

## Online-Sicherheit

Die Nutzung des Internet ist für die meisten von uns heute selbstverständlich. Leider fehlt es vielen Nutzerinnen und Nutzern allerdings noch an dem erforderlichen Bewusstsein um ihre eigene Sicherheit.

Wem ist schon bewusst, dass Computer, sobald sie ans Internet angeschlossen sind, systematisch nach Schwachstellen abgesucht werden? – Der erste Angriff erfolgt meist bereits nach wenigen Sekunden, die der Rechner online ist.

**Ob ein solcher Angriff erfolgreich ist, hat jeder Internet-Nutzer zum großen Teil selbst in der Hand! Hier kann man schon mit geringem Aufwand viel für die eigene Sicherheit tun!**

Mit dem **1x1 DER ONLINE-SICHERHEIT** haben wir für Sie 10 grundlegende Tipps zusammengestellt. Sollte Ihnen beim ein oder anderen Tipp das genaue Vorgehen unklar sein, schauen Sie sich auf den Seiten der „Spezialisten“ um. Erste Adressen für Fragen der technischen Sicherung sind:

Ü [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)

Ü [www.sicher-im-netz.de](http://www.sicher-im-netz.de)

Ü [www.verbraucher-sicher-online.de](http://www.verbraucher-sicher-online.de)

**Auf diesen Seiten finden Sie zu den grundlegenden Tipps weitergehende Informationen, detaillierte Anleitungen und hilfreiche Querverweise.**

## DAS 1x1 DER ONLINE-SICHERHEIT

Quelle: BSI / eigene Bearbeitung

1. Nutzen Sie ein **Anti-Viren-** und ein **Anti-Spyware-Programm** und halten Sie diese durch automatische Updates auf dem aktuellen Stand!
2. Setzen Sie eine **Personal Firewall** ein! Sie schützt vor Angriffen aus dem Internet und verhindert zudem bei einer Infektion des PCs, dass ausspionierte Daten an einen Angreifer gesendet werden können.
3. Sofern Sie nicht die automatisierten Update-Funktionen nutzen, **aktualisieren** Sie Ihr Betriebssystem, Ihren Browser und andere verwendete Software regelmäßig!
4. Gehen Sie nie mit Administrator-Rechten (Windows-Standard) online, denn so können Schadprogramme auf alle Daten und Rechnerfunktionen zugreifen! Richten Sie für alle Nutzer **Benutzerkonten mit eingeschränkten Rechten** ein. So werden auch private Daten vor unbefugtem Zugriff geschützt.
5. Gehen Sie sorgfältig mit Ihren **Zugangsdaten** um! Halten Sie Benutzernamen und Kennwörter für E-Mail-, Shopping-, Banking- oder Bezahlendienste unter Verschluss! Wählen Sie **sichere Passwörter** und wechseln Sie diese in regelmäßigen Abständen!
6. Seien Sie vorsichtig beim Öffnen von **E-Mail-Anhängen** – diese können Schadprogramme enthalten. Im Zweifel fragen Sie beim Absender nach, ob der Anhang tatsächlich von ihm stammt.
7. Seien Sie vorsichtig bei **Downloads** von Webseiten! Vergewissern Sie sich vor dem Download von Programmen aus dem Internet, ob die Quelle vertrauenswürdig ist.
8. Seien Sie zurückhaltend mit der Veröffentlichung bzw. Weitergabe von **persönlichen Informationen!** Online-Betrüger nutzen zuvor ausspionierte Daten, wie etwa Surfgewohnheiten oder Namen aus dem persönlichen Umfeld, um Vertrauen zu erwecken.
9. Achten Sie bei Übertragungstechnologien wie Voice over IP (VoIP) oder Wireless LAN (WLAN) vor allem auf eine **Verschlüsselung** Ihrer Kommunikation, damit Ihre Daten nicht von Dritten mitgelesen bzw. abgehört werden können.
10. Kommt es trotz aller Schutzmaßnahmen zu einer Infektion des PCs mit einem Schädling, können wichtige Daten verloren gehen. Um den Schaden möglichst gering zu halten, sollten Sie regelmäßig **Sicherungskopien** Ihrer Daten auf externen Datenträgern (CD/DVD, USB-Stick, externe Festplatte) erstellen.

## Was tun, wenn...

Befürchten Sie, dass Ihr Rechner trotz aller Vorsichtsmaßnahmen mit einem Schadprogramm infiziert, dass Ihre Daten ausgespäht oder Ihre Zugangsdaten missbraucht wurden, sollten Sie zügig reagieren.

- Beim Verdacht einer **Infektion mit Schadsoftware** finden Sie hilfreiche Tipps zum Beispiel auf der Internet-Seite des BSI ([www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)) unter dem Stichwort „Infektionsbeseitigung“.
- Beim Verdacht eines **Missbrauchs von Zugangsdaten** sollten Sie diese umgehend ändern und sich an den Betreiber des jeweiligen Internet-Portals wenden. Große Anbieter haben für solche Fälle spezielle Konflikt-Management-Dialoge. Im Falle eines strafrechtlich relevanten Missbrauchs (Daten wurden ausgespäht, ein Benutzerkonto missbraucht etc.) sollten Sie außerdem eine **Strafanzeige** bei Ihrer Polizei erstatten – dies ist in Hamburg unter [www.polizei.hamburg.de](http://www.polizei.hamburg.de) auch online möglich.

Sollten Ihnen darüber hinaus im Internet Seiten mit **jugendgefährdenden oder rechtswidrigen Inhalten** auffallen, nutzen Sie die dafür eingerichteten Meldestellen unter:

Ü [www.internet-beschwerdestelle.de](http://www.internet-beschwerdestelle.de)

Ü [www.jugendschutz.net](http://www.jugendschutz.net)

Bei Hinweisen und Fragen rund um **unseriöse Geschäftspraktiken** (wie z.B. Abo-Fallen oder Gewinn-Benachrichtigungen) wenden Sie sich an Ihre Verbraucherzentrale, in Hamburg unter:

Ü [www.vzhh.de](http://www.vzhh.de)

## Empfehlenswerte Seiten

### Ü [www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)

Aktuelle, verlässliche und unabhängige Informationen zu allen Fragen der sicheren Nutzung von Computer und Internet bietet das Bundesamt für Sicherheit in der Informationstechnik.

### Ü [www.datenschutz.de](http://www.datenschutz.de)

Fragen des Datenschutzes in den Neuen Medien werden auf der Seite des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein beantwortet.

### Ü [www.klicksafe.de](http://www.klicksafe.de)

Die Initiative „klicksafe“ informiert Kinder, Jugendliche, Eltern, Multiplikatoren sowie Internetanbieter über Sicherheitsthemen und Entwicklungen im Internet. Außerdem finden sich nützliche Hinweise auf europäische Projekte und Initiativen, Beratungs- und Beschwerdestellen sowie Broschüren zur Medienkompetenz.

### Ü [www.sicher-im-netz.de](http://www.sicher-im-netz.de)

Der Verein „Deutschland sicher im Netz“ (DsiN) hat das Ziel, bei Verbrauchern und in Unternehmen ein Bewusstsein für einen sicheren Umgang mit Internet und IT zu fördern sowie einen praktischen und messbaren Beitrag für mehr IT-Sicherheit zu leisten. Produktneutral und herstellerübergreifend versteht sich DsiN e.V. als Partner für die Politik, gesellschaftliche Gruppen und die Wissenschaft im Bereich Sicherheit in der Informationstechnik.

### Ü [www.surfer-haben-rechte.de](http://www.surfer-haben-rechte.de)

Das vom Bundesverband der Verbraucherzentralen getragene Portal möchte Verbraucher befähigen, sich sicher im Internet zu bewegen und aktiv zu partizipieren. Hierfür werden eine Aufklärungs- und Informationskampagne sowie die rechtliche Überprüfung von Internetangeboten/-portalen angeboten.

### Ü [www.verbraucher-sicher-online.de](http://www.verbraucher-sicher-online.de)

Die Seite informiert Verbraucherinnen und Verbraucher umfassend, unabhängig und verständlich über die sichere Internetnutzung, den sicheren Umgang mit Computern, Barrierefreiheit sowie den Zugang zu digitalen Inhalten und Informationen.



**POLIZEI** Hamburg  
Sicherheit geht alle an

# Wir informieren:

# Online

# Sicherheit

#### IMPRESSUM

Landeskriminalamt Hamburg  
LKA 12 – Fachkommissariat Prävention und Opferschutz  
Bruno-Georges-Platz 1  
22297 Hamburg

Tel.: 040 42 86 - 7 12 10

Fax: 040 42 86 - 7 12 09

[kriminalpraevention@polizei.hamburg.de](mailto:kriminalpraevention@polizei.hamburg.de)

[www.polizei.hamburg.de](http://www.polizei.hamburg.de)

[www.polizei.hamburg.de](http://www.polizei.hamburg.de)