starten oder explizit etwas zu installieren.
2. Der Download der Malware wird beim normalen Aufruf der Website automatisch im Hintergrund gestartet. So werden Firewalls überbrückt und bieten diesbezüglich keinen Schutz.
3. Nicht nur zwielichtige, sondern auch seriöse, bekannte und oft besuchte Webseiten könnten mit Schadcode infiziert sein.

## Gegenmassnahmen

Zum Schutz sollten Sie immer die aktuellste Version des Browsers sowie aller Plug-Ins (Hilfsprogramme, welche die Funktionalitäten des Browsers erweitern) verwenden.

Eine weitere wichtige Schutzmassnahme ist ein stets aktuelles Antivirenprogramm. Da viele Viren komprimiert heruntergeladen werden und sich erst auf dem Gerät des Benutzers auspacken, können diese durch den Virenscanner nicht immer entdeckt werden. Deshalb ist es unerlässlich, die Festplatte einer regelmässigen (z.B. wöchentlichen) vollständigen Virenprüfung zu unterziehen.

## Webseiten prüfen

Norton (Symantec) stellt auf ihrer Webseite einen Dienst zur Verfügung, mit welchem Sie den Status der Sicherheit (und allfällige Bedrohungen) bekannter Webseiten erfahren können.

Öffnen Sie hierzu die Webseite Norton Safe Web (https://safeweb.norton.com/?ulang=deu) und tippen Sie die Adresse der gewünschten Webseite in das vorgesehene Feld ein. Sie erhalten die Bewertung der Webseite von Norton.

*Unter Drive-By-Download versteht man die Infektion eines Gerätes mit Malware (z.B. Viren, Trojaner) allein durch den Besuch einer Webseite. Dabei werden in der Regel Schwachstellen des Browsers oder dessen Plug-Ins ausgenutzt.*

## Weiterführende Informationen für Interessierte

### Technik

Webseiten beinhalten heute häufig dynamische Funktionen, die mittels Technologien wie JavaScript, Java, Adobe Flash etc. realisiert werden. Diese Techniken erlauben die ständige Kommunikation zwischen Browser und Webserver während einer Sitzung (Dauer, die ein Besucher auf der Webseite bleibt), ohne dass der Besucher eine Aktion ausführen muss. Dies wird z.B. eingesetzt, um Werbebanner auszutauschen, Listen zu laden oder Daten an den Webserver zu übertragen.

Üblicherweise werden diese Aktionen in einer sogenannten «Sandbox» des Browsers ausgeführt. Eine Sandbox ist in der Regel ein Bestandteil des Browsers oder eines Plug-Ins, um das Gefahrenpotential im Internet zu verringern. Hierbei wird unbekannten Skripts ein abgeschlossener Bereich zur Verfügung gestellt, in welchem sie sicher ausgeführt werden können (d.h. nur begrenzten Zugang z.B. zur lokalen Festplatte haben).

Wenn nun aber der Browser oder eines der Plug-Ins eine entsprechende Sicherheitslücke aufweist, können solche Skripts direkt auf das Gerät des Benutzers zugreifen. Somit ist es möglich, dass Malware ohne eine bewusste Aktion des Webseitenbesuchers vom Webserver zum Browser und über die Sicherheitslücke auf das Gerät des Benutzers gelangt.

### Schutz durch Deaktivierung von Skriptsprachen?

Wirklich gute Schutzmassnahmen gegen Drive-By-Downloads existieren zurzeit keine. Um die Sicherheit weiter zu erhöhen, könnten die Skriptsprachen deaktiviert werden. Dies ist allerdings eine nicht wirklich praxistaugliche Lösung, da rund 95 Prozent aller Webseiten auf oben genannte Technologien angewiesen sind und somit sehr viele Seiten nicht mehr korrekt angezeigt werden könnten.