



Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit



Sicheres Surfen im Internet
– so schützen Sie sich!

http://www



Inhalt

Inhaltsverzeichnis	3
Neue Web-Technologien	5
Gefahren im Internet	6
Schutzmaßnahmen für sicheres Surfen	8
Seien Sie achtsam! Geben Sie Hackern keine Chance!	9





Das Internet hat inzwischen alle Bereiche des täglichen Lebens erschlossen. Dabei wird vor allem das World Wide Web (kurz: WWW oder Web) mit seinen reichhaltigen Angeboten von Jung und Alt gleichermaßen zum „Surfen“ genutzt. Ganz gleich, ob man kabelgebunden oder kabellos im Internet surft, vielfältige Inhalte können betrachtet und heruntergeladen werden. Die neueren Entwicklungen des WWW nennt man *Web 2.0*. Nutzerinnen und Nutzer erstellen, bearbeiten und publizieren Inhalte und wirken so aktiv bei der Gestaltung von Webportalen, sozialen Netzwerken oder Internetenzyklopädien mit.

Viele Möglichkeiten sind erst durch die Entwicklung der neuen Web-Technologien entstanden. Aber gerade diese neuen Technologien 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

Web 2.0 ist ein Schlagwort, welches eine neue Dimension des World Wide Web beschreibt: 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 und für Sie. Zum Beispiel kann ohne eigenes Verschulden nur beim bloßen Ansehen einer entsprechend präparierten Internetseite bereits Schadsoftware auf den heimischen PC übertragen werden, die etwa zukünftig eingegebene Passwörter, Bank- oder Kreditkartendaten bei 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 PC ohne Ihr Wissen oder 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 in Internet-Cafes und bei so genannten freien Internetzugängen ist das Sicherheitsrisiko bei der Angabe von persönlichen Daten nicht einzuschätzen. Wegen der nicht nachprüfaren 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 sensible 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 PC zu behalten und „Übernahme“ durch Angreifer sicher zu verhindern. Dabei ist es vor allem wichtig, das eigene Betriebssystem und die für die Internetnutzung verwendeten Programme (Webbrowser, E-Mail-Programm, PDF-Reader, Flashplayer, etc.) 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** und aktualisieren Sie diese regelmäßig.
- Installieren und aktivieren Sie ein **Anti-Virenprogramm** und aktualisieren Sie dieses regelmäßig.
- Laden Sie regelmäßig **Systemupdates** für Ihr Betriebssystem herunter und installieren Sie diese. Viele Betriebssysteme bieten entsprechende Automatismen an.
- 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.
- **Löschen** Sie *Cookies* und *Flash-Cookies* regelmäßig, am besten nach jeder Sitzung. Das automatisierte Löschen kann oftmals im Browser bei den Einstellungen konfiguriert werden.

Cookie

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





- **Vermeiden Sie Online Banking** in Internetcafes. Tippen Sie dort generell **keine Passwörter** bei der Internetnutzung ein.
- **Ändern Sie Ihre Passwörter regelmäßig.** Verwenden Sie mindestens 8 Zeichen umfassende, sichere Passwörter, bestehend aus Zeichen, Ziffern und Sonderzeichen. Speichern Sie Kennwörter, PINs und TANs oder Ihre Kreditkartendaten niemals auf dem PC!
- Seien Sie achtsam bei E-Mails mit unbekanntem Anhängen. **Löschen Sie verdächtige E-Mails** direkt und ohne sie zu öffnen.
- 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 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 CD-ROM/DVD oder externen Festplatten, 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.

Flash-Cookie

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

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 99-550
E-Mail: ref6@bfdi.bund.de
Internet: www.datenschutz.bund.de

Realisation: Diamond media GmbH
Bildnachweis: dreamstime, fotolia, iStockphoto