

INFORMIEREN. AGIEREN. VORBEUGEN.



[Wie Urlauber abgezockt werden >](#)
[< Kaffeefahrten](#)

Zehn Tipps zu Ihrer Sicherheit im Internet

So schützen Sie sich vor Internetbetrügern



Sicherheitsmaßnahmen wie Verschlüsselung sind in der modernen Welt unverzichtbar

© m. schuckart, fololia

Die moderne Kommunikationswelt hat auch ihre dunkle Seite: Internetbetrüger versuchen mit immer neuen Techniken, Computernutzer auszuspionieren und um ihr Geld zu bringen. Wie Sie sich vor diesen und anderen Gefahren schützen können, zeigen wir in unseren zehn Tipps.

Halten Sie Ihre Software immer auf dem aktuellen Stand!

Die Hersteller von Betriebssystemen, Office-Software, Internetbrowsern, aber auch von Sicherheitssoftware oder Media-Playern schließen immer wieder Sicherheitslücken in ihren Produkten. Die aktualisierte Software wird über automatische Update-Services oder über die Webseiten der Hersteller bereitgestellt. Sie sollten diese Updates so rasch wie möglich installieren – Internetbetrüger nutzen diese Lücken gerne für ihre Aktivitäten. Das gilt übrigens auch für Geräte wie Digitalkameras oder iPods, bei deren Anschluss an PCs oder Laptops ebenfalls Computerschädlinge übertragen werden können.

Installieren Sie Sicherheitssoftware und halten Sie die Programme aktuell!

Firewalls und Virenschutzprogramme halten Eindringlinge fern und blockieren verseuchte E-Mails oder andere unerwünschte Nachrichten. Auch hier gilt: Updates möglichst rasch installieren, da die Internetkriminellen ihre Angriffe ständig neu gestalten.

Vorsicht bei Nachrichten und Links aus unsicheren Quellen!

Alle Arten von Nachrichten – ob Text, Videos oder Grafiken – können mit Schadsoftware verseucht sein. Der Rechner kann schon alleine durch das Öffnen der Nachricht selbst infiziert werden, nicht erst durch das Klicken auf Anhänge! Daher gilt: Nachrichten aus nicht vertrauenswürdigen Quellen sollten am besten gleich gelöscht werden. Links sollten nur dann verfolgt werden, wenn die Quelle wirklich sicher ist. Betrüger nutzen zunehmend auch Foren wie [Social Networks](#), um dort Links auf gefälschte Seiten zu platzieren und persönliche Daten auszuspionieren.

Vorsicht beim Herunterladen von Software aus dem Internet!

Es gibt zahlreiche Möglichkeiten, um Videos, Grafiken, Sounds oder Softwareprogramme aus dem World Wide Web herunterzuladen – allerdings können dadurch eine ganze Reihe von Problemen entstehen: So kann etwa schädliche Software wie Spionageprogramme unbemerkt mit auf den Rechner geladen werden. Immer wieder verstecken Abzocker aber auch Abonnement-Bestimmungen im Kleingedruckten, das vor dem Download oft achtlos weggeklickt wird. Der überraschte Nutzer merkt dann zu spät, dass durch das Herunterladen etwa eines Klingeltons gleich ein teures Jahresabo abgeschlossen wurde. Andererseits macht man sich durch das Herunterladen von beispielsweise urheberrechtlich geschützten Videos aus Online-Börsen strafbar. Daher gilt: Vor dem Download besser genauer hinsehen!

Verschlüsseln Sie drahtlose Netzwerke!

Über ungesicherte W-LAN können Eindringlinge auf Ihren Computer eindringen und dort geheime Daten ausspionieren. Sie können aber auch auf Ihre Kosten im [Internet](#) surfen, oder Ihren Rechner für üble Zwecke wie den Versand von [Spam](#)-Nachrichten oder den Download illegaler Inhalte missbrauchen. Es lohnt sich also, die Sicherheitskonfigurationen anzupassen. Die von den Herstellern vorab eingestellten Schutzmaßnahmen können von Angreifern oft mühelos umgangen werden.

Führen Sie unterschiedliche Benutzerkonten!

Viele Computernutzer arbeiten ständig als „Administratoren“ – oft ohne es zu wissen. Wenn Sie über ein solches Benutzerkonto arbeiten, haben Sie uneingeschränkte Rechte, Einstellungen auf Ihrem Rechner zu ändern. Das bedeutet aber auch, dass Eindringlinge auf Ihrem Computer ungleich mehr Schaden anrichten können, als wenn Sie nur mit eingeschränkten Rechten arbeiten. Ein weiterer Grund für die Einrichtung von beschränkten Benutzerkonten: Sie können damit die Rechte von Mitbenutzern limitieren

Wählen Sie sichere Passwörter und gehen Sie sorgfältig damit um!

Ein [Passwort](#) zu knacken ist mit der „richtigen“ Software heutzutage keine schwierige Aufgabe für Kriminelle – machen Sie es Ihnen daher möglichst schwer, indem Sie längere Kombinationen von Ziffern und Buchstaben ohne erkennbaren Zusammenhang wählen. Verzichten Sie auf den Einsatz von elektronischen [Passwort](#)-Speichertools, denn dort suchen Computerspione am ehesten nach den Daten. Bewahren Sie die Zugangsdaten auch nicht im direkten räumlichen Zusammenhang zu Ihrem Rechner auf – das Post-it am Schreibtisch ist zwar bequem, lädt aber geradezu zum Missbrauch ein.

Seien Sie vorsichtig bei der Weitergabe persönlicher Informationen!

Besonders in [Social Networks](#) wie [Facebook](#) oder Studi-VZ, aber auch in Online-Diskussionsforen ist die Verlockung groß, persönliche Daten und Vorlieben preiszugeben. Vor allem Jugendliche platzieren dort gerne Fotos oder Videos aus dem persönlichen Umfeld online, die dann vielleicht auch von möglichen Arbeitgebern gefunden werden können. Machen Sie sich immer bewusst, dass alles, was Sie der elektronischen Welt anvertrauen, von Millionen Menschen mitgelesen werden kann. Das [Internet](#) vergisst nie!

Sichern Sie Daten extern und verschlüsseln Sie mobile Geräte!

So modern Ihr neuer Rechner auch sein mag – irgendwann kann auch er kaputt gehen. Nicht nur der














normale Materialverschleiß kann dazu beitragen, auch Viren und Würmer können Festplatten unlesbar machen. Daher sollten Sie Ihre Daten regelmäßig auf externen Festplatten oder anderen Speichermedien sichern. Das gilt auch für Laptops, bei denen noch ein anderes Risiko dazu kommt: Sie können auf Reisen leicht verloren gehen oder gestohlen werden!

Misstrauen Sie dem „schnellen Geld“ im Internet!

Wie in der „normalen Welt“ gilt auch im **Internet**: Hände weg von dubiosen Jobangeboten, mit denen man etwa als Finanzagent merkwürdig rasch und mühelos reich werden kann, oder verblüffend günstigen Schnäppchen! Damit kann man nicht nur eine Menge Geld verlieren, sondern sich beispielsweise als unfreiwilliger Geldwäscher auch ernste strafrechtliche Probleme einhandeln!

Detaillierte Hinweise dazu finden Sie unter anderem beim [Bundesamt für Sicherheit in der Informationstechnik \(BSI\)](#) und dem [Sicherheitskompass der Polizei-Beratung Online](#)

Folgende Artikel könnten Sie auch interessieren:

-  [Der digitale Nachlass](#)
-  [Sicher zum Gebrauchtwagen](#)
-  [Bankgeschäfte und Einkaufen im Netz](#)
-  [Fakt oder Fake?](#)
-  [Wer will an meine Daten?](#)
-  [Falsche Freunde im Internet](#)
-  [Medikamenten-Festpreise auch fürs Ausland](#)
-  [Abmahnungen gehören nicht in den Müll!](#)
-  [Phishing – so können Sie sich schützen](#)
-  [IT-Profis, keine Mausschubser](#)
-  [Internetkriminalität auf jeden Fall anzeigen!](#)
-  [Malware und Spyware - „Stars“ der Internetkriminalität](#)
-  [Auf Siegel und Impressum achten!](#)

[Alle Artikel dieser Kategorie](#)

Weitere Infos zum Thema Diebstahl / Betrug



Wie man gefälschte Dokumente erkennt und überprüfen kann

Es muss einfach gut aussehen

Auf einem Tisch in der Urkundenprüfstelle bei der [Polizei](#) in...[\[mehr erfahren\]](#)



Abgelenkt und abgezockt

Vorsicht vor Taschendieben!

Taschendiebe nutzen gerne große Menschenmengen und dichtes Gedränge...[\[mehr erfahren\]](#)



Vorsicht vor Betrügern und Dieben

Tipps für einen sicheren Urlaub

Natürlich sollen Sie Ihren Urlaub genießen und keinesfalls hinter...[\[mehr erfahren\]](#)



Die Polizei ruft zu besonderer Wachsamkeit gegenüber Handy-Dieben auf

Smartphones sind Wertsachen

Handys - das waren früher bloße Gebrauchsgegenstände von...[\[mehr erfahren\]](#)



Beim Karneval lauern viele Gefahren

K.O.-Tropfen, Diebstahl, Belästigung

Ob Karneval, Fasching oder Fastnacht: Vor Beginn der Fastenzeit...[\[mehr erfahren\]](#)

Cookie Einstellungen

- Statistiken
- Essentiell

Wir nutzen Cookies auf unserer Website, die in unserer [Datenschutzerklärung](#) beschrieben sind. Wir verwenden anonyme Statistiken, um unsere Website zu verbessern. Bitte unterstützen Sie unsere wichtige Präventionsarbeit und akzeptieren Sie alle Cookies. Vielen Dank!

Nur essentielle Cookies akzeptieren Alle akzeptieren