Bundesamt
für Sicherheit in der
Informationstechnik

BSI FÜR BÜRGER

INS INTERNET - MIT SICHERHEIT

Surfen, aber sicher!

Basisschutz leicht gemacht

10 Tipps für ein ungetrübtes
Surf-Vergnügen

www.bsi-fuer-buerger.de ▪ www.facebook.com/bsi.fuer.buerger

Ins Internet – mit Sicherheit!

Viele nützliche und wichtige Dienstleistungen werden heute über das Internet in Anspruch genommen. Dazu zählen beispielsweise Bankgeschäfte oder Online-Einkäufe. Aber auch die Kontaktpflege zu Freunden und Familie wird zum Beispiel über soziale Netzwerke einfacher. Neben den vielen Chancen, die das Netz bietet, gibt es aber auch Risiken. Schadsoftware oder Identitätsdiebstahl können großen Schaden anrichten. Wie Sie sich davor schützen, lesen Sie hier.

Die 10 wichtigsten Tipps, die Internetnutzer für ein ungetrübtes Surf-Vergnügen immer beherzigen sollten, haben wir hier für Sie zusammengestellt – Basisschutz leicht gemacht.

Weitere Hinweise und Hilfestellungen bieten wir auf unserer Web-Seite *www.bsi-fuer-buerger.de* an.

Verwenden Sie einen aktuellen Web-Browser

Nutzen Sie nach Möglichkeit einen Web-Browser mit Sandbox-Technologie (engl. übersetzt: „Sandkasten“, das heißt die Software ist vom Rest des Systems weitgehend abgeschirmt), wie beispielsweise Google Chrome. Dadurch ist es für Angreifer aus dem Internet wesentlich schwieriger, Kontrolle über Ihren Rechner zu erhalten.

Deaktivieren Sie Komponenten und Plug-Ins in den Einstellungen Ihres Browsers. Einstellungen (unter anderem „privater Modus“, „Verlauf löschen“, „Cookies nicht für Drittanbieter zulassen“) verringern die Speicherung von vertraulichen Informationen, die Aufschlüsse über Sie und Ihr Verhalten im Web zulassen.

Nutzen Sie ein Programm zum Blockieren von Werbung.

2 Aktualisieren Sie regelmäßig Ihre Software

Verwenden Sie stets eine aktuelle Version des Betriebssystems und der von Ihnen installierten Programme. Spielen Sie umgehend die Sicherheitsupdates für Ihre Software, insbesondere für Ihren Web-Browser und Ihr Betriebssystem ein. Nutzen Sie wenn möglich die Funktion zur automatischen Aktualisierung.

Deinstallieren Sie zudem nicht benötigte Programme. Je weniger Anwendungen Sie nutzen, desto kleiner ist die Angriffsfläche Ihres gesamten Systems.

Verwenden Sie ein Virenschutzprogramm und eine Firewall

Installieren Sie bei Windows-Betriebssystemen ein Virenschutz- und ein Anti-Spyware-Programm und aktualisieren Sie beide regelmäßig. Setzen Sie eine Personal Firewall ein. Diese ist in den meisten Betriebssystemen bereits integriert. Sie schützt bei richtiger Konfiguration vor Angriffen aus dem Internet und verhindert zudem bei einer Infektion des PCs, dass ausspionierte Daten an einen Angreifer übersendet werden können.

Legen Sie unterschiedliche Benutzerkonten an

Schadprogramme haben die gleichen Rechte auf dem PC wie der angemeldete Benutzer. Daher sollten Sie nur dann als Administrator arbeiten, wenn es unbedingt erforderlich ist. Richten Sie für alle Nutzer des PCs unterschiedliche passwortgeschützte Benutzerkonten ein. Vergeben Sie für diese Konten nur die Berechtigungen, die der jeweilige Nutzer für seine Arbeit braucht. So werden auch private Dateien vor dem Zugriff anderer Benutzer geschützt. Surfen Sie im Internet mit einem dieser eingeschränkten Benutzerkonten und nicht als Administrator.

Nutzen Sie unterschiedliche Passwörter und ändern Sie sie regelmäßig

Bewahren Sie alle Passwörter und Benutzernamen sicher auf. Ändern Sie unbedingt von Herstellern voreingestellte Passwörter und wechseln Sie diese in regelmäßigen Abständen. Verwenden Sie unterschiedliche, nicht erratbare Passwörter für die verschiedenen Anwendungen und Dienste. Das Passwort sollte mindestens acht Zeichen lang sein, nicht im Wörterbuch vorkommen und aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen. Unter keinen Umständen sollten Sie Ihr Passwort an Dritte weitergeben.

Müssen Sie sich viele Passwörter merken, nutzen Sie nicht den Passwort-Speicher des Web Browsers. Stattdessen empfiehlt sich ein Passwort Verwaltungsprogramm wie beispielsweise keepass.

6 Seien Sie vorsichtig bei E-Mails und deren Anhängen

Wenn möglich, sollten Sie auf die Darstellung und Erzeugung von E-Mails im HTML Format verzichten. Zudem sollten Sie beim Öffnen von E Mail Anhängen vorsichtig sein. Schadprogramme werden oft über Dateianhänge in E-Mails verbreitet. Im Zweifelsfall fragen Sie lieber beim Absender nach, ob der Anhang tatsächlich von ihm stammt. Nutzen Sie dabei aber nicht die in der E-Mail angegebenen Kontaktmöglichkeiten. Sie könnten gefälscht sein. Ist Ihnen der Absender nicht bekannt, dann seien Sie beim Öffnen von E Mail Anhängen besonders vorsichtig.

7 Laden Sie Daten nur aus vertrauenswürdigen Quellen herunter

Seien Sie vorsichtig, wenn Sie etwas aus dem Internet herunterladen. Vergewissern Sie sich vor dem Download von Programmen, ob die Quelle vertrauenswürdig ist. Nutzen Sie nach Möglichkeit die Web-Seite des jeweiligen Herstellers zum Download.

Seien Sie zurückhaltend mit der Weitergabe persönlicher Daten

Online-Betrüger steigern ihre Erfolgsraten, indem sie ihre Opfer individuell ansprechen: Zuvor ausspionierte Daten, wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld, werden dazu genutzt, Vertrauen zu erwecken. Persönliche Daten gelten heute als Währung im Netz und so werden sie auch gehandelt.

9 Schützen Sie Ihre Daten durch Verschlüsselung

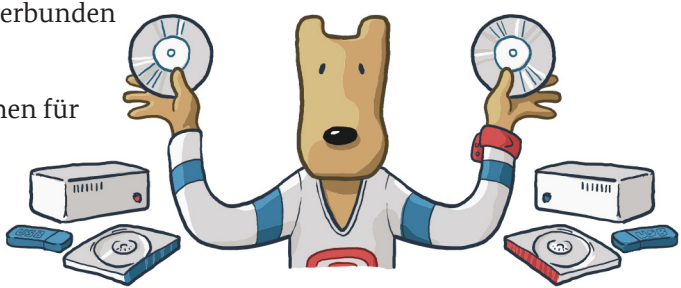
Übertragen Sie Ihre persönlichen Daten ausschließlich über eine verschlüsselte Verbindung, beispielsweise durch die Nutzung des sicheren Kommunikationsprotokolls https. Sie erkennen dies an der von Ihnen aufgerufenen Internetadresse, die stets mit https beginnt und an dem kleinen geschlossenen Schloss-Symbol in Ihrem Web-Browserfenster. Schützen Sie Ihre vertraulichen E-Mails mit Ende-zu-Ende-Verschlüsselung.

Wenn Sie die Übertragungstechnologie Wireless LAN (WLAN) nutzen, achten Sie hier besonders auf die Verschlüsselung Ihrer Kommunikation. Nutzen Sie dazu den aktuellen Verschlüsselungsstandard WPA2 Ihres Routers und wählen Sie ein komplexes, mindestens 20 Zeichen langes Passwort.

10 Fertigen Sie regelmäßig Sicherheitskopien an

Kommt es trotz aller Schutzmaßnahmen zu einer Infektion des PCs, können wichtige Daten verloren gehen. Um den Schaden möglichst gering zu halten, sollten Sie regelmäßig Sicherungskopien Ihrer Dateien auf CD-ROM, DVD, USB Sticks oder auf externen Festplatten erstellen. Diese Datenträger sollten nur bei Bedarf mit dem PC verbunden sein.

Auch Clouddienste können für Online-Backups herangezogen werden.



Surfen, aber sicher!

Basisschutz für den Computer
Die BSI-Checkliste

- ✔ Verwenden Sie einen aktuellen Web-Browser
- ✔ Aktualisieren Sie regelmäßig Ihre Software
- ✔ Verwenden Sie ein Virenschutzprogramm und eine Firewall
- ✔ Legen Sie unterschiedliche Benutzerkonten an
- ✔ Nutzen Sie unterschiedliche Passwörter und ändern Sie sie regelmäßig

- ✔ Seien Sie vorsichtig bei E-Mails und deren Anhängen
- ✔ Laden Sie Daten nur aus vertrauenswürdigen Quellen herunter
- ✔ Seien Sie zurückhaltend mit der Weitergabe persönlicher Daten
- ✔ Schützen Sie Ihre Daten durch Verschlüsselung
- ✔ Fertigen Sie regelmäßig Sicherheitskopien an

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189, 53175 Bonn
E-Mail: mail@bsi-fuer-buerger.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de
www.facebook.com/bsi.fuer.buerger
Telefon +49 (0) 22899 9582-0
Service-Center +49 (0) 800 274 1000

Stand
August 2016

Illustrationen
Leo Leowald

Artikelnummer
BSI IFB 16/250