

Gefährliche Webseiten – Systeme vor Angriffen schützen

Viren, die sich in **Downloads** und hinter böartigen Links, **Bannerwerbung** und **Pop-up-Fenstern** verstecken. Formulare, die Ihre Passwörter abfangen: **Das Internet kennt viele Gefahren** – und Cyberkriminelle tausend Wege, um an Ihre vertraulichen Daten und Informationen zu gelangen.

Viele Fallen können Sie durch Vorsicht und umsichtiges Verhalten bei der Nutzung von Internetseiten und -diensten umgehen. Wenn Sie aber doch einmal unachtsam sind oder auf einen perfiden Trick hereinfallen, sollten **alle offenen Türen** in Ihrem Browser und Ihrem System **bestmöglich verschlossen** sein, durch die Cyberkriminelle nach Ihren Daten greifen können.

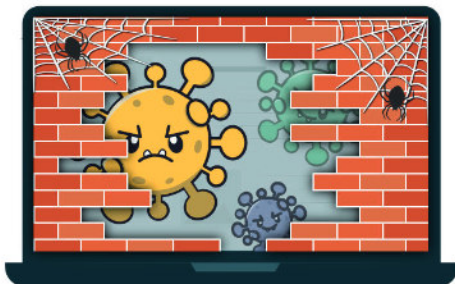


Aber welche Türen sind das? Und wie können Sie sie schließen?



Schauen Sie sich einmal an, wie **IT-Sicherheitsexpertin Ronja** ihren Rechner gegen Cyberangriffe und Datenverluste abgesichert hat.

Veraltete Browser und Systeme



Computerviren und andere Schadprogramme nutzen geschickt offene Sicherheitslücken in Browsern und Betriebssystemen aus. Sie nisten sich ein, leiten Datenströme um und manipulieren Informationen, die auf Ihrem Rechner gespeichert sind. Und verbreiten sich rasend schnell in angeschlossene Systeme.

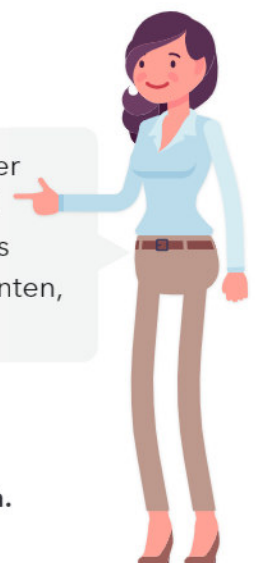
Ronja sagt: „Für den Zugriff auf das Internet verwende ich einen **modernen Browser** der neuesten Generation. Ich Sorge auch dafür, dass alle meine Programme stets aktuell bleiben, und installiere alle **Sicherheitsupdates** – sowohl für den **Browser** als auch für das **Betriebssystem**. Dadurch werden effektiv Lücken geschlossen, die Viren ausnutzen könnten, um Unheil anzurichten.“



Verwenden Sie moderne Browser und Betriebssysteme.



Installieren Sie alle Sicherheitsupdate, die Ihnen zur Verfügung gestellt werden.



Unsichere Programme



Jede Software, die auf Ihrem Rechner installiert ist, stellt eine potenzielle Gefahr für die Sicherheit Ihrer Daten dar. Cyberkriminelle versuchen darin Sicherheitslücken und offene Schnittstellen ausfindig zu machen und durch Viren und andere Schadprogramme auszunutzen.

Ronja sagt: „Nicht jedes Programm wird auch optimal und schnell vom Hersteller gewartet. **Sicherheitslücken** werden oftmals erst spät geschlossen - oder überhaupt nicht! Mit jedem Programm, das Sie auf Ihrem Rechner installiert haben, steigt daher die Wahrscheinlichkeit, dass ein **Virus** diese Schwachstellen finden und ausnutzen kann. Darum habe ich von meinem System alle **Programme und Browser-Plugins** verbannt, die ich **nicht wirklich benötige**.“



Deinstallieren Sie Programme und Browser-Plugins, die Sie nicht wirklich benötigen.



Erweiterte Rechte auf Internetseiten



Internetseiten können Zugriff z. B. auf die Kamera oder das Mikrofon anfordern, die in Ihrem Rechner installiert sind. Cyberkriminelle machen sich das zunutze. Sie hören Ihre vertraulichen Gespräche ab oder filmen Ihre Tastatur, wenn Sie Passwörter zu vertraulichen Diensten und Systemen eingeben.

Ronja sagt: „Meinen Browser habe ich so eingestellt, dass er mich informiert, bevor eine Webseite auf meine **Kamera** oder mein **Mikrofon** zugreifen möchte. Den **Zugriff** gestatte ich nur, wenn ich mir ganz sicher bin, der Webseite vertraue und die Freigabe der Funktionen auch wirklich **sinnvoll und notwendig** erscheint. Und sollte es doch einmal einem Schadprogramm gelingen, diese Sperre zu überlisten, habe ich die Kameralinse an meinem Laptop vorsorglich abgeklebt.“



Gestatten Sie erweiterte Rechte (z. B. den Zugriff auf Kamera und Mikrofon) nur, wenn Sie der Internetseite vertrauen und der Zugriff notwendig erscheint.



Unsichere Werbebanner



Mit Hilfe psychologischer Tricks in Werbebannern auf Internetseiten, versuchen Cyberkriminelle Sie zum Klick auf Links zu animieren. Geben Sie hier nicht acht, landen Sie möglicherweise auf böartigen Seiten oder starten den Download einer vireninfectierten Software.

Ronja sagt: „Ok, **Werbefilter** sind nicht per se böse oder gefährlich. Oftmals ist es tatsächlich nur Werbung. Dennoch können sich Cyberkriminelle Werbefilter zunutze machen und darüber Schadcode verbreiten. Das nennt man „**Malvertising**“. Manchmal wird der Schadcode sogar direkt ausgeführt – Sie müssen dafür noch nicht einmal auf den Banner klicken!

Ich gehe daher auf Nummer sicher! Ein installiertes **Werbefilter-Plugin** (z. B. Adblock Plus) blockiert sehr zuverlässig alle Werbefilter. So kann eventuell anhängender Schadcode meinen Browser erst gar nicht erreichen.“



Installieren Sie ein geeignetes **Werbefilter-Plugin** oder nutzen Sie die Filtermöglichkeiten Ihres Browsers.



Unsichere http-Verbindungen



Manche Links rufen Internetseiten über das unsichere http-Protokoll auf. Daten, die hierüber übermittelt werden, sind unverschlüsselt und können von Cyberkriminellen auf dem Übertragungsweg leicht abgefangen werden. Besonders Bankverbindungen oder Passwörter, die häufig über Formulare auf Internetseiten übermittelt werden, geraten dabei in große Gefahr, ausgelesen, manipuliert und für kriminelle Zwecke verwendet zu werden.

Ronja sagt: „Mit dem **https-Protokoll** surfe ich grundsätzlich sicherer im Netz. Informationen, die ich mit einer Webseite teile, werden darüber **verschlüsselt** übertragen. Cyberkriminelle, die versuchen die Daten abzufangen, erhalten so nur Zeichensalat.

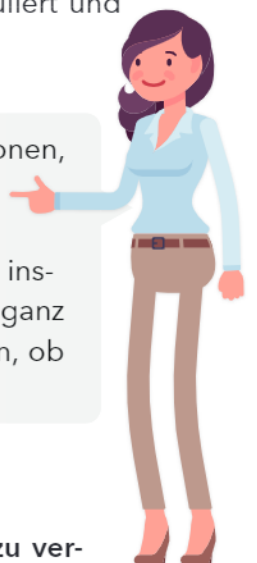
Als kleine Unterstützung habe ich in meinem Browser das Plugin „**HTTPS Everywhere**“ installiert. Es checkt, ob für eine Webseite das https-Protokoll verfügbar ist, und leitet mich ganz automatisch darauf um. So muss ich nicht bei jedem Klick und jedem Link überprüfen, ob gerade das unsichere http- oder das sichere https-Protokoll verwendet wird.“



Surfen Sie sicherer im Netz über das **https-Protokoll**



Nutzen Sie das „**HTTPS Everywhere**“-Plugin, um immer das https-Protokoll zu verwenden, wenn es verfügbar ist.



Alles klar?

Machen Sie es wie IT-Sicherheitsexpertin Ronja:



Schützen Sie den Aufruf von Internetseiten über Ihren Browser,



verwenden Sie verschlüsselte Übertragungsprotokolle,



halten Sie Ihren Rechner sauber



und Ihre Programme immer up to date.

So machen Sie den Cyberkriminellen das Leben schwer und Ihre Ausflüge ins Internet sicherer.

Bleiben Sie wachsam!

