Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

# Das Internet sicher nutzen

*10 Tipps zur sicheren Nutzung des Internets*

Sicher im
digitalen Alltag

# Tipps zur sicheren Nutzung des Internets

Die Möglichkeiten im Internet sind vielfältig und nützlich: Sie können Bankgeschäfte erledigen und in Onlineshops einkaufen, aber sich auch in sozialen Netzwerken mit Freunden und Familie austauschen. Neben den vielen Chancen, die das Netz bietet, gibt es aber auch Risiken, wie Schadsoftware oder Identitätsdiebstahl, vor denen Sie sich schützen sollten.
Zehn wichtige Tipps, die Sie für ein sicheres Surf-Vergnügen beherzigen sollten, haben wir hier für Sie zusammengestellt. Ausführliche Informationen zu den Tipps finden Sie auf den nachfolgenden Seiten dieser Broschüre sowie auf unserer Webseite: bsi.bund.de/internetsicherheit

1. Richten Sie Ihren Webbrowser sicher ein und halten Sie ihn aktuell. Browser-Erweiterungen sollten ggf. deaktiviert oder deinstalliert werden.
2. Halten Sie Ihr Betriebssystem und andere Software aktuell, indem Sie die automatische Installation von Updates zulassen.
3. Nutzen Sie Anwendungen zum Virenschutz und eine Firewall. Einige Betriebssysteme bieten bereits solche Anwendungen an, diese müssen allerdings aktiviert werden.
4. Legen Sie unterschiedliche Benutzerkonten an und verzichten Sie, wenn möglich, auf eine Nutzung des Geräts mit Administratorrechten.
5. Schützen Sie sowohl Ihre lokalen Benutzerkonten wie auch Ihre Online-Konten mit sicheren Passwörtern. Nutzen Sie, wenn möglich, zusätzlich eine Zwei-Faktor-Authentisierung.
6. Seien Sie vorsichtig bei E-Mails sowie den Anhängen und Links, die sich darin befinden. Sie werden auch eingesetzt, um Geräte mit Schadprogrammen zu infizieren oder Daten abzugreifen.
7. Seien Sie vorsichtig bei Downloads, insbesondere wenn es sich dabei um Programme handelt. Laden Sie diese am besten über die Herstellerseiten herunter.

8. Seien Sie zurückhaltend mit der Weitergabe persönlicher Daten und teilen Sie diese nur über verschlüsselte Verbindungen (https).
9. Achten Sie beim Surfen immer auf eine verschlüsselte Verbindung (https). Sie erkennen sie an einem Schlosssymbol oder einer ähnlichen Kennzeichnung in der Adressleiste des Browsers.
10. Fertigen Sie regelmäßig Sicherheitskopien auf externen Speichermedien an.

1

# Passen Sie Ihren Webbrowser an und halten Sie ihn aktuell

Zum Surfen im Internet benötigen Sie einen Browser. Bei Erweiterungen, Add-ons oder auch Plug-ins handelt es sich um kleine Programme, die Ihren Browser mit zusätzlichen Funktionen ausstatten können. Deaktivieren oder deinstallieren Sie die Programme, die Sie nicht unbedingt benötigen. Das ist oftmals über die gleichnamigen Menüpunkte in den Einstellungen Ihres Browsers möglich. Dort können Sie auch weitere Einstellungen zur Sicherheit und zum Datenschutz vornehmen, die die Speicherung von vertraulichen Informationen und ihre Übermittlung an Dritte reduzieren. Als vertraulich gelten Informationen, die Aufschluss über Sie oder Ihr Verhalten im Netz zulassen. „Privater Modus“ oder „Verlauf löschen“ verhindern beispielsweise, dass andere Nutzerinnen und Nutzer desselben Gerätes sehen, welche Internetseiten Sie besucht haben.

„Cookies nicht für Drittanbieter zulassen“ sorgt dafür, dass nur Webseiten Ihr Surfverhalten verfolgen können, die Sie tatsächlich besucht haben.

Achten Sie auch darauf, dass Ihr Webbrowser immer auf dem aktuellen Stand ist. Mit Aktualisierungen werden auch Sicherheitslücken geschlossen.
Nutzen Sie ein Programm zum Blockieren von Werbung, um sich vor Malvertising, also der Verbreitung von Schadsoftware über Werbeeinblendungen, zu schützen.

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

2

# Halten Sie Ihr Betriebssystem und andere Software aktuell

Verwenden Sie eine aktuelle Version des Betriebssystems und der installierten Programme. Nutzen Sie wenn möglich die Funktion zur automatischen Aktualisierung. Ob das Betriebssystem Ihres Computers auf dem aktuellen Stand ist, erfahren Sie in den Einstellungen unter Update. Achten Sie auch auf Hinweise zu neuen Versionen des Betriebssystems oder von Anwendungen.

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

3

# Nutzen Sie Anwendungen zum Virenschutz und eine 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 zur Unvorsichtigkeit verleiten, sie garantieren keine vollständige Sicherheit.

4

# Legen Sie unterschiedliche Benutzerkonten an

Schadprogramme haben die gleichen Rechte auf dem PC wie das Benutzerkonto, über das sie auf den Rechner gelangt sind. Als Administrator haben Sie vollen Zugriff auf fast alle Bereiche Ihres PCs. 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. Je nach Betriebssystem ist dies über die (System-) Einstellungen oder die Systemsteuerung möglich. Vergeben Sie für diese Konten nur die Berechtigungen, die die jeweilige Nutzerin oder der jeweilige Nutzer benötigt. So werden auch private Dateien vor dem Zugriff anderer geschützt. Surfen Sie im Internet mit einem eingeschränkten Benutzerkonto und nicht in der Rolle des Administrators.

5


# Schützen Sie Ihre Online- und Benutzerkonten mit sicheren Passwörtern

Vergeben Sie für jedes Online- und Benutzerkonto ein eigenes, sicheres Passwort und ändern Sie schnellstmöglich alle Passwörter, wenn diese in falsche Hände geraten sein könnten. Ändern Sie auch die von den Herstellern oder Diensteanbietern voreingestellten Passwörter nach der ersten Nutzung.
Diese Kriterien gelten für ein sicheres Passwort:

- Sie müssen sich ein Passwort gut merken können.
- Je länger das Passwort ist, desto besser.
- Das Passwort sollte mindestens acht Zeichen lang sein.
- Für ein Passwort können in der Regel alle verfügbaren Zeichen genutzt werden, also Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.

- Das vollständige Passwort sollte nicht im Wörterbuch vorkommen. Gängige Zahlenfolgen oder Tastaturmuster kommen ebenfalls als sicheres Passwort nicht in Frage.
- Einfache Ziffern oder Sonderzeichen vor oder nach einem normalen Wort zu ergänzen, ist nicht empfehlenswert.

Dort, wo eine Zwei-Faktor-Authentisierung (2FA) angeboten wird, können Sie damit den Zugang zu Ihrem Onlinekonto zusätzlich absichern. Ein Passwortmanager kann die Handhabung unterschiedlicher Passwörter erleichtern.
Besonders wichtig: Geben Sie Ihre Passwörter niemals an Dritte weiter.

Weitere Informationen zu sicheren Passwörtern: **bsi.bund.de/account-schutz**

6

# 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 verwenden Sie stattdessen ein reines Textformat. Die Nutzung des HTML-Formats können Sie über die Einstellungen Ihres Mailprogramms ändern. Seien Sie vorsichtig beim Öffnen von E-Mail-Anhängen oder beim Klick auf einen Link, denn Schadprogramme werden oft über in E-Mails integrierte Bilder oder Dateianhänge verbreitet oder verbergen sich hinter Links. Besonders zu beachten ist das bei E-Mails, deren Absenderin oder Absender Ihnen nicht bekannt ist.

Falls Ihnen eine E-Mail von einem bekannten Absender seltsam vorkommen sollte, fragen Sie lieber bei der Absenderin oder dem Absender nach, ob die E-Mail tatsächlich von ihr oder ihm stammt. Nutzen Sie dabei aber nicht die in der E-Mail angegebenen Kontaktmöglichkeiten. Sie könnten gefälscht sein.

Unerwünschte oder gefährliche E-Mails können Sie an einigen Merkmalen identifizieren: Indem Sie mit der Maus über den Absender fahren oder auf diesen klicken, können Sie beispielsweise erkennen, ob der Absender gefälscht ist. Achten Sie dabei auf wirre Buchstabenfolgen, den Tausch durch optisch ähnliche Buchstaben oder eine ausländische Domain, also die Endung der E-Mail-Adresse. Überprüfen Sie auch die Betreffzeile und den Text der E-Mail auf Sinnhaftigkeit und Rechtschreibung. Betrüger machen hier oft Fehler. Seien Sie zudem skeptisch, wenn eine schnelle Reaktion von Ihnen eingefordert wird.

7

# Seien Sie vorsichtig bei Downloads, insbesondere von Programmen

Seien Sie vorsichtig, wenn Sie etwas aus dem Internet herunterladen, insbesondere wenn es sich dabei um Programme handelt. Meiden Sie Quellen, bei denen Sie Zweifel an der Seriosität haben. Vergewissern Sie sich vor dem Download von Programmen, ob die Quelle vertrauenswürdig ist. Nutzen Sie dafür Suchmaschinen, um gegebenenfalls mehr Informationen über den Hersteller zu erhalten oder Erfahrungsberichte von anderen Benutzerinnen oder Benutzern einzuholen.

Nutzen Sie nach Möglichkeit die Webseite des jeweiligen Herstellers zum Download und verschlüsselte Seiten, die Sie an der Abkürzung „https“ in der Adresszeile Ihres Browsers erkennen.

8

# Seien Sie zurückhaltend mit der Weitergabe persönlicher Daten

Kriminelle im Internet 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. Überlegen Sie, welchen Onlinediensten Sie Ihre persönlichen Daten anvertrauen möchten.

Auch die ungeschützte Weitergabe persönlicher Daten in offenen ungesicherten Netzen sollte vermieden werden.

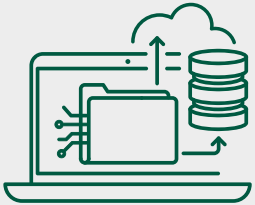
9

# Schützen Sie Ihre Daten durch Verschlüsselung

Besuchen Sie und geben Sie Ihre persönlichen Daten ausschließlich auf Internetseiten ein, die eine verschlüsselte Verbindung anbieten. Nutzt die Seite das sichere Kommunikationsprotokoll https, erkennen Sie dies an der aufgerufenen Internetadresse. Sie beginnt dann stets mit https und in der Adresszeile Ihres Webbrowsers findet sich meist ein kleines geschlossenes Schlosssymbol oder eine ähnliche Kennzeichnung. Vertrauliche E-Mails lassen sich auch verschlüsseln. Prüfen Sie dafür die Möglichkeiten Ihres E-Mail-Anbieters.

Wenn Sie die Übertragungstechnologie Wireless LAN (WLAN) zum Surfen im Internet 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. Zugriff auf den Router erhalten Sie über eine festgelegte Internetadresse, die im Handbuch Ihres Routers vermerkt ist.

10



# Fertigen Sie regelmäßig Sicherheitskopien an

Kommt es trotz aller Schutzmaßnahmen zu einer Infektion eines Ihrer Geräte, können wichtige Daten verloren gehen. Dies gilt ebenso bei dem Verlust eines Geräts oder einem anderweitigen Defekt. Um den Schaden möglichst gering zu halten, ist es wichtig, regelmäßig Sicherungskopien, sogenannte Backups, Ihrer Dateien auf externen Festplatten oder USB-Sticks zu erstellen. Diese Datenträger sollten nur bei Bedarf mit dem PC verbunden sein. Cloud-Dienste können für Sicherungskopien von verschlüsselten Daten herangezogen werden.
Stellen Sie aus der Sicherungskopie nur Ihre Daten wieder her. Bei einem Neuaufsetzen des Geräts sollten keine Programme aus einer Sicherungskopie genommen werden, da diese bereits infiziert sein könnten.

# Weiterführende Informationen

- Auch mit dem Smartphone oder Tablet surfen wir oft im Internet. Sorgen Sie auch bei diesen Geräten für einen guten Basisschutz.
  bsi.bund.de/smartphone-sicherheit
- Wenn Sie die Möglichkeit haben, sich über ein Virtuelles Privates Netzwerk (VPN) mit Ihrem Heimnetz bzw. dessen Router zu verbinden, können Sie auch in öffentlichen WLAN-Hotspots genauso sicher unterwegs sein, wie Sie es von zu Hause gewohnt sind. Ein VPN ist eine besonders gesicherte Verbindung zwischen zwei Punkten. Dabei wird ein Tunnel aufgebaut, z. B. von einem Smartphone durch das öffentliche Internet zu Ihrem Heimnetz, von wo aus Sie dann Ihren eigenen Internetzugang nutzen können. Moderne Router bieten oft die Möglichkeit, ein VPN einzurichten.
  bsi.bund.de/vpn

# 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. Als unabhängige und neutrale Anlaufstelle bietet es Ihnen für einen sicheren digitalen Alltag umfangreiche Informationen.

# IMPRESSUM

**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: service-center@bsi.bund.de
Internet: www.bsi.bund.de
www.facebook.com/bsi.fuer.buerger
Service-Center: +49 (0) 800 274 1000

**Stand:** März 2021
**Bilder:** © GettyImages
**Layout und Gestaltung:** Faktor 3 AG

**Artikelnummer:** BSI-IFB 21/250