

# 10 Sicherheitstipps für Online-Surfer

Der folgende Text informiert Sie in aller Kürze über die Sicherheitsrisiken bei der Nutzung des Internets und gibt Tipps, wie Sie durch Beachtung von 10 einfachen Grundregeln, die vom Bundesministerium für Wirtschaft und Technologie [www.bmwi.de] erarbeitet wurden, die Sicherheit ihres Systems optimieren können.<sup>1</sup>

## Sicher durchs weltweite Datennetz

Wie im realen Leben auch, gibt es bei der Nutzung des Internets Risiken. Genau so wie Sie nicht die Wohnung verlassen, ohne die Tür zu verschließen oder einer unbekannt Person Ihre Kreditkarte überlassen, sollten Sie sich auch vor dem Surfen im World Wide Web mit den Sicherheitsfragen des Internet auseinandersetzen, damit das Online-Surfen für Sie zu einem entspannten Erlebnis ohne unerwünschte Nebenwirkungen wird. Mit der rasant wachsenden Zahl der Internet-Nutzer sowie der steigenden wirtschaftlichen Bedeutung dieses Netzwerks nehmen auch diese Gefahren zu. Lassen Sie sich aber hierdurch nicht abschrecken. Denn es gibt für den normalen Nutzer weitaus weniger Bedrohungen, als gemeinhin angenommen wird (zumindest nicht mehr, als im realen Leben auch). Typische Gefahrenquellen im Internet sind heute:

- Mitlesen und Verändern von Daten aufgrund der offenen Übertragung.
- Viren: kleine Programme, die sich selbständig "vermehren" und Schaden an Ihrem Computersystem anrichten können, z.B. die Festplatte formatieren oder die Leistung bremsen.
- Trojanische Pferde: Programme, die andere Funktionen ausführen, als dem Nutzer bewusst sind, z.B. die Passwortdatei an einen Angreifer übertragen.
- Maskeradeangriffe wie IP- oder Web-Spoofing, bei denen falsche Angaben vorgetäuscht werden.

Sie müssen kein Internet-Profi oder Programmierer sein, um sich gefahrlos durch die neue Online-Welt zu bewegen. Schon wenn Sie die folgenden 10 Grundregeln beachten, können sie Ihre Sicherheit um ein Vielfaches steigern.

## 10 Grundregeln für Ihre Sicherheit im Internet

Regel Nr. 1    Machen Sie einen persönlichen Sicherheitscheck

Regel Nr. 2    Überlegen Sie genau, wer Ihr Vertrauen verdient

Regel Nr. 3    Speichern Sie sensible Daten (Passwörter, Kreditkartennummern usw.) nicht auf Ihrer Festplatte ab

---

<sup>1</sup> Eine entsprechendes Faltblatt ist ebendort erhältlich.

- Regel Nr. 4 Betrachten Sie Programme aus dem Internet zunächst grundsätzlich als unzuverlässig
- Regel Nr. 5 Nutzen Sie nur die aktuelle Version Ihrer bevorzugten Internet-Zugangssoftware
- Regel Nr. 6 Aktivieren Sie die Sicherheitsoptionen Ihres Internet-Browsers
- Regel Nr. 7 Setzen Sie zusätzliche Sicherheitssoftware ein
- Regel Nr. 8 Übermitteln Sie sensible Daten über offene Leitungen niemals unverschlüsselt
- Regel Nr. 9 Machen Sie regelmäßige Sicherheitskopien (Backups) von Ihren Datenbeständen
- Regel Nr. 10 Konfigurieren Sie sich einen eigenen Internet-PC (für Power-Surfer)

### **Regel Nr. 1: Machen Sie einen persönlichen Sicherheitscheck**

Nehmen Sie sich, bevor Sie Ihren neuen Internet-Anschluss aktivieren, einige Minuten Zeit und machen Sie einen persönlichen und realistischen Sicherheitscheck. Nutzen Sie die Sicherheitseigenschaften des Betriebssystems und installieren Sie keine überflüssigen Server-Software, durch die der Rechner erst von außen erreichbar wird. Vor allem: Welchen Schaden verkraften Sie, wenn trotz aller Vorsicht etwas schief geht? Hier gilt z.B.: Ein PC, der größere Mengen sensibler Daten speichert (z. B. den Geschäftsverkehr eines Rechtsanwaltes), sollte nicht als Internet-PC eingesetzt werden. Außerdem: ein Online-Shopper wird sich vor allem um die Sicherheit bei der Übermittlung seiner Kreditkartennummer kümmern, während diejenigen, die gerne in den Internet-Programmsammlungen stöbern, sich vorwiegend mit der Wirksamkeit von Antiviren-Programmen auseinandersetzen sollten. In jeden Fall heißt es: Bleiben Sie realistisch. Nicht überall im Internet lauern Piraten, die es nur darauf abgesehen haben, Ihre privaten E-Mail zu lesen. Nicht jeder "Chat-Partner" ist darauf aus, Sie um Ihre Ersparnisse zu erleichtern.

### **Regel Nr. 2: Überlegen Sie genau, wer Ihr Vertrauen verdient**

Denn nicht jeder ist im Internet das, was er zu sein vorgibt. Für Experten ist es vergleichsweise einfach, z. B. eine E-Mail-Adresse zu fälschen oder eine ganze Web Site vorzugaukeln - sogar die Ihrer Hausbank, der Sie Ihre Kundendaten mitteilen, um sich auszuweisen. Vorsicht ist ebenso angebracht bei manchem günstigen Angebot im Web. Die Seriosität des Anbieters kann schwer zu überprüfen sein. Vergleichen Sie also regelmäßig die Adressen, die Sie in der sog. URL-Leiste angeben (oder des Links, den Sie anklicken), mit den Angaben, die Sie in der Task-Leiste sehen. Diese Angaben sind schwieriger zu fälschen. Und darüber hinaus: geben Sie Informationen nur preis, wenn Sie verlässlich wissen, wer diese Daten erhält und was mit diesen geschehen soll. "Social Engineering", d. h. Erschleichung von Auskünften bei potentiellen Opfern, ist bei Hackern beliebt, um an benötigte Informationen zu kommen ("Entschuldigen Sie, ich heiße Meyer, bin Sicherheitschef bei X-Online und brauche Ihr Passwort, um Sicherheitstests durchführen zu können.").

**Regel Nr. 3: Speichern Sie sensible Daten (Passwörter, Kreditkartennummern usw.) nicht auf Ihrer Festplatte ab**

Denn der Zugriff auf die Festplatte steht nicht nur dem PC-Eigentümer offen; solange Sie online sind, können sich grundsätzlich auch außenstehende Dritte ein Bild von Ihren Datenspeicher machen. Dies erfordert zwar überdurchschnittliches Expertenwissen, doch Ihr Computer hat im Netz eine eigene Adresse und ist damit zugänglich auch für "Kontaktangebote" der unerwünschten Art. Ein wichtiger Tipp für Windows 9x-Nutzer: Speichern Sie vor allem Ihr Passwort für den Anwählvorgang nicht ab; so erschweren Sie den Aufbau unerwünschter Internet-Verbindungen. Am besten trennen Sie die Leitung nach Abschluss Ihrer Online Sitzung auch "physikalisch", d.h. lösen das Modem- bzw. ISDN-Kabel zwischen PC und Telefonanschluss.

**Regel Nr. 4: Betrachten Sie Programme aus dem Internet zunächst grundsätzlich als unzuverlässig**

Denn Sie können kaum sicher beurteilen, ob die Quelle seriös ist. Mit Programmen, die aus dem Internet auf die heimische Festplatte geladen werden, können Viren oder Trojanische Pferde übertragen werden. Dies kann auch durch das Öffnen eines Anhangs einer elektronischen Mail geschehen. Deshalb öffnen Sie solche Anhänge nicht, während Sie gerade online sind. Speichern Sie den Inhalt zuerst ab, prüfen Sie ihn mit entsprechenden Programmen oder durch Kontrolle des Quellcodes (z. B. bei einem JavaScript-Programm) und öffnen Sie erst dann die fragliche Datei. Testen Sie unbekannte Programme, falls möglich, auf einem Zweitrechner. Und beobachten Sie aufmerksam, ob es dabei zu "Überraschungen" kommt, wie z.B. Warnmeldungen Ihres PCs oder nicht von Ihnen veranlasste Einwahlversuche.

**Regel Nr. 5: Nutzen Sie nur die aktuelle Version Ihrer bevorzugten Internet-Zugangsoftware**

Denn nur die jeweils aktuellen Versionen der gängigen Internet-Software können gewährleisten, dass die bis dahin bekannt gewordenen Sicherheitslücken in diesen Programmen geschlossen sind. Fast täglich werden neue Sicherheitsprobleme entdeckt, zu schnell um jeweils mit neuen Versionen des ganzen Programms darauf zu antworten. Nicht zuletzt deshalb arbeiten die Programmierer der großen Hersteller stets mit Hochdruck daran, sog. "Bug-Fixes" zu entwickeln, d. h. kleine Programme, mit denen sich diese konkreten Probleme beheben lassen. Informieren Sie sich deshalb regelmäßig über die neueste Entwicklung: die meisten Hersteller unterhalten entsprechende Informationsdienste. Überlegen Sie sich genau, ob Sie Zusatzprogramme, z. B. zum Darstellen von 3D-Welten oder zum Audio-Empfang in Ihren Web-Browser einbinden wollen. Denn auch solche Zusatzprogramme, sog. Plug-Ins, können zusätzliche, unkontrollierbare Sicherheitslücken eröffnen.

**Regel Nr. 6: Aktivieren Sie die Sicherheitsoptionen Ihres Internet-Browsers**

Denn Ihre Sicherheit im Internet lässt sich beträchtlich steigern, wenn Sie die Sicherheitsoptionen Ihres Internet-Browser intelligent einsetzen. Wichtig ist hier vor

allem, dass Sie die Zulassung von ActiveX-Controls ausschließen und die Ausführung von Java-Applets nur nach Rückfragen gestatten. Bei diesen sog. "aktiven Inhalten" handelt es sich um kleine eigenständige Programme, die auf Ihrem PC ausgeführt werden und dort u. U. ein unkontrollierbares Eigenleben entwickeln können (z.B. Ihre Passwortdatei per E-Mail versenden). Ob Sie die sog. "Cookies" ausschließen wollen, müssen Sie ganz individuell entscheiden. Im Zweifel entscheiden Sie sich gegen solche "Kekse", die eine fremde Web Site auf Ihrer Festplatte ablegt, denn diese Daten können auch dazu genutzt werden, um Benutzerprofile anzulegen.

#### **Regel Nr. 7: Setzen Sie zusätzliche Sicherheitssoftware ein**

Denn manche Sicherheitsprobleme lassen sich nicht alleine "mit Bordmitteln" lösen. Wichtigstes Zusatzwerkzeug: ein leistungsfähiger Virenschanner, der in der Lage ist, auch neue Viren zu erkennen. Fast täglich werden neue Viren entdeckt und es ist durchaus möglich, dass Sie sich bei einem Ausflug in die Online-Welt "infizieren". Bei weiterer Sicherheitssoftware sollten Sie ernsthaft prüfen, vor welchen konkreten Gefahren Sie sich dadurch schützen wollen und vor allem, ob das Kosten/Nutzen-Verhältnis stimmt. Denn hierbei gilt ebenfalls: absolute Sicherheit kann es auch im Internet nicht geben - selbst wenn manche Hersteller das versprechen.

#### **Regel Nr. 8: Übermitteln Sie sensible Daten über offene Leitungen niemals unverschlüsselt**

Denn jede Datenübertragung im Internet kann von potentiellen Angreifern grundsätzlich abgefangen und ausgespäht werden. Schützen Sie daher Ihre private und geschäftliche Korrespondenz durch den Einsatz sicherer Verschlüsselungsverfahren. Die Qualität hängt dabei nicht nur von der Schlüssellänge und dem verwendeten Algorithmus ab. Auch Verfahren mit 40 Bit Schlüssellänge, wie sie heute teilweise im Einsatz sind, bieten einen gewissen Schutz. Die Verwendung von längeren Schlüsseln ist aber in jedem Fall empfehlenswert. Ein Angreifer mit einer "normalen" Ausstattung, müsste dann erhebliche Mühe aufwenden, um aus dem Kryptogramm den Klartext zu gewinnen - meist mehr Mühe, als es die verschlüsselten Daten wert sind.

#### **Regel Nr. 9: Machen Sie regelmäßige Sicherheitskopien (Backups) von Ihren Datenbeständen**

Dies ist eine der wichtigsten Regeln überhaupt, denn es ist meist zu spät (und wenn, dann sehr teuer), die gespeicherten Informationen zu retten, falls das "Kind erst einmal in den Brunnen gefallen ist". Zum bequemen Datensichern können Sie z. B. eine Wechselfestplatte, einen CD-Brenner, oder ein Streamer-Laufwerk einsetzen. Wichtig ist jedoch, dass Sie regelmäßig (ca. alle zwei Wochen) eine Sicherung der geänderten sowie der neu dazu gekommenen Daten vornehmen. Und bewahren Sie Ihre Backups sicher, d. h. getrennt vom PC, auf.

**Regel Nr. 10: Konfigurieren Sie sich einen eigenen Internet-PC (für Power-Surfer)**

Ganz Sicherheitsbewusste sollten mit einem separaten PC in das Internet starten. Ausstattung: Betriebssystem und Internetzugangsoftware, ggf. ein Virenschutzprogramm. Dann sind Sie in der Tat sicher vor den meisten Bedrohungen, die derzeit vom weltweiten Datennetz bekannt sind. Und internettaugliche PCs sind heute bereits kostengünstig zu haben (Mindestausstattung: 133 MHz, 32 MB RAM, 500 MB Festplatte). Halten Sie sich dennoch zusätzlich an unsere Sicherheitstipps. So kann kaum noch etwas schief gehen bei Ihren Ausflügen in die Online-Welt.

**Weiterführende Informationen**

Die Initiative "Sicherheit im Internet und in der Informationsgesellschaft" bietet eine zentrale Informationsplattform für alle mit der IT-Sicherheit relevanten nationalen und internationalen Fragen. [[www.sicherheit-im-internet.de](http://www.sicherheit-im-internet.de)] Weitere Ausführungen zum Thema Informationssicherheit bietet in Internet das Bundesamt für Sicherheit in der Informationstechnik [[www.bsi.de](http://www.bsi.de)].