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 das Erledigen von Bankgeschäften oder Online-Einkäufe, aber auch der Austausch mit Freunden und Familie – zum Beispiel über Soziale Netzwerke oder Messenger. Neben den vielen Chancen, die das Netz bietet, gibt es aber auch Risiken, wie Schadsoftware oder Identitätsdiebstahl, vor denen Sie sich schützen sollten. Wie Sie das machen, lesen Sie hier.

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

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

Verwenden Sie einen aktuellen Webbrowser

Deaktivieren Sie Komponenten und Plug-Ins in den Einstellungen Ihres Browsers. Weitere 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, um sich vor Malvertising, also der Verbreitung von Malware über Werbeeinblendungen, zu schützen.

Tragen Sie die Adressen für besonders sicherheitskritische Webseiten, etwa für das Onlinebanking, zunächst von Hand in die Adresszeile des Browsers ein und speichern Sie die so eingegebene Adresse als Lesezeichen, das Sie ab dann für den sicheren Zugang nutzen.

Halten Sie Ihre Software aktuell

Verwenden Sie eine aktuelle Version des Betriebssystems und der von Ihnen installierten Programme. Nutzen Sie wenn möglich die Funktion zur automatischen Aktualisierung, die oft die Standardeinstellung ist.

Spielen Sie andernfalls umgehend die Sicherheitsupdates für Ihre Software ein, insbesondere für Ihren Webbrowser und Ihr Betriebssystem.

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

Nutzen Sie Virenschutz und Firewall

In den gängigen Betriebssystemen sind ein Virenschutz und eine Firewall integriert, die schon in der Standardkonfiguration Angriffe aus dem Internet erschweren. Aktivieren Sie diese oder verwenden Sie ein Virenschutzprogramm eines anderen Anbieters.

Bedenken Sie, dass diese Maßnahme nur begleitend wirksam sein kann. Ihre Anwendung verringert nicht die Bedeutung der übrigen Tipps dieser Broschüre. Lassen Sie sich nicht durch einen aktivierten Virenschutz oder die Firewall zu Unvorsicht verleiten, sie garantieren keine vollständige Sicherheit.

Legen Sie unterschiedliche Benutzerkonten an

Schadprogramme haben die gleichen Rechte auf dem PC wie das Benutzerkonto, über das sie auf den Rechner gelangt sind. Daher sollten Sie nur dann mit Administratorrechten arbeiten, wenn es unbedingt erforderlich ist.

Richten Sie für alle Nutzerinnen oder Nutzer des PCs unterschiedliche, passwortgeschützte Benutzerkonten ein. Vergeben Sie für diese Konten nur die Berechtigungen, die die jeweilige Nutzerin oder der jeweilige Nutzer für seine Arbeit braucht. So werden auch private Dateien vor dem Zugriff anderer Benutzerinnen oder Benutzer geschützt. Surfen Sie im Internet mit einem der eingeschränkten Benutzerkonten und nicht in der Rolle des Administrators.

Nutzen Sie unterschiedliche Passwörter, die Sie bei Bedarf ändern

Bewahren Sie alle Passwörter und Benutzernamen sicher auf und ändern Sie schnellstmöglich alle Passwörter, die in falsche Hände geraten sein könnten. Verwenden Sie unterschiedliche, nicht erratbare Passwörter für die verschiedenen Anwendungen und ändern Sie die von den Herstellern voreingestellten Passwörter vor der ersten Nutzung.

Es ist wichtig, dass Sie sich ein Passwort gut merken können. Grundsätzlich gilt: Je länger, desto besser. Das Passwort sollte mindestens acht Zeichen lang sein, nicht im Wörterbuch vorkommen und aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen.

Dort, wo eine Zwei-Faktor-Authentisierung angeboten wird, können Sie damit den Zugang zu Ihrem Account absichern. Ein Passwortmanager, wie z. B. keepass, kann die Handhabung unterschiedlicher Passwörter erleichtern.

Geben Sie Ihre Passwörter nicht an Dritte weiter.

Seien Sie vorsichtig bei E-Mails und deren Anhängen

Verzichten Sie, wenn möglich, auf die Darstellung und Erstellung von E-Mails im HTML-Format, und seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen. Besonders wichtig sind diese beiden Tipps bei E-Mails, deren Absender Ihnen nicht bekannt ist, denn Schadprogramme werden oft über in E-Mails integrierte Bilder oder Dateianhänge 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.

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 Webseite 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.

Auch die unbeabsichtigte Weitergabe persönlicher Daten in offenen Netzen sollte vermieden werden. Nutzen Sie in öffentlichen WLAN-Hotspots nach Möglichkeit ein mit Ihrem Heimnetz verbundenes VPN (Virtuelles Privates Netzwerk), da sonst unverschlüsselt übertragene Daten von Dritten mitgelesen werden können. Gleichzeitig schützt ein VPN auch vor einer Reihe weiterer Angriffe auf Ihren Rechner und die darauf gespeicherten Daten.

Schützen Sie Ihre Daten durch Verschlüsselung

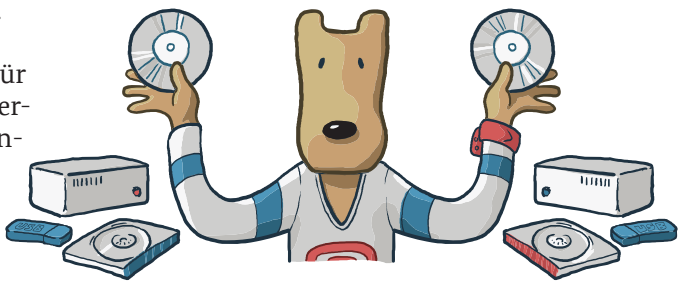
Übertragen Sie Ihre persönlichen Daten ausschließlich über eine verschlüsselte Verbindung, beispielsweise durch die Nutzung des sicheren Kommunikationsprotokolls https. Sie erkennen dies an der von Ihnen aufgerufenen Internetadresse, die stets mit https beginnt, und an dem kleinen geschlossenen Schloss-Symbol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

Wenn Sie die Übertragungstechnologie Wireless LAN (WLAN) nutzen, achten Sie hier besonders auf die Verschlüsselung des Funknetzes. Wählen Sie in Ihrem Router den Verschlüsselungsstandard WPA3 oder, wenn dieser noch nicht unterstützt wird, bis auf Weiteres WPA2. Wählen Sie ein komplexes, mindestens 20 Zeichen langes Passwort.

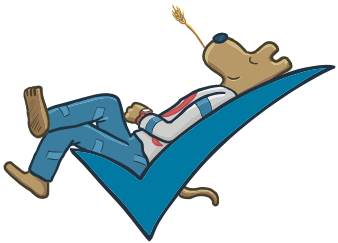
Fertigen Sie regelmäßig Sicherheitskopien an

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

Cloud-Dienste können für Sicherungskopien von verschlüsselten Daten herangezogen werden.



Surfen, aber sicher!



Basisschutz für den Computer
Die BSI-Checkliste

- ✔ Verwenden Sie einen aktuellen Webbrowser.
- ✔ Halten Sie Ihre Software aktuell.
- ✔ Nutzen Sie Virenschutz und Firewall.
- ✔ Legen Sie unterschiedliche Benutzerkonten an.
- ✔ Nutzen Sie unterschiedliche Passwörter und ändern Sie sie bei Bedarf.

- ✔ 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.

Das BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verfolgt das Ziel, die Digitalisierung in Deutschland sicher zu gestalten. Im Sinne des digitalen Verbraucherschutzes sensibilisiert das BSI die Verbraucherinnen und Verbraucher für Sicherheitsrisiken im Cyber-Raum und die sichere Nutzung digitaler Technologien. Mit dem Informationsangebot „BSI für Bürger“ bietet es eine unabhängige und neutrale Anlaufstelle zu Fragen der Informations- und Cyber-Sicherheit.

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
53175 Bonn

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
Juli 2019

Illustrationen
Leo Leowald· www.leowald.de

Artikelnummer
BSI-IFB 19/250