Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Sicheres Surfen im Internet

Inhalt

Inhaltsverzeichnis 3

Neue Web-Technologien 5

Gefahren im Internet 6

Das sichere Surfen 8

Seien Sie achtsam! Geben Sie Hackern keine Chance! 9


Adobe Stock

In unserer modernen Welt ist das Leben ohne Internet kaum mehr vorstellbar. Nahezu alle wichtigen Informationen finden sich heute im „Web“, das mit seinen reichhaltigen Angeboten von Jung und Alt gleichermaßen zum „Surfen“ genutzt wird. Ganz gleich, ob man kabelgebunden oder kabellos im Internet surft, vielfältige Inhalte können betrachtet und heruntergeladen werden oder Geschäfte „Online“ erledigt werden. Besonders attraktiv sind heute die „Sozialen Netzwerke“, bei denen viele Personen freiwillig einen Großteil ihrer privaten Daten abgeben. Hier lauern auch heute und vor allem in Zukunft eine Reihe von Gefahren, die derzeit noch nicht genau erkennbar sind.

Viele Möglichkeiten sind erst durch die Nutzung der neuen Angebote entstanden. Aber gerade diese neuen Angebot bringen Gefahren mit sich, vor denen sich Nutzerinnen und Nutzer wirksam schützen sollten. Jeder Einzelne sollte darauf achten, nicht die eigene Privatsphäre aufs Spiel zu setzen oder verwundbar für Hackerangriffe zu werden.

Web 2.0
Es ist wirklich eine neue Dimension des World-Wide Web, das Web 2.0:
Der Internetnutzer gestaltet das Internet aktiv und nicht nur passiv.
Der Schwerpunkt liegt hier auf dem sozialen Austausch, beispielsweise im Bereich von sozialen Netzwerken oder Internetenzyklopädien.

Gefahren im Internet

Die Nutzung des Internet birgt Gefahren für den PC, das Tablet, das Smartphone etc. und für Sie. Zum Beispiel kann ohne eigenes Verschulden nur beim bloßen Ansehen einer entsprechend präparierten Internetseite bereits Schadsoftware auf Ihr Gerät übertragen werden, die etwa zukünftig eingegebene Passwörter, Bank- oder Kreditkartendaten bei der Eingabe abgreift und diese an Unbekannte übermittelt *(Spyware)*.

Spyware
Als Spyware (zu Deutsch etwa Schnüffelprogramm oder -software) wird Software bezeichnet, die Ihre Daten auf Ihrem Gerät ohne Ihr Wissen oder Ihre Zustimmung ausspioniert.

Diese Daten ermöglichen dann dem Unbekannten z. B. die Plünderung Ihres Bankkontos. Oder Sie werden auf präparierte Internetseiten gelockt, beispielsweise auf eine der eigenen Bank nachempfundenen Webseite. Dort werden Sie zur Eingabe von PIN und TAN veranlasst (Phishing).

Beim Surfen und bei so genannten freien Internetzugängen (z.B. offene WLANs) ist das Sicherheitsrisiko bei der Angabe von persönlichen Daten nicht einzuschätzen. Wegen der nicht nachprüfbaren Sicherheit der verwendeten Systeme und der möglicherweise aktiven Schadsoftware (Spyware) sollten Sie keinesfalls persönliche Informationen und Passwörter eingeben.

Phishing
Phishing (abgeleitet von „Passwort“ und „Fischen“) sind Versuche, über gefälschte WWW-Adressen an Ihre sensiblen Daten zu gelangen. Ein typisches Angriffsgebiet ist das Online-Banking.

Das sichere Surfen

Werden Sie aktiv, erkennen Sie die beschriebenen Bedrohungen und Angriffe und treffen Sie Vorkehrungen, um die Kontrolle über Ihren eigenen Geräte zu behalten und die „Übernahme“ durch Angreifer sicher zu verhinderen. Dabei ist es vor allem wichtig, Ihre eigenen Geräte und die dort für die Internetnutzung verwendeten Programme immer aktuell zu halten und somit die Ausnutzung bekannt gewordener Sicherheitslücken zu verhindern. Nachfolgend finden Sie eine Auflistung der wichtigsten Regeln für sicheres Surfen im Internet. Die Einstellung Ihres Webbrowsers ist dabei sehr wichtig, dazu finden Sie Informationen z. B. auf der Internetseite für Bürger beim Bundesamt für Sicherheit in der Informationstechnik **(https://www.bsi-fuer-buerger.de)**.

Seien Sie achtsam! Geben Sie Hackern keine Chance!

- Installieren und aktivieren Sie eine **Firewall** auf dem PC und aktualisieren Sie diese regelmäßig.
- Installieren und aktivieren Sie ein **Anti-Virenprogramm** auf PC, Smartphone und Tablet und aktualisieren Sie dieses regelmäßig.
- Laden Sie regelmäßig **System-Updates** für Ihre Geräte herunter und installieren Sie diese.
- Gehen Sie sorgfältig mit Ihren **Benutzernamen und Kennwörtern** um. Dazu gehören neben dem Bereich des Online-Bankings auch Zugangsdaten für soziale Netzwerke, Online-Shops und ähnliche Webseiten.

Cookie
Ein Cookie (zu Deutsch: „Keks“ oder „Plätzchen“) ist eine kleine Datei, die beim Surfen im Internet auf dem eigenen Gerät abgelegt wird. Cookies erlauben es einem Anbieter, auf Ihrem Gerät Informationen zu hinterlegen und entsprechend Ihrem Surfverhalten Nutzerprofile anzulegen.

- **Flash** ist eine veraltete Technologie und oft ein Einfallstor für Schadsoftware. Deinstallieren Sie den Flash-Player oder stellen Sie zumindestens Ihren Webbrowser so ein, dass vertrauenswürdige Flash Inhalte zum Anzeigen einzeln per Mausklick aktiviert werden müssen.
- **Löschen Sie** *Cookies* und *Flash-Cookies* regelmäßig, am besten nach jeder Sitzung. Das automatisierte Löschen kann oftmals im Browser unter Einstellungen ausgewählt werden.
- **Vermeiden** Sie **Online-Banking** in Internetcafés und an öffentlichen Terminals. Tippen Sie dort generell **keine Passwörter** bei der Internetnutzung ein. Wer Bankgeschäfte per Handy erledigt, sollte sich jedoch nicht die TAN auf dasselbe Gerät schicken lassen.
- **Ändern** Sie Ihre **Passwörter regelmäßig**. Verwenden Sie mindestens 10 Zeichen umfassende, sichere Passwörter, bestehend aus Buchstaben, Ziffern und Sonderzeichen. Speichern Sie Kennwörter, PINs und TANs oder Ihre Kreditkartendaten niemals auf Ihren Geräten.
- Seien Sie achtsam bei E-Mails mit unbekannten Anhängen. **Löschen Sie verdächtige E-Mails sofort** und ohne sie zu öffnen.

Flash-Cookie
Flash-Cookies sind Dateien, die von Webseiten, die Flash einbinden, benutzerspezifische Daten auf Ihr Gerät schreiben und später wieder auslesen können. Flash-Cookies unterliegen denselben Regeln wie die herkömmlichen Cookies. Die Informationsmenge, die sie zu speichern in der Lage sind, ist jedoch um ein Vielfaches größer.

- Laden Sie ausschließlich Programme aus **vertrauenswürdigen Quellen** herunter.
- Achten Sie darauf, dass Seiten zum Online-Banking oder Internetshops **https-verschlüsselt** sind. Haben Sie hierbei ein Augenmerk auf „https“ in der Adresszeile und ein geschlossenes grünes Schloss-Symbol in der Statuszeile des Browsers.
- Digitale Zertifikate bescheinigen die Vertrauenswürdigkeit von Kommunikationspartnern im Internet. Achten Sie z. B. auf einen grünen oder blauen Balken vor der Adresszeile im Webbrowser „Firefox“.
- Erstellen Sie regelmäßig Sicherungskopien Ihrer Dateien auf DVD oder externen Festplatten, die nur für diesen Zweck eingesetzt werden, um einem eventuellen Datenverlust aufgrund einer Infektion vorzubeugen.
- Achten Sie bei der Verwendung von Funknetzen auf die Verschlüsselung Ihrer Kommunikation. Benutzen Sie mindestens den WPA2-Standard. Rufen Sie bei der Verwendung unsicherer Netze keine persönlichen/sensiblen Daten auf und übertragen Sie diese nie ungesichert.

WPA2
Wi-Fi Protected Access 2 ist ein Sicherheitsstandard für Funknetzwerke. Es ist deutlich sicherer als der veraltete Standard (WEP) und sollte daher verwendet werden.

Herausgeber:

Der Bundesbeauftragte für den Datenschutz
und die Informationsfreiheit
Husarenstraße 30
53117 Bonn

Tel. +49 (0) 228 99 77 99-0
Fax +49 (0) 228 99 77 99-5550
E-Mail: referat23@bfdi.bund.de
Internet: www.datenschutz.bund.de

Realisation: Appel & Klinger Druck und Medien GmbH
Bildnachweis: fotolia, iStockphoto, Adobe Stock

Stand: Januar 2019