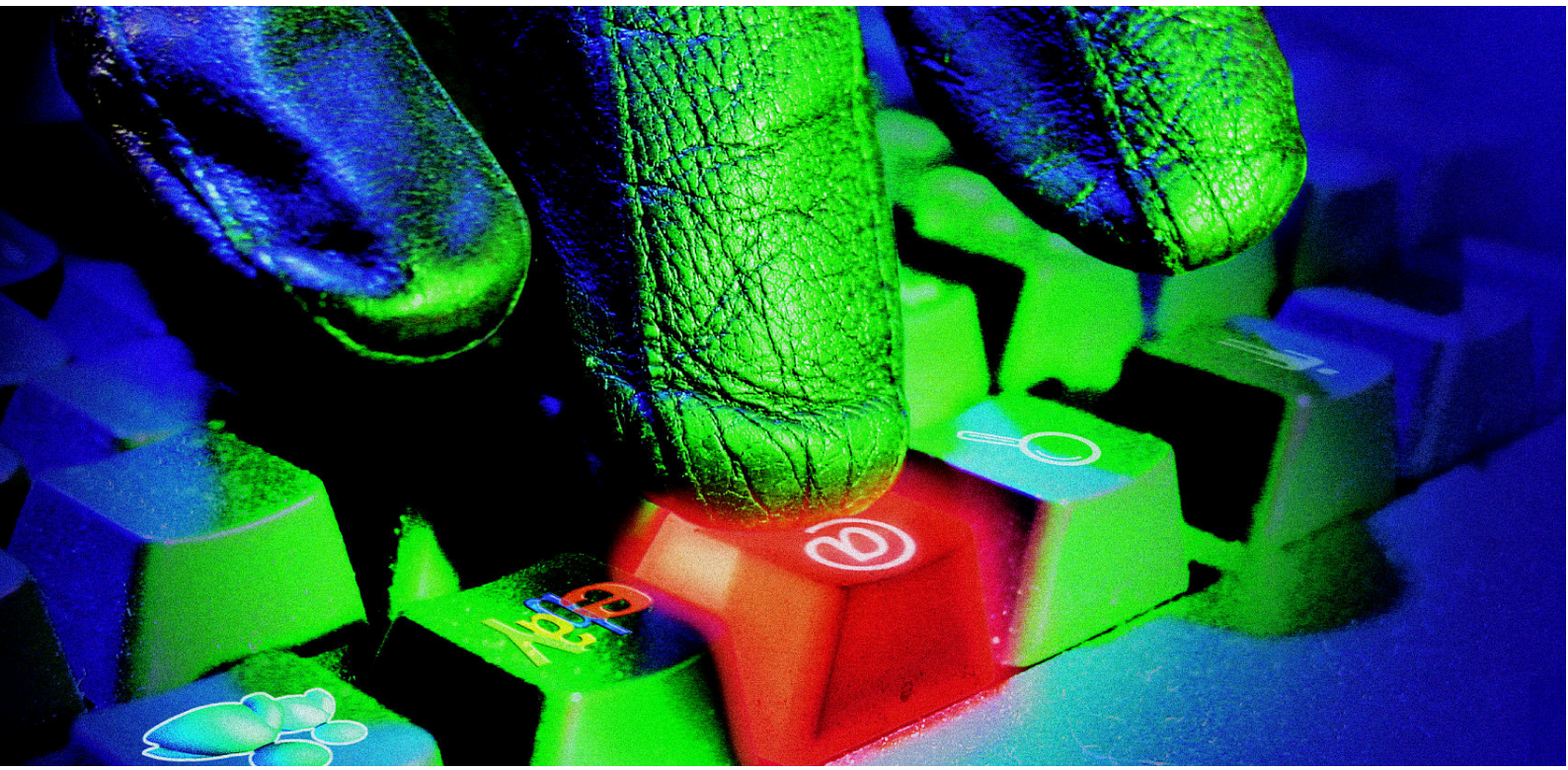


Special: So erkennen Sie betrügerische Angebote

Gemeine Web-Fallen

Ein falscher Klick, und Sie schulden Abzockern 190 Euro. Oder haben einen Zwei-Jahres-Vertrag am Bein. Oder Ihr Rechner ist mit Viren verseucht. Unser Ratgeber-Special erklärt, mit welchen Tricks Online-Betrüger heute arbeiten und wie Sie sich schützen.

Kriminelle im Internet werden immer raffinierter wenn es darum geht, an Ihre Identität und Ihr Geld zu gelangen oder Schädlinge auf Ihren PC zu schleusen. Wir sagen, welche Fallen bei Ebay lauern, wo die Tücken beim Amazon-Marketplace-Shop liegen können und wann Antiviren-Software böse ist. Außerdem erklären wir, welche Tricks einige Anbieter von Internet-Abos anwenden, wie Betrüger versuchen, mit Ihrer Kreditkarte einzukaufen, und wann angeblich billige Software-Downloads für Sie teuer werden.

Viele PC-Anwender fühlen sich auf unsicherem Terrain, wenn sie im Internet unterwegs sind. Doch sich grundlegend zu schützen ist gar nicht so schwierig: Wenn Sie ein paar elementare Regeln beachten, gehen Sie Fallstricken mühelos aus dem Weg. Wir klären über die gefährlichsten Internet-Fallen auf und haben einfache Tipps zusammengestellt, mit denen Sie die häufigsten Gefahren ausschließen.

Die Inhalte im Überblick:

Abzocker im Web

Die 10 fiesesten Web-Fallen

Ein falscher Klick, und Sie schulden den Abzockern 190 Euro! Damit Sie nicht zu den Opfern zählen, klären wir hier über die 10 gefährlichsten Internet-Fallen auf.

Von **Arne Arnold, Daniel Behrens** und **Frank Ziemann**

Abzocker haben neue Tricks entwickelt, um an Ihr Geld und an Ihre Daten zu kommen und Ihren PC zu kontrollieren. So flatterten mehreren Opfern Rechnungen ins Haus, nur weil sie eine Mail geöffnet haben. In anderen Fällen bezahlen die Opfer Waren von Amazon Marketplace und Ebay, erhalten aber nie ein Paket. Wir haben die 10 fiesesten Abzock-Fallen im Internet zusammengetragen.

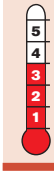
1 Abo-Fallen: Hier müssen Sie für Freeware zahlen

Abzocke: Sie suchen eine bestimmte Freeware, und die Suchmaschine hat Sie auf eine professionell gestaltete Download-Site geschickt, etwa Win-Loads.net. Alles passt – bis auf das Ärgernis, dass Sie sich vor dem Download registrieren müssen. Wer hier seine Daten einträgt, schließt ein Abo von 8 Euro pro Monat ab, mit einer Laufzeit von 2 Jahren – insgesamt sind das 192 Euro für Software, die Sie überall sonst kostenlos bekommen. Über diesen Abovertrag werden Sie nur im Kleingedruckten am Rand der Seite informiert. Mit dieser Methode finden die Abzocker viele Opfer, beispielsweise auch bei Mega-Downloads.net und Opendownload.de.

Betroffene sollten auf keinen Fall voreilig zahlen, sondern sich wehren. Infos gibt's etwa über die Seite *www.abzocknews.de/abgezockt-was-jetzt/*.

HIER LESEN SIE ...

- **welche** Fallen bei Ebay lauern
- **wo** die Tücken beim Amazon-Marketplace-Shop liegen können
- **wann** Antiviren-Software böse ist
- **welche** Tools Gefahren abwehren



Unsere Gefahrenskala:
Zu jeder Falle zeigen wir mit einem Thermometer, wie groß die Gefahr ist. 1 bedeutet „gering", 5 „sehr groß".

Abwehr: Geben Sie Ihre persönlichen Daten grundsätzlich nur auf seriösen Web-Seiten ein.

2 Schadcode sperrt Sie aus Windows aus und will Lösegeld

Abzocke: Ein neuer Schädling hat es auf Windows XP abgesehen. Er ändert das Kennwort für die Windows-Anmeldung. Beim nächsten Neustart können Sie sich also nicht mehr anmelden. Sie erhalten statt dessen einen Hinweis auf eine gebührenpflichtige Telefonnummer, unter der man das neue Passwort angesagt bekommt. Das Ganze ist als Service von Microsoft zur verbesserten Sicherheit des Systems getarnt.

Abwehr: Bislang ist dieser Virus nur in Russland aufgetaucht. Schützen können Sie sich gegen solche Schädlinge generell so, dass Sie nur mit Benutzerrechten in Windows angemeldet sind. Dann kann die Malware nicht aktiv werden (Infos auf Seite 64).

3 Das Öffnen einer Werbemail führt zu einem teuren Abo

Abzocke: Wer sich auf der Website Gewinnstar.com anmeldet, wird von den Betreibern für einige Gewinnspiele eingetragen. Eine Abzocke ist das juristisch nicht, da die Site auf die Leistung und die Kosten hinweist. Beim Verbraucherschutz melden sich aber mehr und mehr Opfer, die niemals auf der Site des Gewinnspiel-Eintragservices gewesen sind und dennoch eine Rechnung über 90 bis 200 Euro bekommen haben.

Ein Betroffener, der die Abzocker kontaktiert hat, erhielt folgende Antwort: Man habe eine Mail von einem Partner von Gewinnstar.com gelesen und bestätigt. Damit sei der Vertrag zustandegekommen. Beweisen will die Firma das mit den Log-Dateien eines Internet-Servers, in denen sich die IP-Adresse des Opfers befindet.

So gehen die Betrüger vor: Sie kaufen Adressen inklusive Mail- und Postanschrift. An die Mailadresse senden sie so lange Werbung für Gewinnstar.com oder gar mit Mitteilungen zu angeblichen Gewinnen, bis das Opfer eine der Mails öffnet. Ein unsichtbares Pixel in der Mail verweist auf einen Server der Kriminellen. Diese wissen dadurch, dass die Mail geöffnet wurde. Anschließend verschicken sie eine Rechnung an die Postanschrift.

Abwehr: Lassen Sie stets den Spamfilter Ihres Mailprogramms aktiviert. Für Opfer: Informationen, wie Sie sich helfen lassen können, gibt's über *www.abzocknews.de* und *www.verbraucherschutz.de*.

4 Käufer behaupten, die Lieferung wäre nicht angekommen

Abzocke: Online-Händler und auch private Gelegenheitsverkäufer werden immer wieder von kriminellen Banden übers Ohr gehauen. Diese suchen sich gezielt Angebote aus, bei denen der Versand ohne nachverfolgbare Sendungsnummer erfolgt, zum Beispiel als Päckchen oder als Warensendung. Einige Tage, nachdem sie die Artikel erhalten haben, behaupten sie, diese seien nicht angekommen. Zuerst versuchen sie, den Händler unter Druck zu setzen, und fordern das Geld zurück.

Bei Ebay-Auktionen können die Betrüger noch einen Schritt weiter gehen. Wenn der Artikel über Paypal bezahlt wurde, beantragen sie den Paypal-Käuferschutz. Der Verkäufer muss dann einen Versandbeleg vorlegen. Wenn er keinen vorweisen kann, zieht Paypal das Geld von ihm ein und überweist es dem Käufer zurück. So haben die Betrüger Ware und Geld.

Abwehr: Wertvolle Produkte sollte man unbedingt als versichertes Paket versenden. Auch schadet es nichts, die Sendung vor dem Versand zu fotografieren – obwohl das allein kein stichhaltiger Beweis dafür ist, dass sie auch wirklich abgeschickt wurde.

Paypal-Käuferschutz wird missbraucht: Betrüger nutzen ihn aus, indem sie behaupten, die bestellte und über Paypal bezahlte Ware sei nie angekommen. Den Schaden hat der Verkäufer (Abzocke 4)

5 Vorsicht vor gefälschten Amazon-Kaufbestätigungen

Abzocke: Über Amazon Marketplace (*www.amazon.de/marketplace*) kann jedermann neue oder gebrauchte Artikel zum Verkauf anbieten. Wenn eine Bestellung eingegangen ist, schickt Amazon eine Mail an den Verkäufer. Kriminelle sind auf die Idee gekommen, diese Kaufbestätigung zu fälschen. Sie verwenden dazu den Originaltext und tauschen nur Produktnummer und -bezeichnung sowie die Empfängeradresse aus. In den bisher bekannt gewordenen Fällen sind in den Mails Lieferadressen in Nigeria angegeben. Ohne einen echten Kauf über Amazon Marketplace vorzunehmen, schicken sie diese Mail an den Verkäufer. Dessen Mailadresse ist häufig offen in seinem Profil hinterlegt, damit Interessenten vor einem Kauf Fragen stellen können.

Zusätzlich zur Kaufbestätigung erhalten die Verkäufer meist eine selbstgetextete Mail in sehr gebrochenem Deutsch. Die Betrüger versuchen darin Druck aufzubauen, indem sie angeben, das Produkt werde kurzfristig als Geburtstagsgeschenk benötigt. Oder sie behaupten, der Verkäufer werde von Amazon Marketplace ausgeschlossen, wenn er den Artikel nicht sofort versende.

Abwehr: Egal ob Amazon, Ebay oder eine andere Verkaufsplattform – schauen Sie immer in Ihrem Kundenkonto nach, ob tatsächlich ein Verkauf stattgefunden hat. Verlassen Sie sich also nicht allein auf die Informationen in einer Mail. ›

KOSTENLOSE TOOLS Schutz vor Abzockern und Viren

Programm	Beschreibung	Internet	Preis	Seite
Antivir Personal Free 9.0	Antiviren-Tool	*www.free-av.de*	privat: gratis	64
AVG Link-Scanner 8.5	Warnt vor gefährlichen Websites	*www.linkscanner.de*	privat: gratis	64
Sandboxie 3.38	Schutzzone für Webbrowser	*www.sandboxie.com*	privat: gratis	65
Mokafive Player 2.1 1)	Virtueller PC	*www.mokafive.com/trial/player.php*	gratis	65
Zone Alarm 7.0/7.1	Desktop-Firewall	*www.zonealarm.com*	privat: gratis	64

Alle Tools laufen unter Windows XP und Vista. 1) englischsprachig

Bei Ebay gekauft: Auf den ersten Blick erkennt man, dass die Musik-CD gefälscht ist, bei der Film-DVD muss man genauer hinschauen (Abzocke 6)

6 Verkäufer liefern mehr oder weniger gute Fälschungen

Abzocke: Millionenumsätze werden mit gefälschten Produkten gemacht – nicht nur auf Flohmärkten, sondern auch im Web. Es gibt dubiose Angebote auf Ebay, Amazon, Booklooker/Disklooker und bei vielen weiteren Online-Shops. Wir haben die Probe aufs Exempel gemacht und eine umfangreiche internationale Alfred-Hitchcock-Kollektion zu einem Preis gekauft, den wir für die gleiche Zahl an DVD-Rohlingen hätten zahlen müssen.

Die Kollektion stellte sich als professionell hergestellte Pressung aus Fernost heraus, die in allen Sprachen problemlos läuft. Es ist sehr fraglich, ob die Urheberrechts-Inhaber je einen Cent gesehen haben.

Gleiches passiert vielen Käufern nicht nur bei Film-DVDs, sondern auch bei Audio-CDs, Markenkleidung und PC-Hardware. So sind nach wie vor fast alle auf Ebay angebotenen USB-Sticks mit 128 GB Fälschungen, die in Wirklichkeit eine geringere Kapazität bieten (siehe PC-WELT 8/09, Seite 7).

Abwehr: Wenn Ihnen Gefälschtes als echt verkauft wurde, hat man Sie betrogen. Wenn jedoch Angebote schon verdächtig günstig sind, sollten Sie das Geschäft nur mit Bedacht tätigen. Man kann Sie in diesem Fall kaum als hereingelegtes Opfer ansehen.

7 Trickbetrüger zocken Ebay-Verkäufer ab

Abzocke: Mit einem besonders fiesen Trick schafft es ein Krimineller, gleich zwei Leute auf Ebay auszunutzen. Wir erklären den Trick anhand eines Diebes, der an ein iPhone kommen will: Dafür verkauft er selbst ein iPhone auf Ebay – natürlich nur zum Schein, denn er besitzt keins. Gleichzeitig kauft er ein iPhone bei einem richtigen Ebay-Verkäufer. So kommt der Dieb zu einem ahnungslosen Käufer, der als Erstes sein künftiges iPhone bezahlen will. Gleichzeitig hat er einen Verkäufer, der als Erstes sein Geld haben will. Er lässt sich also vom richtigen Verkäufer die Bankverbindung nennen.

Die Daten gibt er seinem ahnungslosen Käufer. Die Folge: Der Käufer überweist das Geld an den echten Verkäufer. Der ist erst mal zufrieden und verschickt sein iPhone – an die Adresse des Diebes. Der echte Käufer ist also sein Geld los, bekommt dafür aber keine Ware. Früher oder später wird sich die Polizei beim Verkäufer melden. Der Käufer musste sie einschalten, da er vergeblich auf sein iPhone gewartet hat. An den Kriminellen kommt keiner ran: Das genutzte Ebay-Konto hatte er sich per Phishing zuvor von jemanden geklaut, und die Lieferadresse liegt im Ausland.

Abwehr: Wenn Sie Ware auf Ebay verkaufen, dann fordern Sie vom Käufer im Überweisungstext die Ebay-Auktionsnummer. Das nützt auch dem Käufer, da beide Parteien Abweichungen schnell entdecken können.

SCHUTZPAKET Diese Tools und Tipps wehren alle Gefahren ab

Schritt 1: Arbeiten Sie nur mit eingeschränkten Benutzerrechten

Arbeiten Sie nicht in einem Windows-Konto mit Administratorrechten. Das allein ist ein extrem wirksamer Schutz, denn die meisten Schädlinge können sich nur dann ins System einklinken, wenn das Konto Admin-Rechte bietet. Die Rechte eines Windows-Benutzerkontos bestimmen Sie über „Systemsteuerung, Benutzerkonten“.

Schritt 2: Nutzen Sie ein aktuelles Antivirenprogramm

Gegen Viren und anderen schädlichen Code schützt Sie ein gutes Antivirenprogramm. Empfehlenswert ist etwa **Antivir Personal Free** (auf DVD, privat: gratis).

Schritt 3: Verwenden Sie eine leistungsfähige Firewall

Eine Firewall meldet Programme, die Daten ins Internet senden. **Zone Alarm Free**

hat sich mit Recht den Status eines Klassikers erobert. Der einzige Haken an solchen kostenlosen Desktop-Firewalls: Sie selbst müssen entscheiden, ob das gemeldete Programm online gehen darf oder nicht. Für fortgeschrittene Anwender kein großes Problem, für Einsteiger aber recht schwierig.

Schritt 4: Setzen Sie auf einen informativen Link-Scanner

Kriminelle hacken populäre Websites – oder erstellen eigene – und verbreiten darüber Malware. Damit Sie erst gar nicht auf solche Sites gelangen, installieren Sie den **AVG Link-Scanner** (privat: gratis). Er fügt in den Google- und Yahoo-Suchergebnislisten hinter jedem Treffer ein Symbol an. „Grün“ bedeutet, die Seite ist ungefährlich, „Rot“ heißt, dass sie Schädlinge verbreitet. Bei „Gelb“ ist zwar keine direkte Gefahr einer Infektion gegeben, aber erhöhte Vorsicht geboten, zum Beispiel wenn Sie persönliche Daten eingeben. Ein oranger Button gibt an, dass die Seite zwar selbst harmlos ist, aber Links zu schädlichen Seiten enthält. Das graue Icon mit Fragezeichen weist darauf hin, dass die Adresse bisher nicht überprüft worden ist.

8 Ebay & Co: Schecks platzen mit 4 Wochen Verzögerung

Abzocke: Betrüger schicken Mails an die Verkäufer von wertvollen Waren und bieten an, für einen sehr guten Preis sofort zu kaufen. Sie geben an, im Ausland zu sitzen und deshalb per Scheck bezahlen zu wollen. Die Kriminellen weisen zur Beruhigung darauf hin, dass Sie die Ware erst versenden müssen, wenn das Geld Ihrem Konto gutgeschrieben ist.

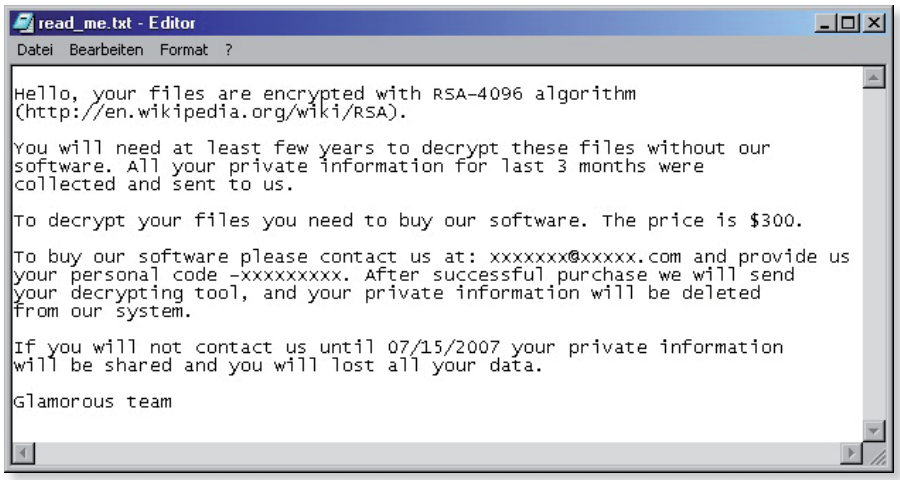
Der Clou der Betrüger: Schecks ausländischer Banken schreibt Ihnen Ihre Bank in der Regel nach wenigen Tagen gut, ohne den Betrag von der anderen Bank erhalten zu haben. Wenn das andere Geldinstitut nach ein paar Wochen meldet, dass der Scheck nicht gedeckt ist, bucht Ihre Bank das Geld von Ihrem Konto wieder zurück. Das ist so üblich und steht auch in den AGB der Institute.

Abwehr: Vermeiden Sie ausländische Schecks zur Bezahlung von Auktionsware. Wenn das nicht möglich oder erwünscht ist, dann lassen Sie sich von Ihrer Bank den Zeitpunkt nennen, an dem das Geld garantiert sicher ist.

9 Angebliche Antiviren-Software erpresst zum Kauf

Abzocke: Gauner bieten im Internet angebliche Sicherheits-Software an, etwa Antiviren-Programme. Diese gibt's erst mal kostenlos zum Download. Wer aber nach der Installation einen Scan mit dem Tool startet, bekommt als Ergebnis auf jeden Fall die Meldung, dass der PC mit Viren verseucht ist. Die meisten der Abzocker-Tools melden Viren, obwohl keine vorhanden sind, einige bringen den Schädling gar selbst mit. Um diese zu entfernen, fordert das Tool den Anwender auf, die Vollversion zu kaufen. Mit drastisch klingenden Warnungen vor Schäden am PC durch die Viren wird der Nutzer regelrecht zum Kauf erpresst.

Abwehr: Sicherheits-Tools sollten Sie nur installieren, wenn diese von einem vertrauenswürdigen Anbieter stammen. Das Sicherheitslabor AV-Test (*www.av-test.org*) bietet Links zu fast allen seriösen Antiviren-Herstellern der Welt. Welche Programme sich bewährt haben, lesen Sie in unserem Artikel „Tipps und Tests: Sicherheits-Suiten".



Erpressung: Der Virus verschlüsselt alle Anwenderdateien auf dem PC und fordert dann in dieser Textdatei ein Lösegeld für das Passwort zum Entschlüsseln (Abzocke 9)

10 Malware manipuliert Google-Ergebnisseiten

Abzocke: Online-Betrüger verbreiten Malware, die Google-Ergebnislisten im Browser manipuliert: Wenn in den Trefferlisten Adressen von Online-Shops enthalten sind, bei denen die Online-Betrüger Mitglied im Partnerprogramm sind, werden diese Links von der Malware geändert. Sie führen zwar trotzdem noch zum richtigen Ziel, senden aber unbemerkt die Partnernummer der Betrüger mit. Wenn der Surfer dann zum Beispiel bei Amazon etwas bestellt, erhalten die Kriminellen eine Provision vom Shop.

Nicht jeder Schädling, der die Google-Suchergebnisse auf dem PC manipuliert, ist so harmlos für den Anwender. Es gibt auch welche, die in die Suchergebnisse Links zu verseuchten Websites einbauen. Die Schädlinge verbreiten sich weiter, indem sie auf der Festplatte nach Zugangsdaten für FTP-Server forschen. Finden sie welche, suchen sie auf dem FTP-Server nach HTML-Dateien und bauen ihr Weiterverbreitungs-Script ein. Wenn die HTML-Seiten zu einer Website gehören, werden deren Besucher infiziert. Vorausgesetzt, sie surfen mit einem Browser, der Sicherheitslücken enthält.

Abwehr: Benutzen Sie eine aktuelle Antiviren-Software (siehe Kasten auf Seite 64), und installieren Sie jedes Browser-Update sofort nach Erscheinen.

SICHER SURFEN Schutz durch Virtualisierung

Stecken Sie Ihren Browser in einen Sandkasten

Wenn Sie Ihren Browser in einer Sandbox („Sandkasten") laufen lassen, ist Ihr System ziemlich gut vor Viren, Würmern und Trojanern geschützt, die sich beim Surfen einnisten. Dazu nutzen Sie **Sandboxie**. Das Tool legt auf dem Desktop ein Icon mit dem Namen „Sandboxed Web Browser" an. Wenn Sie darauf klicken, startet der unter Windows als Standard festgelegte Browser innerhalb einer Sandbox – zu erkennen an den Zeichen [#] am Anfang und am Ende des Fenstertitels. Downloads, bei denen Sie sicher sind, dass sie ungefährlich sind, können Sie aus der Sandbox herauskopieren. Den restlichen Inhalt der Sandbox sollten Sie spätestens dann löschen, wenn Sie eine Infektion feststellen.

Setzen Sie auf eine komplette Virtualisierung

Noch sicherer als der Browser-Sandkasten ist es, mit einem virtuellen PC zu arbeiten. Diesen erhalten Sie zum Beispiel mit dem kostenlosen **Mokafive Player**. Zusätzlich müssen Sie sich noch ein virtuelles Betriebssystem herunterladen. Am einfachsten nutzen Sie „Fearless Browser" – ein Eintrag dafür ist in Mokafive Player schon vorgesehen. Sie klicken auf den Play-Button (Pfeilchen), schon startet der System-Download, und der virtuelle PC beginnt bereits währenddessen zu booten. Sie landen in einem einfach zu bedienenden Linux-System mit vorinstalliertem Firefox-Browser. Damit können Sie nach Herzenslust im Web surfen – Viren und Würmer können dem Hauptsystem nichts anhaben.

Wehren Sie alle Schädlinge ab

Die 10 schlimmsten Viren-Fallen

Ein falscher Klick, und Ihr Rechner ist mit Viren verseucht. Die Kriminellen im Internet werden immer raffinierter, wenn es darum geht, Schädlinge auf Ihren PC zu schleusen. Wir verraten die gefährlichsten Tricks – und wie Sie sich schützen.

Von **Arne Arnold, Daniel Behrens** und **Frank Ziemann**

Virenprogrammierer sind ganz versessen auf Ihren Rechner, denn jeder neue verseuchte PC bringt den Programmierern und Kriminellen mehr Geld.

Haben Hacker etwa ein paar hundert PCs mit einem Bot infiziert, dann vermieten sie diese Computer an Spammer, die darüber millionenfach ihre Werbemails aussenden. Auf der anderen Seite gibt es immer mehr Schädlinge, die es auf Ihre Daten, Log-ins, Online-Banking-Infos und Kreditkartennummern abgesehen haben.

Wir klären über die 10 fiesesten Viren-Fallen im Internet auf und sagen, wie Sie Ihren Rechner schützen.

1 Populäre Software mit Malware verseucht

Gefahr: Verbreiter von Malware nutzen den Hype um neue Software, um ihre Schädlinge unters Volk zu bringen. Beispiel Windows 7: Schon mehrere Tage, bevor Microsoft die Vorabversion (Release Candidate) zum Download bereitgestellt hat, zirkulierte in Tauschbörsen ein Download mit diesem Namen. Viele Anwender, die es nicht abwarten konnten, sind darauf hereingefallen. Statt des Betriebssystems erhielten sie eine Scareware, also ein betrügerisches, vorgebliches Antivirusprogramm (Seite xx). Bereits im Januar haben Online-Kriminelle auf die gleiche Weise das Interesse an Apples neuer Software iWork '09 ausgenutzt, um einen Bot zu verbreiten. Sie haben damit ein Botnet aus gekaperten Macs aufgebaut.

Abwehr: Nicht jede Antiviren-Software erkennt Scareware und blockt sie ab, wenn sie gerade frisch in Umlauf gebracht wurde. Daher lautet die Abwehrstrategie, Software aus fraglichen Quellen entweder gar nicht herunterzuladen oder aber erst in einer virtuellen Maschine (Informationen siehe Kasten auf Seite 72) zu testen.

HIER LESEN SIE ...

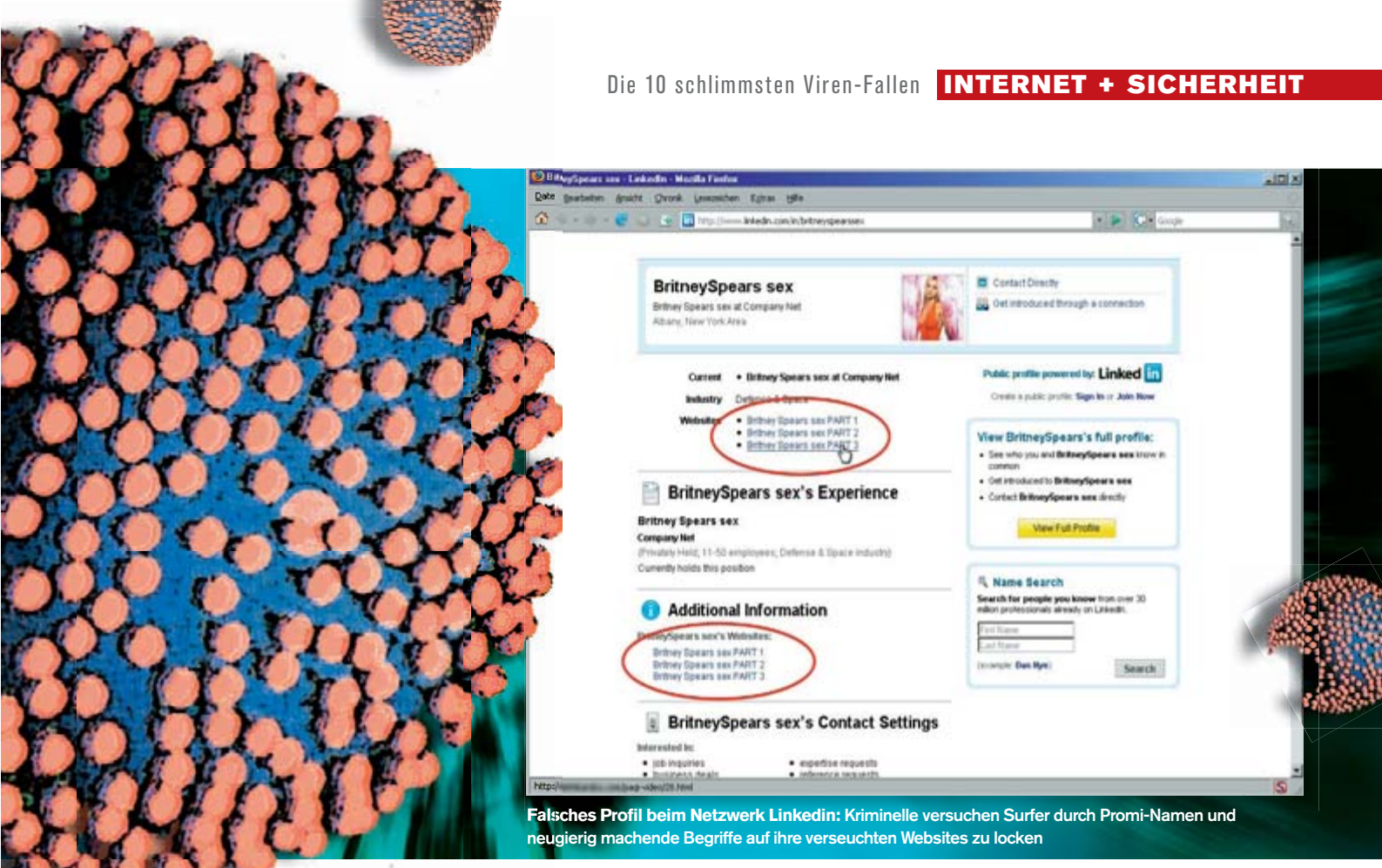
- **welche** beliebten Programme in Wirklichkeit Viren enthalten
- **wie** Sie nicht auf Trojaner hereinfallen
- **warum** ein eingeschränktes Benutzerkonto Ihr System schützt
- **mit welchen** Tools Sie gefahrlos surfen

Unsere Gefahrenskala:
Zu jeder Viren-Falle zeigen wir mit einem Thermometer, wie groß die Gefahr ist. 1 bedeutet „gering", 5 „sehr groß".

2 Viren-Attacke auf Outlook-Anwender

Gefahr: Phishing bezeichnet eine Methode, bei der eine Mail mit gefälschtem Absender den Nutzer auf eine gefälschte Website lockt. Dort soll das Opfer seine persönlichen Daten und Log-ins verraten. Ist die Seite gut gemacht, also etwa eine perfekte Nachbildung der Website einer Bank, dann stolpern tatsächlich etliche Anwender in die Falle. Trickreich gemacht war eine Phishing-Attacke auf Anwender von Microsoft Outlook Anfang Juni 2009. In der Phishing-Mail wurden die Benutzer aufgefordert, ihr E-Mail-Programm über ein Online-Verfahren neu zu konfigurieren. Der beigefügte Link führte angeblich zu Microsoft, tatsächlich aber auf eine Phishing-Site. Dort sollten die Anwender ihren Benutzernamen und ihr Passwort angeben. Dadurch erlangten die Kriminellen die Kontrolle über das Mailkonto des jeweiligen Benutzers. Andere Mails dieser Art verwiesen auf einen Virus.

Abwehr: Überprüfen Sie vor der Eingabe von Log-in-Daten immer, ob die Adresse oben im Browser die der gewünschten Website ist. Nutzen Sie zudem einen Link-Scanner und ein Antiviren-Programm (Infos siehe Kasten auf Seite 72).



Falsches Profil beim Netzwerk Linkedin: Kriminelle versuchen Surfer durch Promi-Namen und neugierig machende Begriffe auf ihre verseuchten Websites zu locken

3 Falscher Flash-Player installiert Trojaner

Gefahr: Per Mail oder Suchmaschinen-Spam verbreiten Kriminelle Links zu angeblich besonders spannenden oder lustigen Web-Videos. Wer den Link anklickt, landet auf einer Seite, auf der es noch keinen Clip zu sehen gibt. Es wird nur ein Bild angezeigt, das ein abspielbereites Video vortäuscht. Wer dieses Video per Klick zum Starten bringen will, bekommt eine Aufforderung, die neueste Version von Adobe Flash Player herunterzuladen und zu installieren. In besonders gut gemachten Fällen landet das Opfer auf einer Download-Site, die dem Original von Adobe täuschend ähnlich sieht. Der Server der gefälschten Site steht meist in Ländern mit einem unterentwickelten Internet-Recht. So bleiben diese Sites lange online. Damit aber nicht genug. Lediglich der eigentliche Download-Link und die Web-Adresse, in der jeweils „addobe“ statt „adobe“ steht, weisen bei genauer Betrachtung auf die Täuschung hin. Die zum Download angebotene Datei heißt wie das Original „install_flash_player.exe“ und trägt das gleiche Symbol. Damit enden jedoch die Gemeinsamkeiten. Was unvorsichtige Web-Surfer mit der Datei tatsächlich erhalten, ist Malware: ein Trojanisches Pferd, das Anmeldedaten für das Online-Banking ausspionieren soll.

Abwehr: Das beste Mittel gegen solche Schädlinge ist erhöhte Wachsamkeit, wenn Sie von einer Web-Seite zum Download von Updates aufgefordert werden. Prüfen Sie die Download-Adresse genau, und installieren Sie zusätzlich einen Link-Scanner (siehe Kasten auf Seite 72).

4 Gefälschte Promi-Profile locken mit Sexfotos

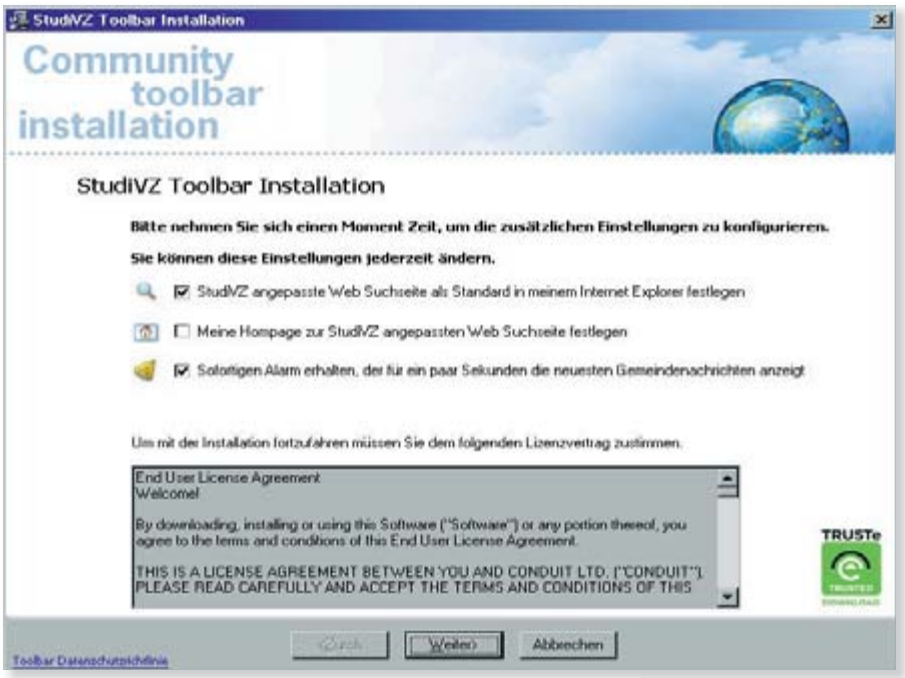
Gefahr: Online-Kriminelle adressieren die Neugier, indem sie mit Nacktbildern von Stars und Sternchen locken. Immer häufiger geschieht dies in sozialen Netzwerken. Bei Linkedin waren zum Beispiel eine Zeitlang gefälschte Profile von Britney Spears, Beyoncé, Shakira, Victoria Beckham und Hulk Hogan online. Darin waren Links zu Websites enthalten, auf denen es angeblich intime Fotos zu sehen geben sollte. Doch statt nackter Tatsachen erhielten arglose Anwender einen Trojaner über einen gefälschten Flash-Player (siehe links) oder per Drive-by-Download (Seite 74).

Abwehr: Unbekannte Websites sollten Sie über einen virtuellen PC oder mit Sandboxie aufrufen (siehe Kasten Seite 72). ›

DIE 5 BESTEN SCHUTZPROGRAMME Kostenlose Tools gegen Viren

Programm	Beschreibung	Internet	Preis	Seite
Antivir Personal Free 9.0	Schützt vor Viren	*www.free-av.de*	privat: gratis	72
AVG Link-Scanner 8.5	Warnt vor gefährlichen Websites	*www.linkscanner.de*	privat: gratis	72
Sandboxie 3.38	Schutzzone für Web-Browser	*www.sandboxie.com*	privat: gratis	72
Mokafive Player 2.1 1)	Virtueller PC	*www.mokafive.com/trial/player.php*	gratis	72
Zone Alarm 7.0/7.1	Firewall für den Desktop-PC	*www.zonealarm.com*	privat: gratis	72

Alle Tools laufen unter Windows XP und Vista. 1) englischsprachig



Setup-Programm für eine inoffizielle StudiVZ-Toolbar: Hierin hatten Kriminelle Malware versteckt und auf diese Weise Anmeldedaten für das soziale Netzwerk ausspioniert

5 Gehackte Promi-Sites verbreiten Schädlinge

Gefahr: Websites von Prominenten sind ein beliebtes Ziel von kriminellen Hackern, die Malware verbreiten wollen. Der hohe Bekanntheitsgrad sichert eine große Zahl von Besuchern und damit potenziellen Opfern.

Im April dieses Jahres hatte es die offizielle Website von Ex-Beatle Paul McCartney erwischt. Nach dem Eindringen in den Webserver haben die Kriminellen etliche Seiten so präpariert, dass sie per Drive-by-Download (Seite 74) automatisch Malware auf die Rechner der Besucher übertragen. Die Surfer hatten nichts auf der Site angeklickt und waren dennoch allein durch den Besuch der Seite infiziert.

Abwehr: Den besten Schutz bietet auch hier das Surfen innerhalb einer virtuellen Maschine oder in Sandboxie (Seite xx). Wenn es Ihnen zu umständlich ist, diese Methoden auch für bekannte und häufig genutzte Seiten zu nutzen, raten wir zumindest zu Antivirenprogramm und Link-Scanner (siehe Kasten unten).

6 Gefälschte Toolbars mit Spionage-Software

Gefahr: Zusätzliche Symbolleisten im Browser sind beliebt – manche Anwender haben bereits so viele installiert, dass kaum noch Platz für die Inhalte der Web-Seiten bleibt. Diese Beliebtheit nutzen Kriminelle aus: Vor kurzem ist zum Beispiel eine manipulierte Internet-Explorer-Symbolleiste für das beliebte soziale Netzwerk StudiVZ aufgetaucht. Sie sieht absolut echt aus, hat aber einen Schädling im Gepäck, der auf mehreren Wegen Daten des befallenen PCs ausspioniert. Die Sicherheitsexperten von McAfee haben ihn als Variante des Trojanischen Pferds Backdoor-CEP klassifiziert.

Der Schädling verhält sich passiv, wenn bestimmte Sicherheitsprogramme laufen oder er in einer virtuellen Maschine ausgeführt wird. Ansonsten injiziert er Schad-Code in laufende Prozesse. Der Schädling ist nur schwer zu entdecken, denn er wird nie als Datei auf die Festplatte geschrieben.

Nach der Toolbar-Installation startet der Internet Explorer und ruft die Website von StudiVZ auf. Wenn sich der Anwender dort einloggt, greift der Schädling die Anmeldedaten ab. Die ausgespähten Daten werden an einen Server in Deutschland übertragen.

Schutz: Laden Sie Software jeglicher Art nur von absolut vertrauenswürdigen Quellen herunter, und prüfen Sie vor dem Download, ob die Web-Adresse im Browser stimmt oder gefälscht ist. Für StudiVZ gibt es übrigens keine offizielle Toolbar.

SO SURFEN SIE SICHER Firewall, Virtualisierung und Benutzerrechte richtig einsetzen

Sperren Sie Schädlinge aus

Antiviren-Programm: Gegen Viren und anderen schädlichen Code schützt Sie ein gutes Antiviren-Programm. Empfehlenswert ist etwa das kostenlose und bewährte **Antivir Personal Free** (*www.free-av.de*).

Firewall: Eine Firewall meldet Programme, die Daten ins Internet senden. Empfehlenswert ist der Klassiker **Zone Alarm Free** (*www.zonealarm.com*). Der einzige Haken an solchen kostenlosen Desktop-Firewalls: Hier müssen Sie selbst entscheiden, ob das gemeldete Programm online gehen darf oder nicht. Für fortgeschrittene Anwender ist das meist kein großes Problem, für Einsteiger aber eventuell sehr schwierig.

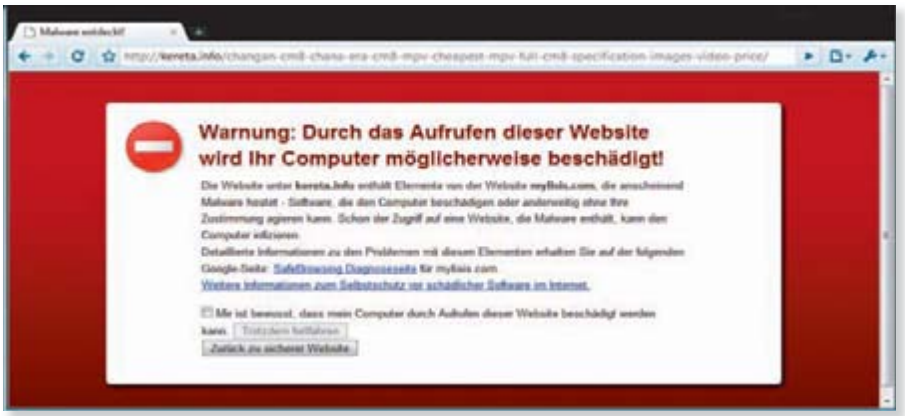
Link-Scanner: Kriminelle hacken populäre Websites und verbreiten darüber Malware. Damit Sie erst gar nicht auf solche Sites gelangen, installieren Sie den **AVG Link-Scanner** (*www.linkscanner.de*). Dieser ergänzt in den Google- und Yahoo-Suchergebnislisten jeweils ein Symbol. „Grün" steht für eine ungefährliche Seite, „rot" warnt vor Schädlingen.

Schützen Sie Ihr System

Browser-Sandbox: Wenn Sie Ihren Browser in einer Sandbox (Sandkasten) laufen lassen, ist Ihr System ziemlich gut vor Schädlingen geschützt, die sich beim Surfen einnisten wollen. Dazu nutzen Sie etwa das Tool **Sandboxie** (*www.sandboxie.com*).

Virtualisierung: Noch sicherer als ein Browser-Sandkasten ist ein virtueller PC. Diesen erhalten Sie etwa mit dem kostenlosen **Mokafive Player** (*www.mokafive.com/trial/player.php*). Zusätzlich müssen Sie ein virtuelles Betriebssystem herunterladen. Am einfachsten nutzen Sie „Fearless Browser" – ein Eintrag dafür ist in Mokafive vorhanden.

Benutzerrechte: Arbeiten Sie nicht in einem Windows-Konto mit Administratorrechten. Das ist ein extrem wirksamer Schutz, denn die meisten Schädlinge können sich nur dann ins System einklinken, wenn das Konto Admin-Rechte bietet. Die Rechte eines Windows-Benutzerkontos steuern Sie über „Systemsteuerung, Benutzerkonten".



Web-Filter: In diesem Fall hat der Browser Google Chrome erfolgreich eine potenziell gefährliche Website geblockt. Doch es gibt Wege, über die Kriminelle solche Filter austricksen können

7 Schädlinge werden beim Surfen eingeschleust

Gefahr: Durch so genannte Drive-by-Downloads („Herunterladen im Vorbeigehen") werden beim Besuch manipulierter Websites heimlich Schädlinge in den Rechner geschleust. Es handelt sich also um einen verdeckten Angriff auf ahnungslose Besucher einer vermeintlich harmlosen Website. Der Browser des Anwenders dient dabei dem Angreifer als Hilfsmittel, um schädlichen Code in dem Rechner unterzubringen.

So funktioniert der Angriff: Zunächst präparieren die Kriminellen eine Website, auf die potenzielle Opfer gelockt werden sollen. Zum Teil hacken sie dazu bereits bestehende Sites. Eine andere Methode ist es, eine eigene Internet-Site zu eröffnen.

Auf einer solchen Web-Seite sind dann Javascripts und/oder unsichtbare Rahmen (Iframes oder Inlineframes genannt) eingebettet, die weiteren Code von einem anderen Server holen. Sie ermitteln den vom Besucher verwendeten Browser und laden passenden Exploit-Code, der eine Sicherheitslücke des Browsers ausnutzt.

Ohne dass der Besucher davon etwas bemerkt, wird so ein Trojanisches Pferd in seinen Rechner geschleust und ausgeführt. Der PC wird damit zum Beispiel Teil eines Botnets. Diese wiederum dienen etwa dazu, Spam zu versenden. Zudem spioniert der Wurm oft persönliche Informationen aus, etwa Passwörter zu Online-Diensten oder die Kreditkartennummer.

Abwehr: Installieren Sie eine Antiviren-Software, und installieren Sie jedes Browser-Update sofort nach Erscheinen. Installieren Sie zusätzlich einen Link-Scanner. Näheres dazu siehe Kasten auf Seite 72.

8 Viren umgehen den Web-Filter im Browser

Gefahr: Virenverbreiter speichern seit Neuestem ihre Malware auch auf One-Click-File-Hostern, etwa Rapidshare. Dort kann jeder Anwender Dateien ablegen und für andere zum Download anbieten. Über solche Hoster umgehen Schädlinge die URL-Filter: Diese blocken im Prinzip recht zuverlässig Websites, auf denen sich Viren tummeln. Google führt eine ausführliche schwarze Liste mit gefährlichen Sites, die von Browsern wie Firefox und Chrome genutzt wird. Die One-Click-File-Hoster stehen aber in der Regel auf einer weißen Liste und werden von URL-Filtern nicht geblockt.

Der Sicherheitsspezialist Ralf Benzmüller von G-Data warnt: „Nicht nur Rapidshare ist betroffen. Auch andere Datei-Hosting-Dienste, etwa Mediafire.com, Uploaded.to und Uploading.com, werden zur Verbreitung von Malware missbraucht. Oft werden die Dateien als neueste Versionen von Software, aktuelle Tools oder gecrackte Software angepriesen."

Abwehr: Setzen Sie immer eine aktuelle Antiviren-Software ein (siehe Kasten auf Seite 72). Laden Sie Software nur von Hersteller-Sites und bekannten Download-Archiven wie *www.pcwelt.de* herunter.

Täuschung: Diese Site sieht der Seite von last.fm sehr ähnlich, ist aber gefälscht, um die Log-ins zu stehlen

9 Erwachsenen-Sites im Web schleusen Viren ein

Gefahr: Über Sicherheitslücken in Browser-Plug-ins – etwa fürs Anzeigen von PDF-Dokumenten – schleusen Kriminelle Viren ins System. Das geschieht ohne Zutun des Anwenders. Man muss nur eine speziell präparierte Web-Seite im Browser aufrufen. Diese enthält einen Inlineframe, der etwa auf ein schädliches PDF-Dokument auf einem chinesischen Server verweist. Über eine Sicherheitslücke in älteren PDF-Plug-in-Versionen landet der Virus im System. Damit ahnungslose Anwender solche Web-Seiten auch aufrufen, haben die Kriminellen seit Anfang Juni 2009 mehrere hundert Domains mit anrüchigen Namen erstellt. So landen dort Internet-Surfer, die nach Erwachseneninhalten im Netz suchen.

Abwehr: Aktualisieren Sie stets alle Programme und Plug-ins, die auf Ihrem PC installiert sind. Setzen Sie zudem eine aktuelle Antiviren-Software ein (Infos siehe Kasten auf Seite 72).

10 Angreifer klauen Log-ins bei Last.fm

Gefahr: Last.fm (*www.lastfm.de*) ist ein Online-Musik-Katalog, über den sich kostenlos Musik hören lässt und der von seinen Anwendern selbst zusammengestellt wird. Wer sich dort anmeldet, gibt dem System allerdings auch persönliche Infos preis. Auf diese haben es Phisher abgesehen, die über das interne Nachrichtensystem Botschaften verschicken.

Die Nachrichten lauten etwa „Hey, schau Dir mal Dein Bild in meinem Blog an." Die dazugehörige Web-Adresse ist durch einen URL-Verkürzer unkenntlich gemacht. Wer darauf klickt, wird auf eine Website gelenkt, die der Log-in-Seite von Last.fm zum Verwechseln ähnlich sieht.

Abwehr: Überprüfen Sie vor der Eingabe von Log-in-Daten immer, ob die im Browser angezeigte Adresse stimmt.

Die 10 größten Gefahren im Internet

Vorsicht beim Surfen

Wer kennt Ihre Passwörter? Hat man Ihre Online-Identität geklaut? Jeder, der mit dem PC ins Web geht, ist dort sofort von den 10 größten Gefahren bedroht. Wir zeigen, vor welchen Angriffen Sie sich schützen müssen – und wie Sie sich wappnen.

Von **Arne Arnold**

Selbst wenn Sie sich nicht in den dunklen Ecken des Internets herumtreiben, sind Sie von vielen Online-Gefahren bedroht. Wir nennen die 10 größten Risiken im Web und zeigen, welche Tools und Kniffe Sie davor schützen.

1. Harmlose Websites schleusen Malware ein

Gefahr: sehr groß
Verbreitung: gering

Darum geht's: Malware-Programmierer haben unvorsichtige Anwender im Visier, die es mit dem Schutz ihres PCs nicht so genau nehmen. Solche Nutzer gibt es vor allem auf eigentlich ganz harmlosen Websites – etwa der Site eines Sportstadions, einer Musikgruppe, eines Nachrichtenmagazins, eines Online-Spiels oder eines Prozessorherstellers. Die Angreifer hacken sich in solche Websites ein und platzieren dort gefährlichen Code. Sobald ein Anwender die Website aufruft, ist sein Rechner schon verseucht. Ein Klick auf die Seite ist meist nicht nötig. Ein paar Beispiele:

Forum: Der erste spektakuläre Fall betraf das Forum des Prozessorherstellers AMD (**www.amd.com**). Ende 2004 konnten sich Viren über eine Lücke in Windows einschleichen, allein durch das Betrachten von JPG-Bildern. Das betraf auch den Internet Explorer. Angreifer hatten ein entsprechend präpariertes Bild ins Forum von AMD geschmuggelt.

Community-Sites: Bei den Angreifern sind heute Community-Sites sehr beliebt, um darüber die PCs von Besuchern zu infizieren. Auf Myspace (**www.myspace.de**) finden die Hacker Seiten von prominenten Leuten, die sich dort präsentieren. Diese Seiten werden von vielen Anwendern aufgerufen – auch Nicht-Mitgliedern von Myspace. Durch Sicherheitslücken in der Community-Site gelingt es den Angreifern, dort Java-Script-Code zu platzieren. Die Folge: Wer sich die Seite ansieht und nicht sämtliche Patches für Windows, den Browser und alle Active-X-Anwendungen installiert hat, infiziert seinen PC mit Schad-Software – so geschehen auf der Myspace-Seite der Sängerin Alicia Keys.

Foto: Photodisc

Immer aktuell: Die Freeware Updatestar kennt die gängigsten Programme und sucht automatisch nach erforderlichen Updates. Herunterladen und installieren muss man die Patches aber noch selbst (Punkt 1)

ÜBERBLICK Internet-Gefahren

Online-Gaming-Sites: Millionen von Anwendern nutzen ihren PC auch zum Spielen. Die Spiele, Patches, Infos und vieles mehr gibt's natürlich auf den gut besuchten Online-Gaming-Sites. Verseucht ist seit Monaten etwa die Site Gameige. Dort laden Iframes Websites von einem weiteren Server, die über mehrere Sicherheitslücken Malware einschleusen können. Vorsicht: Gameige war zu Redaktionsschluss noch immer verseucht. Besuchen Sie diese Website nicht!

Der Sicherheits-Spezialist McAfee berichtet von einem Massen-Hack. Im März 2008 sollen mehrere tausend Webserver für Online-Gaming-Sites manipuliert und mit schädlichem Code versehen worden sein. Der gefährliche Code, der schließlich auf den PCs der Anwender landete, spionierte unter anderem die Log-in-Daten zu Online-Spielen aus. Solche Log-ins bringen auf dem Schwarzmarkt teilweise deutlich mehr Geld als eine Kreditkartennummer.

Werbebanner: Der Schadcode lauert manchmal auch hinter Werbebannern – nämlich etwa auf einer verseuchten Site, auf die ein gehacktes Banner verlinkt. Für eine Infektion muss der Anwender dabei auf die Werbung geklickt haben. Betroffen sind wiederum eigentlich harmlose Sites. Die Nachrichten-Site Usatoday.com hat 3,9 Millionen Besucher jeden Tag – und hatte Anfang April 2008 ein gefährliches Werbebanner. Infos über **www.pcwelt.de/96b**.

Aktuelle Themen: Anfang April manipulierten Hacker eine Website, die für die Befreiung Tibets warb. Dort gab es einen

„Ein gefährlicher Flash-Film im Web schleust beim Ansehen Schadcode ein"

Flash-Film, der gegen die Olympischen Spiele in China protestiert. Beim Betrachten des Films schleust sich ein Trojaner über eine Windows-Sicherheitslücke vom November 2007 ins System und versteckt sich mit Rootkit-Technik. Weitere Infos über **www.pcwelt.de/b5b**.

Gegenmittel

1. Skriptblocker installieren: Setzen Sie einen Skriptblocker ein. Dieser verhindert die Ausführung von Java-Script. Java-Script wird für die meisten Angriffe genutzt. Ein empfehlenswerter Skriptblocker ist das kostenlose Firefox-Plug-in **Noscript**.

2. Antiviren-Software nutzen: Ein solches Sicherheits-Tool ist ein absolutes Muss für jeden PC. Kostenlos und empfehlenswert ist etwa **Antivir Personal**.

3. Software aktualisieren: Windows und alle anderen Programme sollten immer auf dem aktuellen Stand sein. Das Einspielen der Patches für Windows aktivieren Sie über „Systemsteuerung, Automatische Updates" bei XP und „Systemsteuerung, Windows Updates" bei Vista. Aktualisierungen für Anwendungen findet die Freeware **Updatestar**. Herunterladen und installieren müssen Sie die Flicken aber noch von Hand. Vor allem Media-Player sollten Sie immer auf dem neuesten Stand halten, da diese häufig gefährliche Sicherheitslücken haben. ›

GRATIS-PROGRAMME IM ÜBERBLICK Gegenmittel bei Internet-Fallen

Programm	Kurzbeschreibung	Internet	Windows	Sprache	Seite
Antivir Personal 8.0[1]	Antiviren-Programm	www.free-av.de	2000, XP, Vista	deutsch	112
Antivir Rescue System 3.4.4	Sicherheits-Boot-CD	www.pcwelt.de/c4b	–	deutsch	115
Comodo Firewall Pro Free 3.0	Firewall	www.comodo.com	XP, Vista	englisch	112
Hotspot Shield 1.03	VPN-Client	www.anchorfree.com	2000, XP, Vista	englisch	114
McAfee Siteadvisor 2.5	Website-Analyse	www.siteadvisor.com	98/ME, 2000, XP, Vista	deutsch	112
Noscript 1.3.1	Script-Blocker	www.noscript.net	98/ME, 2000, XP, Vista	deutsch	111
Updatestar 2.0.464	Versions-Infoprogramm	www.updatestar.com	2000, XP, Vista	deutsch	111
Zone Alarm Free 7.0/7.1[1]	Firewall	www.zonealarm.com	2000, XP, Vista	deutsch	112

1) gratis für pirvate Nutzung

Anti-Phishing-Tool: McAfee Siteadvisor ist eine kostenlose Browser-Erweiterung, die vor gefährlichen Web-Seiten warnt (Punkt 3)

Postfach-Überwachung: Read Notify prüft, ob eine versandte Mail gelesen wird. So kommen Sie Spionen auf die Schliche (Punkt 4)

4. Benutzerkonto nutzen: Starten Sie Windows mit einem Konto, das nur mit Benutzerrechten ausgestattet ist. Der Kontentyp „Administrator" ist für die tägliche PC-Arbeit tabu. Wichtig: Ein Benutzerkonto mit Admin-Rechten sollten Sie immer übrig haben.

2. Malware klaut Ihre Online-Identität

Gefahr: sehr groß
Verbreitung: stark

Darum geht's: Malware, also Viren, Trojaner und andere Schädlinge, nisten sich in Ihrem PC ein. Ein großer Teil der Malware klaut anschließend Log-in-Daten. Dabei geht's längst nicht mehr nur ums Online-Banking, sondern um die Log-ins zu Paypal, die Kreditkartennummer oder Daten zu Online-Spielen. Denn dafür zahlen Kriminelle auf dem Schwarzmarkt bares Geld. Die Zahl neuer Schadprogramme steigt rasant. Im Jahr 2007 betrug das Speichervolumen aller erkannten Schadprogramme 354 Gigabyte; es waren 2,2 Millionen Schädlinge. Das sind vier Mal so viele wie 2006. Der Antiviren-Hersteller Kaspersky rechnet mit einer Verzehnfachung der neuen schädlichen Dateien für 2008: Dieses Jahr wird es also rund 20 Millionen neue Schädlinge geben.

Beispiel: Der Trojaner Ldpinch stiehlt Passwörter, die er in den Passwort-Managern gängiger Browser gefunden hat, und sendet sie an eine Mailadresse. Ldpinch tauchte das erste Mal schon im Jahr 2003 auf. Er verbreitete sich aber erst stärker, als im Jahr 2007 ein Baukasten entwickelt wurde, mit dem sich Varianten des Schädlings erstellen lassen. So entstehen neue Trojaner-Versionen mit wenigen Klicks.

Gegenmittel

1. Antiviren-Software nutzen: Installieren Sie ein Antiviren-Programm, etwa **Antivir Personal**.

2. Firewall installieren: Falls das Antiviren-Tool mal einen Schädling übersieht, blocken Sie die Spionage-Aktion der Malware mit einer Firewall. Empfehlenswert ist der kostenlose Klassiker **Zone Alarm Free**. Fortgeschrittene Anwender können sich die funktionsreiche und kostenlose Firewall **Comodo Firewall Pro Free** ansehen.

3. Phishing-Websites stehlen Ihr Bank-Log-in

Gefahr: gering bis mittel
Verbreitung: sehr stark

Darum geht's: In Ihrem Mailpostfach landen Nachrichten, die vorgeblich von Ihrer Bank kommen und Sie dazu verleiten sollen, einen Link in der Nachricht anzuklicken. Dieser Link öffnet eine Phishing-Website, die mehr oder weniger so aussieht wie die Site Ihrer Online-Bank. Dort werden Sie unter einem Vorwand darum gebeten, Ihre Log-in-Daten sowie meist mehrere TANs (Transaktionsnummern) einzugeben. Diese werden an die Kriminellen übermittelt, die dann Ihr Konto abräumen.

Gegenmittel

1. Bank-Website direkt aufrufen: Rufen Sie die Website Ihrer Bank durch Eingabe in der Browser-Adresszeile auf oder über die Bookmarks in Ihrem Browser. Achten Sie im ersten Fall darauf, dass Sie sich nicht vertippen, da Kriminelle solche Vertipper-Adressen oft mit einer Phishing-Website bestücken.

2. Nutzen Sie eine Antiphishing-Toolbar: Aktuelle Browser wie der Internet Explorer 7 und Firefox 2 bieten schon einen Basisschutz dank integriertem Anti-Phishing-Filter. Am besten erhöhen Sie diesen Schutz aber noch mit einer speziellen Toolbar. Empfehlenswert ist etwa **McAfee Siteadvisor**. Das Browser-Add-on schlägt Alarm, wenn Sie eine Phishing-Site oder eine andere gefährliche Website aufrufen.

4. Das Kennwort Ihres Mailpostfachs ist bekannt

Gefahr: mittel
Verbreitung: gering

Darum geht's: Kriminelle finden die Informationen in einem Mailpostfach sehr interessant. Denn je mehr Details sie über eine Person kennen, desto teurer lassen sich diese Infos verkaufen. Aber nicht nur Diebe sind scharf auf den Griff ins Postfach. Jeder dritte PC-Anwender würde auf fremden PCs herumschnüffeln, sobald sich eine gefahrlose Möglichkeit dazu bietet. Besonders anziehend sind laut einer Studie des Antiviren-Spezialisten Avira Rechner von Bekannten (weitere Infos unter **www.pcwelt.de/79769**).

An das nötige Kennwort für den Zugang kommen Kriminelle über spezielle Malware. Bekannte warten oft einfach ab, bis sie Ihnen bei der Eingabe des Passworts mal über die Schulter gucken können.

Gegenmittel

1. Passwort öfters ändern: Natürlich hilft ein neues Passwort für Ihr Mailkonto umgehend. Am besten, Sie ändern es routinemäßig jeden Monat.

2. Spion überführen: Wollen Sie herausfinden, ob jemand heimlich Ihre Post liest, müssen Sie dem Spion eine Falle stellen. Dafür schicken Sie an sich selbst eine Mail

und präparieren sie so, dass eine heimliche Rückmeldung stattfindet, sobald die Mail geöffnet wird. Dabei hilft etwa der Web-Dienst Read Notify (**www.readnotify.com**).

5. Betrugs-Freeware attackiert Ihren Geldbeutel

Gefahr: groß
Verbreitung: mittel

Darum geht's: Gauner bieten im Internet angebliche Freeware an, die den Anwender aber dazu verleitet, Geld für eine Pro-Version auszugeben. Meist sind es vorgebliche Sicherheits-Tools, die einen Scan des PCs vortäuschen. Sie melden, dass der PC mit einem Virus infiziert ist. Der Schädling lasse sich nur mit der kostenpflichtigen Version entfernen. Bei drastisch klingenden Warnungen ist der Druck auf den Anwender erheblich, die Kauf-Software zu bezahlen.

Wichtig: Fallen Sie nicht auf die Warnungen herein. Die meisten Abzocker-Tools melden Viren, die nicht vorhanden sind.

Für öffentliche WLANs: Hotspot Shield baut eine verschlüsselte VPN-Verbindung auf (Punkt 6)

Gegenmittel

1. Download mit Empfehlung: Sicherheits-Tools sollten Sie nur installieren, wenn diese von einem vertrauenswürdigen Anbieter stammen. Das unabhängige Sicherheitslabor AV-Test (**www.av-test.org**) bietet Links zu fast allen Antiviren-Herstellern der Welt.

2. Online-Scanner nutzen: Für einen Viren-Check gibt es Online-Scanner, die kostenlos nicht nur nach Viren suchen, sondern gefundene Schädlinge auch entfernen. Empfehlenswert ist etwa der Scanner unter **www.bitdefender.de**.

6. Man-in-the-Middle-Attacke bei WLAN-Hotspots

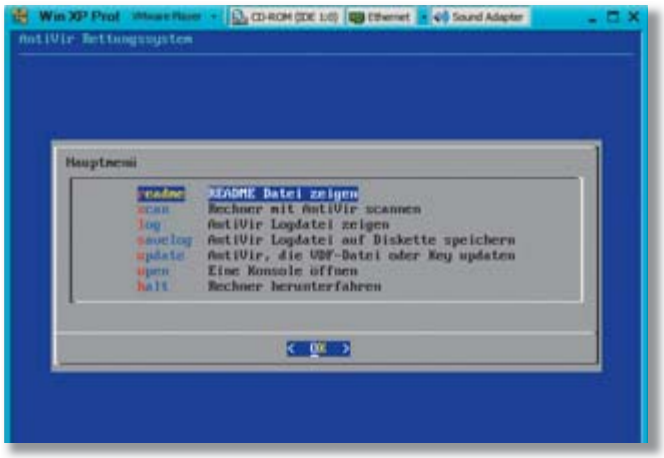
Gefahr: groß
Verbreitung: mittel

Darum geht's: Öffentliche WLAN-Hotspots sind mittlerweile verbreitet. So lässt sich in vielen Cafés kabellos mit dem eigenen Notebook surfen. Doch hier kann der Spion am Nachbartisch über eine Man-in-the-Middle-Attacke Ihre Daten mitlesen. Denn er hat sich in die Verbindung zwischen Ihrem Notebook und dem Access Point eingeklinkt.

Gegenmittel

1. Nutzen Sie ein zweites Mail-konto: Bei öffentlichen WLANs sollten Sie ›

Personensuchmaschine: Dienste wie Yasni.de wissen viel über Internet-Nutzer – inklusive der Wunschliste beim Online-Versender (Punkt 9)



Viren-Check: Das Antivir Rescue System laden Sie sich stets aktuell herunter und brennen es auf eine wiederbeschreibbare CD (Punkt 10)

nach Möglichkeit keine sensiblen Daten wie Passwörter und Kreditkartennummer eingeben. Um trotzdem neue Mails checken zu können, richten Sie sich ein zweites Mailkonto ein, etwa bei einem Freemailer wie Gmx.de, Web.de oder Google.de, und aktivieren Sie bei Ihrem Hauptmailkonto eine Weiterleitung auf diese Adresse. Sollte jemand im WLAN mitloggen, bekommt er nur das Passwort des zweiten Mailkontos, das Sie jederzeit löschen können. Er kann damit nicht auf Ihr Haupt-Mailkonto zugreifen, etwa um ältere Mails zu lesen oder unter Ihrem Namen Mails zu verschicken.

2. Mit VPN-Software surfen: Mit einer VPN-Verbindung (Virtual Private Network) bauen Sie eine gesicherte Verbindung auf. Angriffe darauf sind unwahrscheinlich. Kostenlos geht das mit der englischsprachigen Software **Hotspot Shield**. Der Anbieter stellt auch den nötigen VPN-Server gratis bereit. Die Handhabung ist ganz einfach.

7. Social Engineering raubt Ihnen das letzte Hemd

Gefahr: sehr groß
Verbreitung: stark

Darum geht's: Unter Social Engineering versteht man den Betrug mit Hilfe von psychologischen Tricks. Diese Methode ist extrem erfolgreich. Sie setzt etwa auf die Gier der Menschen. So versprachen Betrüger einem Australier riesige Gewinne, woraufhin dieser insgesamt rund 1,3 Millionen Euro überwies. Als ihm die Sache dann komisch vorkam, informierte er die Polizei. Die Gauner agierten von Europa aus. Bei Internet-Betrug sitzen die Kriminellen oft in einem anderen Land. Die ermittelnde Behörde schätzt, dass in Europa mindestens 18.000 Internet-Betrüger agieren. Oft setzen sie Social Engineering in Spam-artig versandten Mails ein, um die Empfänger zur Installation von Malware zu bewegen.

Gegenmittel

1. Seien Sie misstrauisch: Wenn etwas zu gut klingt, um wahr zu sein, dann ist es wahrscheinlich auch nicht wahr. Bleiben Sie stets misstrauisch.

2. Setzen Sie sich klare Regeln: Wenn Sie grundsätzlich nicht Ihre Kreditkartennummer rausgeben, dann können Sie

„18.000 Internet-Betrüger agieren in Europa, schätzen Ermittler der Polizei"

über diesen Weg auch nicht abgezockt werden. Mit klaren Regeln, was Sie von sich verraten und was Sie bereit sind zu tun, werden Sie nicht auf Betrüger hereinfallen.

8. Angriffe auf den DSL-Router verändern den DNS-Eintrag

Gefahr: sehr groß
Verbreitung: sehr gering

Darum geht's: Cyber-Kriminelle haben es auf die DSL-Router bei Privatnutzern abgesehen. Manipulierte Websites können mit einer Technik namens Cross Site Request Forgery auf den DSL-Router zugreifen und dort den Eintrag für den DNS-Server ändern (Domain Name System). Die Folge: Der Angreifer kann den PC des Anwenders auf beliebige Websites umleiten – etwa auf eine vorgebliche Bank-Site, die die Log-in-Daten stiehlt. Dieser Trick setzt allerdings voraus, dass der Router mit dem werkseitigen Standardpasswort läuft.

Ein weiterer Schwachpunkt ist die UPnP-Fähigkeit von vielen DSL-Routern (Universal Plug and Play). Flash-Dateien (Filme) können DSL-Router von Privatanwendern manipulieren, indem sie wiederum den DNS-Server verändern. Dabei benötigt der Angreifer kein Kennwort für den DSL-Router. Es genügt, dass der Anwender auf eine Website mit einer manipulierten Flash-Datei gelockt wurde und ein veraltetes Flash-Plug-in im Browser laufen hat. Weitere Infos über **www.pcwelt.de/c53**.

Gegenmittel

1. Passwort ändern: Ändern Sie das voreingestellte Standardpasswort, da sich sonst Angreifer über Sicherheitslücken von außen einloggen können. Führen Sie vor dem Ändern des Passworts ein Reset durch (Handbuch). Sollte die Box bereits manipuliert worden sein, wird die Änderung so rückgängig gemacht.

2. UPnP abstellen: Falls Sie Universal Plug and Play (UPnP) nicht benötigen, deaktivieren Sie es in Ihrem DSL-Router.

9. Ihre Datenspur im Web verrät zu viel

Gefahr: mittel
Verbreitung: stark

Darum geht's: Das Internet speichert allgemeine Infos und sehr persönliche Daten zu vielen Privatpersonen. Google und spezialisierte Personensuchmaschinen – etwa

www.yasni.de – finden alle diese Daten und zeigen sie jedem, der danach sucht. Das kann heikel werden, wenn man unvorsichtigerweise Infos ins Internet gestellt hat, die nicht jeder sehen soll. Die meisten Infos verraten die Anwender auf Community-Sites wie **www.myspace.de** oder **www.xing.de**. Aber auch Foren, das Usenet oder etwa der Wunschzettel bei **www.amazon.de** sind eine wahre Fundgrube für Personensuchmaschienen.

Gegenmittel

1. Nutzen Sie ein Pseudonym: Sie können das Pseudonym – also einen beliebigen Namen – um ein erfundenes Geburtsdatum ergänzen. Dann haben Sie einen Benutzernamen, der speziell genug ist, um bei allen möglichen Diensten frei zu sein – etwa Markus-Mustermann-01041963.

2. Schließen Sie Suchmaschinen aus: Wenn Sie Community-Sites nutzen, sollten Sie bei den Einstellmöglichkeiten festlegen, dass nur angemeldete Mitglieder dieser Community Ihre Daten sehen dürfen.

10. Angriffe über verseuchte Hardware

Gefahr: sehr hoch
Verbreitung: gering

Darum geht's: Malware schleicht sich über viele Wege auf den PC. Manchmal steht der PC sogar schon verseucht im Laden, und Sie haben die Pest im Haus, sobald Sie den Rechner einschalten. So geschehen etwa im September 2007 bei Aldi. Betroffen waren nach Angaben des Herstellers Medion ein Teil der vertriebenen Geräte des Typs MD 96290 – sie waren mit einem Bootvirus verseucht. In Australien verschenkte der PC-Hersteller HP USB-Sticks, auf denen sich ein Wurm befand.

Auch diese per Hardware übertragenen Schädlinge sind letztlich eine Internet-Gefahr, denn sie senden unter Umständen Ihre persönlichen Daten ins Web.

Gegenmittel

1. Antiviren-Software nutzen: Installieren Sie ein Antiviren-Programm, etwa etwa **Antivir Personal**.

2. Viren-Check mit Boot-CD: Gelegentlich sollten Sie Ihren PC mit einer bootfähigen Sicherheits-CD starten und dann nach Malware durchsuchen. So finden Sie Malware, die sich bei aktivem Windows versteckt. Empfehlenswert ist hierfür beispielsweise Aviras **Antivir Rescue System**.

Die Download-Falle

Die neue Abzock-Masche kann jeden treffen: Anwender werden mit scheinbar kostenlosen Downloads geködert. Mit wenigen Klicks haben sie einen Zwei-Jahres-Vertrag am Bein – und sind um 192 Euro ärmer.

Von **Tobias Weidemann**

Gratis kann teuer werden: Wer sich in der virtuellen Unterwelt herumtreibt, Filme, Software und Musik herunterlädt oder nach den neuesten Hacker-Tipps sucht, kann selbst Opfer und zur Kasse gebeten werden. So erging es einem PC-WELT-Leser. Marcel F. aus Lübeck erhielt eine Rechnung von der Firma Content Services Limited aus Mannheim: Er habe sich für den Dienst Opendownload.de (*www.opendownload.de*) registriert und sei zur Zahlung von 96 Euro verpflichtet.

Opendownload: Kostenlose Angebote für 96 Euro

Über *www.torrent.to* war Marcel F. dorthin geraten. Die Site bietet teils legale, teils in Deutschland illegale Downloads über das Bit-Torrent-Protokoll an. „Benutzen Sie immer einen aktuellen Client für mehr Geschwindigkeit und maximale Sicherheit“ hatte es direkt oben auf der Site geheißen. Darunter standen Links zu Downloads der aktuellen, vermeintlich kostenlosen Programme. Die Links führten jedoch nicht zur Website der jeweiligen Programmierer der Software, sondern zu Opendownload.de.

Einige Klicks später hatte der Leser die Software dort heruntergeladen, er musste seine Adresse angeben und sich registrieren. Der Haken an der Sache: Das Herunterladen eigentlich kostenlos erhältlicher Software kostet dort 8 Euro im Monat, also 96 Euro im Jahr. Das verrät ein kleiner Hinweis rechts neben dem Anmeldeformular. Da man ein nicht vorzeitig kündbares Zwei-Jahres-Abo eingeht, ist man gleich um 192 Euro ärmer. „Auf einen Werbebanner hätte ich gar nicht geklickt“, erklärt unser Leser. „Aber das Ganze sah aus wie ein Teil der Torrent-Site, und den Kostenhinweis bei Opendownload.de habe ich gar nicht gesehen.“

Noch gerissener gingen die Betreiber einer Site vor, die kostenlose Zeitschriften-PDFs und E-Books bereithielt (die Site wurde inzwischen vom Netz genommen). Sie präsentierten dem Site-Besucher die Information, sein Adobe Reader sei veraltet, und er könne jetzt die neue Version herunterladen. Ein Klick auf das Hinweisfeld brachte den Anwender ebenfalls zu Opendownload.de. Dabei handelte es sich nicht etwa um ein gewöhnliches Werbebanner, sondern um einen Hinweis des Browsers, der ober-

HIER LESEN SIE ...

- **womit** Anwender im Internet übers Ohr gehauen werden
- **warum** Sie in diesem Fall die Vorratsdatenspeicherung nicht fürchten müssen – auch wenn der Betrüger droht, sie zu nutzen
- **warum** so wenige abgezockte Surfer vor Gericht gehen

Fotos: pixelio.de

halb des Fensters auf gelbem Grund erscheint, ähnlich wie Sie das von unterdrückten Pop-ups kennen. Realisiert wurde das über ein Active-X-Element, und viele Anwender werden übersehen haben, dass es sich nicht um eine Statusmeldung des eigenen Browsers handelte. Schon deswegen ist es sinnvoll, derartige unsichere Programme zu unterdrücken – Firefox unterstützt sie erst gar nicht.

Vielfach verlinkte Abzocke via Google-Suche

Doch auch Surfer, die um heikle Websites einen weiten Bogen machen, sind nicht gefeit vor Download-Fallen. Die Abzocker verstehen sich gut auf Suchmaschinenoptimierung: Sie verlinken sich geschickt gegenseitig, und so landen Sites wie *www.opendownload.de* bei einigen Sucheingaben weit oben in der Google-Trefferliste. Durch diese Google-Optimierung tauchen Abzock-Links dann selbst auf seriösen Seiten wie *www.pcwelt.de* auf – und zwar innerhalb der Google-Suchergebnisse. Vorsicht ist also angebracht.

Wie viele Anwender bereits Opfer von Opendownload.de und ähnlicher Sites geworden sind, ist unbekannt. Sicher aber ist, dass sich die Mehrzahl der Leserzuschriften, die wir zu Abo-Sites bekommen, mit Content Services Limited befasst. Die in Mannheim ansässige Firma ist Teil einer Firmengruppe, die ihren Hauptsitz im britischen Cardiff hat. Die Content Services Limited unterhält ein weit verzweigtes Netz von Unternehmen. Mehrere Dutzend Sites konnten wir ermitteln, beispielsweise *http://jede-frau-abschleppen.de*, *http://www.fragschnell.de*, *http://neue-downloads.com*, *http://player-2009.net* oder *http://load2009.com*. Auch stießen wir auf Sites, bei denen die Anmeldung nicht mehr möglich ist.

Schlepper und Betreiber: Alle kassieren ab

Die gesamte Bandbreite an Themen wird abgedeckt – von Datenbanken (Downloads, Rezepte, Songtexte) über Ratgeber und Hilfe (etwa bei Hausaufgaben oder Bewerbungen) bis hin zu Lebenshilfe (Partnerschaft, Lebenserwartung). Die Sites arbeiten nach einem ähnlichen Muster wie Opendownload.de. Fast überall ist der Hinweis, welchen Vertrag der Kunde eingeht, zwar auf der gleichen Höhe wie das Adressfeld vorhanden; er ist aber so beiläufig, dass viele ihn übersehen müssen. Auch wird oft nur die Monatsgebühr angegeben, teilweise noch die Jahresgebühr, nicht aber, dass der Vertrag erst nach zwei Jahren gekündigt werden kann.

Billige Masche: Nur wenige Tools bietet Opendownload.de auf dem eigenen Server an. Meist wird – wie hier bei Google Earth – auf die Original-Site verlinkt

An den Abzock-Praktiken verdienen zwei Parteien: Zunächst der Betreiber der Site, die den Kunden weiterleitet – allerdings nur dann, wenn es zu einem Vertragsabschluss kommt. Aus diesem Grund greifen die Betreiber dieser „Schlepper-Sites“ oft zu Tricks wie den oben beschriebenen. Was pro erfolgreich vermitteltem Kunden gezahlt wird, ist im Fall Opendownload nicht bekannt. In vergleichbaren Fällen zahlt die Abzocker-Site zwischen 15 und 25 Prozent ihres Jahresumsatzes an die Schlepper-Site. Für die Schlepper ist das Geschäft risikolos – sie haben die Kunden lediglich vermittelt. Die geprellten Surfer werden kaum gegen ›

SO SCHÜTZEN SIE SICH Abwehrtipps gegen Download-Abzocke

Keine Chance für Abzocker: Mit unseren Tipps schützen Sie sich gegen die Abo-Falle.

✓ **Seien Sie misstrauisch**, wenn Sie Ihre persönlichen Daten angeben sollen, insbesondere Adresse, Telefonnummer oder Bankverbindung. Falls Sie fiktive Daten angeben: Denken Sie daran, dass Sie neben Ihrer IP-Adresse weitere Spuren hinterlassen, etwa eine auf Ihren Namen registrierte Mailadresse.

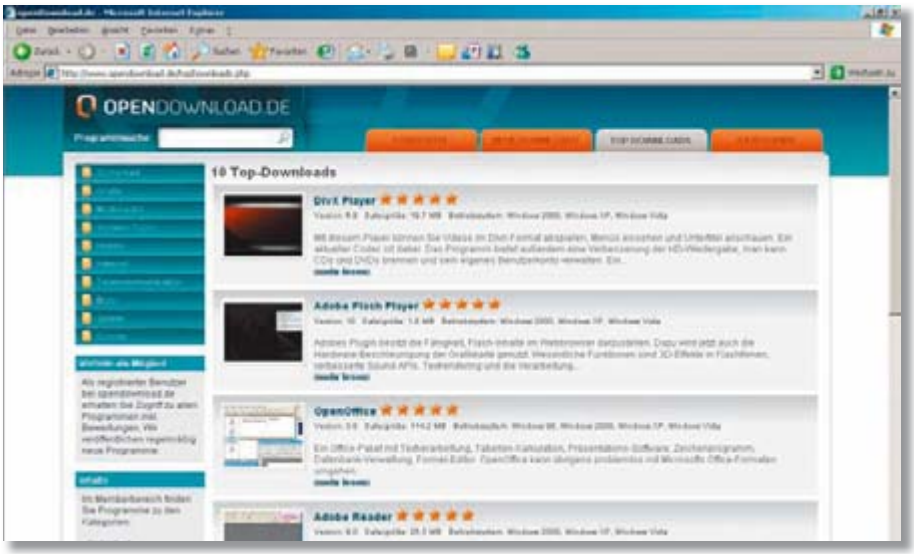
✓ **Prüfen Sie** die Allgemeinen Geschäftsbedingungen (AGB), und schauen Sie auf mögliche Zahlungsverpflichtungen. Speichern Sie die AGB und andere Vertragsbestandteile als PDF ab. Oder erstellen Sie eine Kopie der Seite, die diese zum Zeitpunkt des Vertragsschlusses dokumentiert (etwa mit dem kostenlosen *www.furl.net*). Denn: Auch online können Sie einen gültigen Vertrag eingehen.

✓ **Prüfen Sie bei Erhalt** einer unerwarteten Rechnung, ob Sie wirklich einen Vertrag eingegangen sind. Dazu muss der Anbieter in geeigneter Weise über die Vertragsbestandteile informiert haben. Ein kleiner Hinweis auf die Art der Vertragsbeziehung, möglicherweise ganz am Ende der Seite oder gar nur in den AGB, reicht hierfür nicht aus.

✓ **Auch wenn ein Inkassobüro** eingeschaltet wird, müssen Sie nicht nervös werden. Wichtig zu wissen: Die Extrakosten fürs Inkasso trägt der Anbieter des Dienstes, sofern die Rechnung nicht rechtens ist. Erst wenn ein gerichtlicher Mahnbescheid eintrifft, müssen Sie reagieren: Legen Sie unbedingt binnen 14 Tagen Einspruch ein. Wichtig: Das Gericht, das den Mahnbescheid ausgefertigt hat, hat den Fall nicht geprüft, sondern verlässt sich auf die Aussage des Rechnungsstellers.

✓ **Lassen Sie sich nicht einschüchtern**, auch wenn das Unternehmen mit der Vorratsdatenspeicherung droht. Vermeiden Sie jede unnötige Kommunikation mit dem Rechnungssteller. Insbesondere wenn er Ihre persönlichen Daten (mit Ausnahme der Mailadresse) nicht kennt, brauchen Sie ihm diese auch nicht nachträglich mitzuteilen.

✓ **Jugendliche unter 18 Jahren** können ohne die Zustimmung ihrer Eltern keine Abo-Verträge abschließen. Abgesehen davon: Auch die Eltern haften nur dann, wenn sie ihrer Aufsichtspflicht nicht in ausreichendem Maß nachgekommen sind. Inwieweit sie diese aber im Internet erfüllen müssen (und ob sie das überhaupt können), ist fraglich.



Kostenloses für viel Geld: Der zwielichtige Dienst Opendownload.de bietet nichts, was Sie nicht anderswo gratis bekämen – und das für stolze 192 Euro

die Schlepper vor Gericht ziehen, da sie dann oft zugeben müssten, Sites besucht zu haben, die auch illegale Inhalte anbieten.

Kostenpflichtige Beschwerden: Hotlines bitten zur Kasse

Neben den Anwendern, die zähneknirschend ihre Rechnung bezahlen (pro Kunde immerhin knapp 200 Euro), hat die Opendownload-Abzock-Site eine weitere lukrative Einnahmequelle entdeckt: die Telefongebühren für ihre völlig nutzlose Hotline. Egal zu welcher Tageszeit wir die Hotline anriefen, wir erlebten immer das gleiche: Eine freundliche Frauenstimme weist auf die Sprechzeiten der Hotline hin, teilt mit, dass wir gleich verbunden werden – bis wir schließlich mit einem Hinweis, dass der Teilnehmer nicht erreichbar sei, aus der Leitung fliegen. Selbst wenn es sich hierbei nur um eine 01805-Nummer handelt, die den Anwender 14 Cent pro Minute kostet, landen bei jedem Telefonat einige Cent in der Kasse der Abzocker.

Heiße Luft für viel Geld: 8 Euro pro Monat für nichts als Links

Was bekommt der Kunde eigentlich für seine 8 Euro monatlich von Opendownload? Open Office ist die aktuelle Empfehlung der Site – doch die Datei wird nicht einmal bei Opendownload.de bereitgestellt. Statt dessen gibt es nur einen Link auf die Projektseite. Überhaupt finden sich hier nur kostenlos erhältliche Tools, und die sind – zumindest im Fall der Software größerer Unternehmen (etwa Microsoft, Google, verschiedene Sicherheits-Software-Hersteller) – auch lediglich verlinkt. Eine Ausnahme bildet bislang Adobe: Hier stellt Opendownload den Flash-Player und den Adobe Reader in der jeweils aktuellen Version zur Verfügung – und das, obwohl das Unternehmen selbst seriösen Sites lediglich das Verlinken auf Adobe-Server gestattet. Die Hersteller der Programme sind verständlicherweise wenig begeistert. „Das kann uns nicht egal sein, wenn hier mit unserem guten Namen Kunden hinters Licht geführt werden“, erklärt ein Adobe-Sprecher. Der Fall werde derzeit geprüft.

Abzock-Versuch per Mail-Rechnung und IP-Adresse

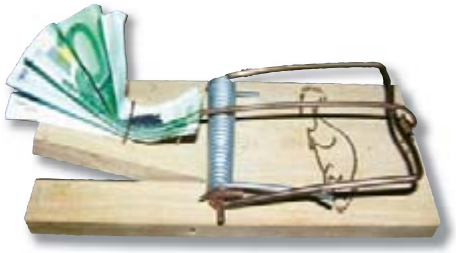
Viele Anwender haben sich nur mit einer gültigen E-Mail-Adresse und falschen Adressangaben angemeldet. Aber auch sie bekommen ihre Rechnung – diese wird ja wie die Zugangsdaten per Mail verschickt. Die Betreiber von Opendownload.de & Co. speichern die IP-Adresse des unfreiwilligen Neukunden und teilen ihm in sämtlichen Rechnungen und Mahnschreiben mit, unter welcher IP-Adresse er wann bei ihnen war. Aufgrund der Vorratsdatenspeicherung seien sie in der Lage, mit Hilfe der Ermittlungsbehörden den Beweis beim Provider anzufordern.

Das ist nur ein Bluff: Die Abzocker kämen gar nicht an die persönlichen Daten ihrer hereingelegten Kunden. Denn nach einem Verfassungsgerichtsurteil vom März 2008 ist es zwar korrekt, dass die Daten vom Provider erfasst und ein halbes Jahr lang gespeichert werden. Hinz und Kunz haben aber nicht das Recht, die Daten einzusehen. Selbst die Staatsanwaltschaft darf sich lediglich bei „schweren Straftaten“ Zugriff auf die Provider-Daten verschaffen. Darunter fallen zwar Computerdelikte und Betrug am PC, allerdings nur sofern ein „Vermögensverlust größeren Ausmaßes“ herbeigeführt wird oder falls durch die „fortgesetzte Begehung von Betrug“ viele Menschen geschädigt werden. Das Gesetz ließe sich eher gegen die Betreiber solcher Sites anwenden als zu deren Nutzen.

Abgemahnt: Abzocker reagieren einfach nicht

Dass die Betreiber vor Gericht ziehen, ist unwahrscheinlich. Schließlich würde dann überprüft, ob die Information darüber, dass der Kunde einen rechtlich bindenden Vertrag abschließt, ausreichend groß und auffällig an der richtigen Stelle positioniert ist. Und es würde untersucht, ob der Vertrag überhaupt zustande gekommen ist: Der Kunde verzichtet nämlich etwa bei Opendownload explizit auf sein Widerrufsrecht. Es ist zwar möglich, dass dieses vorzeitig mit Bereitstellung eines Dienstes erlischt (in diesem Fall also mit der Übermittlung der Zugangsdaten) – nicht aber, dass ein Kunde von vornherein darauf verzichtet.

Der Bundesverband der Verbraucherzentralen (*www.verbraucherzentrale.de*) hat Opendownload.de im Herbst 2008 mehrfach abgemahnt, unter anderem wegen fehlender Endpreisangabe und unangemessener Benachteiligung des Verbrauchers durch die AGB. Zudem wurde ein Verfahren wegen der Beeinträchtigung der Entscheidungsfreiheit der Verbraucher eingeleitet, da in Rechnungen behauptet wurde, die falsche Angabe des Geburtsdatums stelle ein Betrugsdelikt dar. Da Opendownload die Unterlassungserklärungen nicht unterschrieben hat, bereitet die Verbraucherzentrale eine Unterlassungsklage vor. Doch das kann dauern – und muss Opendownload nicht schrecken. Denn im Zweifelsfall ist schnell eine andere Site erstellt, mit der man erneut auf Kundenfang gehen kann.



Abgezockt und ausgeplündert

Die neuen Tricks der Online-Gangster

Bedrohung aus dem Netz: Das Internet ist ein Tummelplatz für Verbrecher aller Art. Hier erfahren Sie, mit welchen Tricks die Online-Betrüger arbeiten und wie Sie sich und Ihr Geld schützen.

Von **Tobias Weidemann**

Die Ganoven von heute sitzen seelenruhig am PC oder Notebook – irgendwo in der Welt. Über das Internet bringen sie ihre Opfer per gestohlener Kreditkartendaten um ihr Geld, bitten sie über Abonnements auf fadenscheinigen Websites oder über vermeintliche Virenmeldungen zur Kasse.

Sicher surfen: Mit einigen Vorkehrungen können Sie auch in Zukunft weitgehend sicher ins Web gehen. Wir erklären Ihnen, worauf Sie achten müssen, wenn Sie den Browser starten, und welche Tools Ihnen dabei helfen, gute Websites von bösen zu unterscheiden.

Trick 1: Sicherheits-Tools, die keine sind

Das kann passieren: Beim Surfen poppt ein Fenster auf: „Ihr PC ist möglicherweise mit Viren verseucht. Klicken Sie hier, um die Schädlinge zu entfernen.“ Der Klick leitet Sie auf eine Site weiter, die angeblich Ihren Rechner nach Schädlingen durchsucht – und auch immer welche findet. Danach erhalten Sie eine vermeintlich sichere Antiviren-Software zum kostenlosen Download. Doch die Überraschung kommt nach dem Start: Um das Tool nutzen zu können, müssen Sie erst eine Lizenz erwerben. Die bekanntesten Sites dieser Machart sind *www.virus-scanonline.com* und *www.winantivirus.com*. Ähnliches gibt's mit Antispyware-Tools auf den Seiten *www.mynetprotector.com* und *www.spystriker.com*.

Anders als versprochen handelt es sich nämlich in den uns bekannten Fällen zwar um einen Gratis-Virenscanner, das Beseitigen von Viren ist aber kostenpflichtig. Noch schlimmer: Um tatsächlich Schädlinge zu finden, installiert ein solches Programm oftmals selbst Viren, Trojaner & Co. Selbst wenn das Tool das nicht tut, wird bei Cookies und anderen minder schlimmen Bedrohungen Alarm geschlagen – man will dem Kunden schließlich vermitteln, dass der Kauf der Software unumgänglich ist. Die angebotenen Tools werden, wenn überhaupt, deutlich seltener mit neuen Virensignaturen versorgt als die bekannten Virenscanner.

HIER LESEN SIE ...

- **wie** schnell Sie im Internet Opfer von Betrügern werden und warum selbst umsichtige Kunden davor nicht sicher sind
- **warum** Sie nicht jeder Warnmeldung trauen sollten
- **wie** Betrüger mit Ihrer Kreditkarte einkaufen
- **welche** Tricks einige Anbieter von Internet-Abos anwenden
- **wann** billige Software für Sie teuer wird
- **warum** Spurensicherung auch im Internet wichtig ist und wie Sie vorgehen müssen

SICHERHEIT SCHAFFEN Kostenlose Tools gegen den Netz-Nepp

Produkt	Einsatzzweck	Win-Betriebssysteme	Internet	Sprache	Seite
Antivir Personal Free Antivirus 8.0	Antiviren-Software	2000, XP, Vista	*www.free-av.de*	deutsch	75
Firefox 3.0 PC-WELT Edition 3.0.1	Sicherer Browser	98/ME, 2000, XP, Vista	*www.pcwelt.de/1b0*	deutsch	75
McAfee Site Advisor 2.5	Sicherheits-Tool	98/ME, 2000, XP, Vista	*www.mcafee.com*	deutsch	76
Norton Antivirus 2008 [1)]	Antiviren-Software	XP, Vista	*www.symantec.com/de*	deutsch	75
Operator 3.1	Anonym-Browser	98/ME, 2000, XP	*http://letwist.net/operator*	englisch	78

Dunkle Geschäfte: Im Internet werden gestohlene Kreditkartendaten gehandelt. Verhindern Sie, dass Ihre Daten dabei sind

Falscher Alarm: Manche Meldung über eine mögliche Gefährdung Ihres PCs dient nur dazu, dass Sie ein angebotenes Programm kaufen

So schützen Sie sich: Lassen Sie die Finger von Programmen, die Ihnen ungefragt beim Surfen im Netz angeboten werden. Nutzen Sie nur Programme, die Sie kennen oder die Ihnen seriöse Quellen wie die PC-WELT ans Herz legen. Leistungsfähig und kostenlos ist beispielsweise **Antivir Personal Free Antivirus** . Auch **Norton Antivirus 2008** leistet hier hervorragende Dienste.

Der richtige Browser: Sie können auch auf **Firefox 3** setzen. Das Programm bietet einige wirkungsvolle Schutzmechanismen vor solchen Nepp-Seiten, die es anhand einer Blacklist aus dem Internet identifiziert. In der aktuellen Version wird der Browser Sie in einigen (aber nicht allen!) Fällen gar nicht erst auf solche Sites lassen, sondern bereits vorher darüber informieren, dass es sich um nicht vertrauenswürdige Sites handelt – glauben Sie ihm.

Trick 2: Phishing und Datendiebstahl

Das kann passieren: Auf Ihrer Kreditkartenabrechnung oder Ihrem Kontoauszug tauchen Zahlungen auf, die Sie nicht veranlasst haben. Größere Summen wurden ohne Ihr Wissen von Ihrem Konto abgebucht, oder Ihre Kreditkarte wurde belastet.

Sie sind möglicherweise Opfer eines Phishing-Angriffs geworden. Über diesen Datenklau haben wir bereits mehrfach berichtet: Dabei werden Kunden unter einem Vorwand aufgefordert, sich auf der Website ihrer Bank anzumelden. Der angegebene Link führt jedoch zu einer betrügerischen Website, auf der man nach Zugangsdaten gefragt wird und eine oder mehrere Transaktionsnummern (TANs) eingeben soll. Stutzig machen sollte es Sie in jedem Fall, wenn mehrere TANs auf einmal verlangt werden – denn das würde keine Bank tun.

Eine gänzlich andere Betrugsmethode ist das Ausspähen von Kreditkartendaten. Das läuft eher selten über Phishing-Sites, sondern meist mit Hilfe eines Keyloggers oder Trojaners. Die Kartendaten werden anschließend auf Online-Plattformen verkauft. Gerade einmal 5 bis 40 US-Dollar kostet ein Datensatz, bestehend aus Kreditkartennummer, Sicherheitszahl und Gültigkeitsdatum. Die Preise richten sich nach Herkunftsland, ausgebender Bank und Art der Karte (Standard- oder Platinkarte). Bei Kartendaten mit 24-Stunden-Garantie erhält der Käufer Ersatz, sofern die Karte bereits gesperrt wurde.

Die Käufer nutzen die Daten auf zwei Arten: Entweder schreiben sie sie mit Hilfe von „Carder Packs“ auf gefälschte Kreditkartenrohlinge, oder sie nutzen sie direkt zum Einkauf im Internet. Dabei erstehen sie ›

Waren für sich persönlich oder auch mit dem Ziel, sie auf dem Schwarzmarkt weiterzuverkaufen.

So schützen Sie sich: Die Freeware **McAfee Site Advisor 2.5** schlägt Alarm, wenn Sie auf einer Website landen, die bereits durch Phishing in Verruf geraten ist. Nutzen Sie zusätzlich eine aktuelle Antiviren-Software, um vor Trojanern und Keyloggern geschützt zu sein. Wenn Ihnen Ihre Bank vermeintlich eine Mail schreibt, sollten Sie sich zudem die URL des entsprechenden Links gut ansehen. Fahren Sie dazu über den Link, und schauen Sie unten links in der Unterzeile des Browsers, auf welche Seite man Sie umleiten will. Handelt es sich dabei nicht um die Site Ihrer Bank, sollten Sie die Mail ignorieren. Grundsätzlich empfehlen wir, nie auf einen Link in einer Mail zu klicken, sondern die Website direkt im Browser anzusteuern.

„Gestohlene Kreditkartendaten werden für ein paar Euro im Netz gehandelt“

Sicher shoppen: Komplizierter liegt der Fall bei Kreditkartendaten. Verringern Sie das Risiko des Datendiebstahls, indem Sie nur auf vertrauenswürdigen Sites einkaufen (achten Sie zum Beispiel auf das Trusted-Shops-Logo). Bevorzugen Sie eine gesicherte SSL-Verbindung, um sich davor zu schützen, ausgespäht zu werden.

Doch das reicht nicht aus: Werden auf der Händlerseite Daten abgefangen, trifft es auch große Anbieter wie kürzlich einen großen Ticket-Händler und eine Flug gesellschaft. Immerhin erleichtert das dem Kunden die Argumentation gegenüber seiner Bank. Denn die Geldinstitute verschanzen sich im Schadensfall oft hinter der Aussage, der Kunde habe offensichtlich fahrlässig gehandelt und Dritten das Ausspähen ermöglicht. Wer hier nachweisen kann, dass er stets eine aktuell gehaltene Security-Software einsetzt (mindestens bestehend aus Firewall und Virenschutz), hat ausreichend vorgesorgt, wie im Juni 2008 das Amtsgericht Wiesloch entschied (Az. 4 C 57/08).

Sind Sie Opfer eines Kreditkartenbetrugs geworden, informieren Sie umgehend Ihre Bank und fordern Sie die Rückbuchung der entsprechenden Zahlung. Die Bank wird daraufhin vom Verkäufer eine Legitimation für den Kauf verlangen, zum Beispiel einen Beleg mit Ihrer Unterschrift.

Teure Fahrt: Wer auf diesem Routenplaner landet, ist gleich eine Menge Geld los – er schließt ein Abo ab

Trick 3: Gratis testen lassen, Kündigung ignorieren

Das kann passieren: Nahezu im Wochenrhythmus hören wir von neuen Abzocktricks, bei denen irgendeine banale Dienstleistung, die es im Netz in der Regel auch gratis gibt, mit einer dubiosen Abo-Masche kombiniert wird. Egal ob Routenplaner (*www.routenplaner-server.com*), Hausaufgaben und Referate (*www.hausaufgaben-heute.com*) oder Kochrezepte (*www.ihre-rezepte.de*) – alles ist im Angebot. Auch vermeintlich kostenlose SMS-Nachrichten (*www.smsfree100.de*) sind dabei, für die etwa eine Monatsgebühr in Höhe von 12 Euro fällig wird. Kündigen lässt sich der Vertrag erst nach 24 Monaten, so dass Gesamtkosten in Höhe von 288 Euro auflaufen.

In nahezu allen Fällen stehen zwar irgendwo die Kosten für den Dienst – doch entweder sehr versteckt innerhalb eines riesigen Vertragstextes oder aber schwer lesbar, etwa in kleiner, hellgrauer Schrift auf hellbraunem Untergrund.

CHECKLISTE Fünf Tipps gegen Online-Betrug

1. Keine persönlichen Daten

Seien Sie zurückhaltend, wenn es um Ihre persönlichen Daten geht. Gerade wenn es sich um (vermeintlich) kostenlose Angebote handelt, benötigt der Anbieter weder Ihre Konto- noch Ihre Adressdaten. Beachten Sie, dass Sie bei kostenlosen Angeboten oftmals akzeptieren müssen, dass Ihre persönlichen Daten weiterverkauft werden.

2. Links prüfen

Wenn Sie Links aus Mails anklicken, sollten Sie immer zuvor untersuchen, wohin diese Sie führen. Das Ziel der Verknüpfung sehen Sie in der Fußzeile des Browsers (unten links im Fenster).

3. Anonym surfen

Seien Sie sich bewusst, dass man Sie immer und überall anhand Ihrer IP-Adresse erkennen kann. Weitgehende Anonymität erreichen Sie mit Hilfe eines anonymisierenden Browsers, einer Kombination aus Verschleierungs-Software und Browser (etwa **Operator**). Setzen Sie diesen ein, wenn Sie Ihre Identität für sich behalten wollen.

4. Beweise sichern

Falls Sie befürchten, dass Sie reingelegt wurden, sichern Sie Beweise. Dazu reicht es manchmal aus, Screenshots der AGBs zu erstellen oder diese auszudrucken. Im Zweifelsfall aussagekräftiger ist aber eine Kopie der Internet-Seite – so, wie sie zum Zeitpunkt des Vertragsabschlusses oder kurz danach im Netz stand. Zuverlässig, einfach und kostenlos erledigt das der Social-Bookmarking-Dienst Furl (*www.furl.net*). Jedem Anwender stehen hierfür 5 GB Speicherplatz zur Verfügung.

5. Infos sammeln

Wenn Ihnen auf einer Website etwas komisch vorkommt, sollten Sie sich die Zeit nehmen und nach dem Anbieter googeln. Vielleicht finden sich in einschlägigen Verbraucherschutzforen bereits Erfahrungsberichte über den Anbieter. Im Zweifelsfall gilt auch hier: Verlassen Sie sich auf den gesunden Menschenverstand – das erspart Ärger.

Die üblichen Verdächtigen: Sites, die bereits als Abzocker bekannt sind, zeigt der neue Firefox erst gar nicht an

Heiße Ware: Bei extrem günstiger Software, die zum Download angeboten wird, handelt es sich oft um illegale Lizenzen

Das Prozedere ist immer gleich: Beim ersten Nutzen des Services werden die persönlichen Daten (meist Adresse, Telefonnummer, Mailadresse und Geburtsdatum) abgefragt. Zumeist wird ein kostenloser Testzeitraum angeboten, innerhalb dessen man sich problemlos wieder abmelden können soll – so wähnt sich der Kunde in Sicherheit. Eine trügerische Sicherheit: Kündigungen werden sehr oft einfach ignoriert.

Reagiert der Kunde nicht auf Zahlungsaufforderungen und Mahnungen, kommt in der Regel ein Inkassounternehmen ins Spiel, das die Summe oftmals recht nachdrücklich einfordert. Um Diskussionen aus dem Weg zu gehen, zeichnen solche Dienste meist die IP-Adresse des Anwenders auf. Mit Hilfe des Internet-Providers lässt sich nachvollziehen, von welchem Anschluss aus das Abo abgeschlossen wurde. Eltern, deren Kinder versehentlich einen solchen Dienst bestellt haben, wird Verletzung der Aufsichtspflicht vorgeworfen.

So schützen Sie sich: Seien Sie misstrauisch, wenn eine Website Sie nach Ihren persönlichen Daten (etwa nach Kontodaten und Postadresse) fragt. Haben Sie oder ein Mitglied Ihres Haushaltes ungewollt ein Abo abgeschlossen, können Sie möglicherweise der Rechtmäßigkeit der Forderung widersprechen. Das setzt aber voraus, dass die Konditionen des Angebots nicht ausreichend klar ersichtlich waren oder dass derjenige, der den Vertrag abgeschlossen hat, hierzu aus Altersgründen noch nicht berechtigt war. Erstellen Sie zur Beweissicherung Screenshots von der dubiosen Seite, oder speichern Sie eine Kopie.

Uns ist kein Fall bekannt, in dem ein solches Unternehmen vor Gericht erfolgreich seine Forderungen eingeklagt hat. Die Gerichte urteilten hier meist, dass die Kosten auf der Website zu versteckt angebracht sind (Amtsgericht München Az 161 C 23695/06) oder nur in den AGB erscheinen. Umgekehrt haben auch einzelne Verbraucherzentralen Betreiber solcher Sites wegen „mangelnder Preisklarheit und Preiswahrheit" verklagt und Recht bekommen (Landgericht Hanau Az 9 O 870/07).

Die Betreiber dürften wenig Interesse daran haben, dass ihre Geschäftspraktiken überhaupt zum Gegenstand eines Gerichtsverfahrens werden – das hält sie meist vom Einreichen einer Klage ab.

Anonym surfen: Sie können verhindern, dass sich Ihre IP-Adresse zuordnen lässt. Wir empfehlen die Freeware **Operator**, eine Kombination aus dem kostenlosen Browser Opera (*www.opera.com*) und der Anonymisier-Software Tor (*www.torproject.org/index.html.de*). Dabei übertragen Sie Daten mit Hilfe eines komplexen Netzwerks aus mehreren tausend Rechnern anonym.

„Vor Gericht bekommen Abo-Gauner Ärger wegen mangelnder Preisklarheit"

Der Datenstrom wird in Fragmente aufgeteilt, die über unterschiedliche Knoten laufen. Da es sich um ein dezentrales Routing auf Zufallsbasis handelt, könnte nicht einmal der Erfinder des Systems herausfinden, welche Datenpakete welchen Weg genommen haben.

Es gibt auch verschiedene Tor-Plug-ins für den Firefox. Diese sind aber komplizierter einzurichten.

Trick 4: Illegale Billig-Software bringt rechtlichen Ärger

Das kann passieren: Sie finden eine Website, auf der es aktuelle Software deutlich günstiger zu kaufen gibt als bei Amazon, Media Markt & Co. Windows Vista Ultimate wird für rund 40 Euro angeboten, Adobe Photoshop CS3 für 85 Euro und Microsoft Office 2007 für rund 50 Euro. Begründet werden die verlockend niedrigen Preise damit, dass es sich um als Großposten eingekaufte OEM-Versionen handle. Das Bezahlen erfolgt meist im Voraus per Kreditkarte. Danach erhalten Sie einen Download-Link oder die Ware auf CD oder DVD – wenn Sie Glück haben. Leser informieren uns immer wieder, dass sie Geld gezahlt und dafür keine Gegenleistung bekommen haben.

Doch selbst wenn die Software auf Ihrem Rechner landet, sind Sie noch nicht aus dem Schneider: Denn in den meisten Fällen handelt es sich schlichtweg um illegale Freischaltcodes, die ein Codegenerator erzeugt, wobei er den Freischalt-Algorithmus der Software austrickst. Das bringt dann oftmals beim Download eines Updates Ärger. Im schlimmsten Fall funktioniert die Software gar nicht erst, und Sie werden natürlich vom Hersteller keinerlei Unterstützung erhalten. In der Regel lassen sich solche Shops nur per Mail oder Anrufbeantworter erreichen.

So schützen Sie sich: Informieren Sie sich vorher im Internet, ob schon jemand Erfahrungen mit einem bestimmten Anbie-

ter hat. Je günstiger und unglaublicher das Angebot klingt, desto misstrauischer sollten Sie werden.

Falls Sie auf ein solches Angebot hereingefallen sind und tatsächlich Ware mit einer zweifelhaften Seriennummer erhalten haben, versuchen Sie nicht, diese über Ebay

„Wer illegale Software weiterverkauft, bekommt oft teure Post vom Hersteller“

oder auf anderem Wege einem unwissenden Dritten unterzujubeln – Sie machen sich strafbar und werden in aller Regel mit einer Schadenersatzforderung des geprellten Unternehmens bedacht – Anwalts- und Abmahnkosten in vierstelliger Höhe drohen.

OEM-Software: Die gibt es wirklich – auch bei seriösen Händlern oder Versendern. OEM (Original Equipment Manufacturer) bedeutet lediglich, dass Sie keinen Support vom Hersteller, sondern vom Händler erhalten, was generell noch nichts Schlechtes sein muss. In einigen Fällen – etwa bei aktueller Adobe-Software – gibt es jedoch gar keine OEM-Versionen (mit Ausnahme der Elements-Programme, die teilweise mit Kameras ausgeliefert wurden). Ein Händler, der eine aktuelle Adobe-OEM-Software der höheren Preisklasse anbietet, muss Sie also misstrauisch machen.

Trick 5: Abmelden von Spam bingt noch mehr Spam

Das kann passieren: Sie erhalten regelmäßig ungefragt Spam-Mails von Viagra-Lieferanten, Online-Casinos und anderen Anbietern. Einige davon scheinen richtig nett zu sein – sie bieten Ihnen am Ende der Mail eine Abmeldemöglichkeit als Link an, falls Sie „versehentlich in den Verteiler aufgenommen wurden“. Wenn Sie dort Ihre Mailadresse mit Bitte um Abmeldung eintragen, habe der Spuk ein Ende, verspricht man Ihnen. „Zur Sicherheit“ und „zum Schutz gegen Missbrauch“ müssen Sie in einigen Fällen zusätzlich Ihre Postadresse und Ihren Namen angeben.

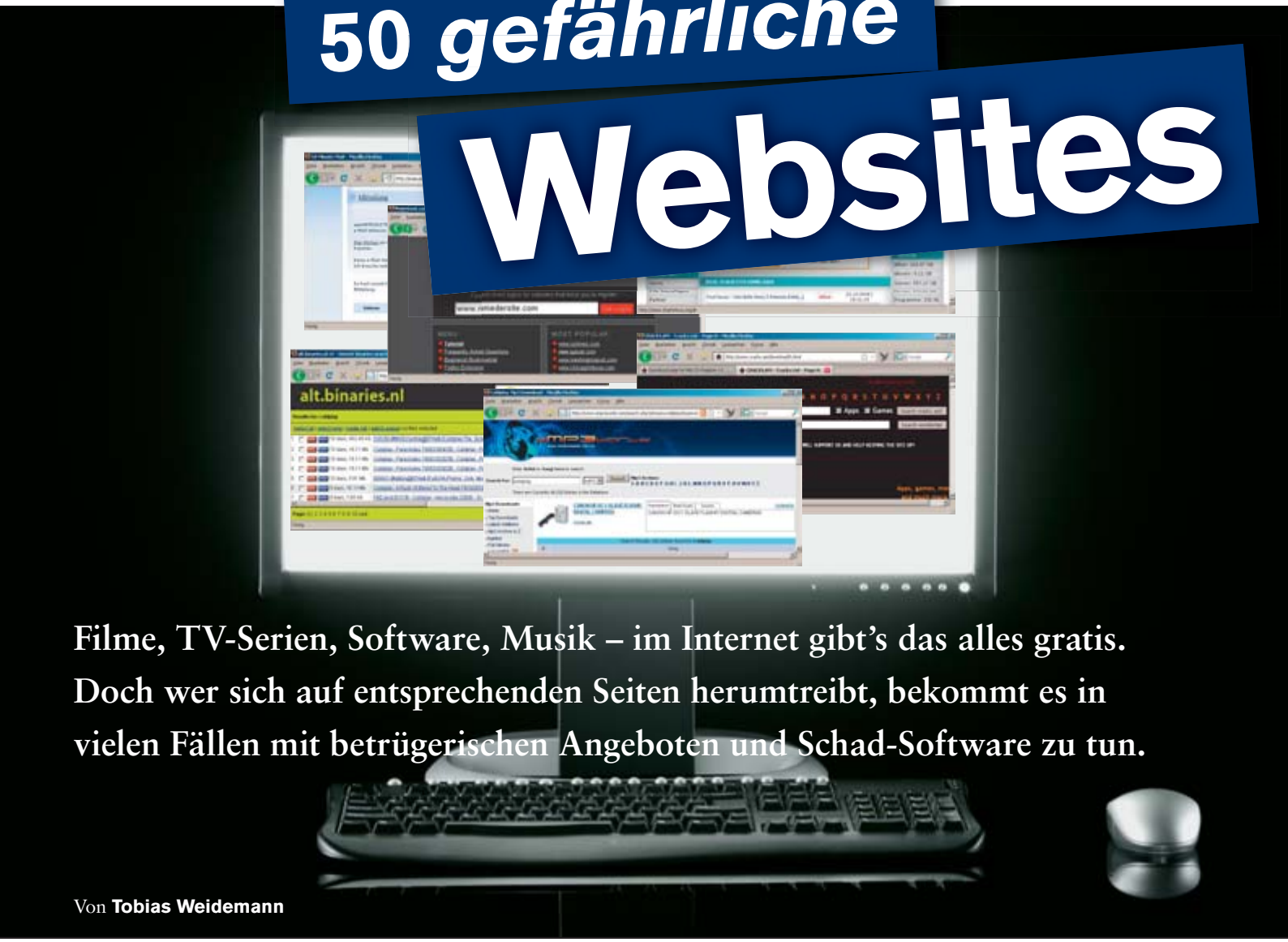
Die Folge: Sie erhalten noch viel mehr unerwünschte Mails als vorher. Der Grund: Die Spammer, die ihre Mails oftmals wahllos an existierende und nicht existierende Adressen verschicken, können erst einmal nicht wissen, welche Adressen tatsächlich genutzt werden und auf welchen wirkungsvolle Spamfilter das Gros der unerwünschten Mails herausfiltern. Erst durch Ihre Antwort zeigen Sie den Spammern, dass Sie ihre Mail wahrgenommen haben. Solche Mailadressen sind auf dem Spam-Markt noch mehr Geld wert – erst recht, wenn neben der Mailadresse auch Name und Wohnort des Opfers bekannt sind.

So schützen Sie sich: Antworten Sie grundsätzlich nicht auf Spam-Mails, und rufen Sie auch nicht die dort angegebenen Seiten auf. Denn oftmals werden Links so generiert, dass der Spammer anhand einer Prüfnummer sehen kann, welcher Empfänger auf den Link geklickt hat. Auch das ist ein eindeutiger Beweis dafür, dass die Mail wahrgenommen wurde, und macht eine Adresse wertvoller.

Hinweis: Diese Praktiken tauchen in der Regel nur bei Spam-Versendern auf, nicht bei seriösen Unternehmen, die oft auch eine solche Abmeldemöglichkeit anbieten.

Alles gratis?

50 gefährliche Websites



Filme, TV-Serien, Software, Musik – im Internet gibt's das alles gratis. Doch wer sich auf entsprechenden Seiten herumtreibt, bekommt es in vielen Fällen mit betrügerischen Angeboten und Schad-Software zu tun.

Von **Tobias Weidemann**

Im Internet gibt es fast nichts, was es nicht gibt: Filme, noch bevor sie im Kino anlaufen, Musikalben mit Bonustiteln, die in Deutschland nicht veröffentlicht worden sind, oder Software, die so nicht im Handel erhältlich ist. Das Internet ist ein Umschlagplatz, der bei den Verantwortlichen von Filmstudios, Plattenfirmen und Software-Häusern für schlaflose Nächte sorgt. Auch wenn nicht jeder illegale Download anstelle eines Kaufs erfolgt, geht der Schaden für die Unternehmen in die Millionen.

Wir haben im Internet recherchiert und stellen Websites vor, die zum Teil wirklich gefährlich sind. Einige Spezialbegriffe, mit denen Sie in den dunklen Ecken des Internets konfrontiert werden könnten, erklären wir in unserem Glossar auf Seite 79.

Das sagt das Gesetz: Auch zum Testen dürfen Sie keine Dateien herunterladen, die das Urheberrecht verletzen. Das kann zivilrechtliche oder sogar strafrechtliche Konsequenzen nach sich ziehen. Belangt wird allerdings meist nicht der Nutzer solcher Sites, sondern häufiger derjenige, der die Dateien ins Internet stellt und anderen zugänglich macht. Dabei ist übrigens egal, wo die Site produziert wird: So wurde Torrent.to kürzlich durch ein deutsches Gericht aus dem Netz genommen, obwohl die Betreiber der Site ebenso wie der Provider im Ausland sitzen. Der Grund war, dass sich die Site vor allem an deutsche Anwender richte. Es erschien daher gerechtfertigt, sie über Landesgrenzen hinweg abzuschalten.

Doch die Industrie hatte nur kurz Zeit, durchzuatmen: Innerhalb weniger Wochen hatten die Betreiber neue Server ans Netz gebracht – wo sie stehen, ist derzeit unklar.

Betreiber bleiben oft unerkannt: Wer hinter solchen Sites steckt, ist übrigens in nahezu allen Fällen ebenfalls nur schwer bis

HIER LESEN SIE ...

- **warum** Sie im Internet praktisch alles herunterladen können, das aber nicht tun sollten
- **wie** Sie sich davor schützen, mit Spam-Mails bombardiert zu werden
- **wo** es nahezu jedes Musikstück zum Download gibt
- **wo** Sie hingehen können, wenn Sie die letzte Folge Ihrer Lieblingsserie verpasst haben

Foto: getty images / Mike Kemp / Rubberball Productions

50 GEFÄHRLICHE SITES Das haben wir geprüft

Breite des Angebots

Wir haben uns auf den gefährlichen Websites angesehen, wie umfangreich das jeweilige Angebot ist.

Dubiose Angebote

Darunter fassen wir sowohl illegale Angebote als auch Fallen, etwa Links auf Abzock-Seiten. Je mehr davon sich auf einer Site finden, desto mehr Achtung-Zeichen haben wir vergeben (maximal fünf), und desto misstrauischer müssen Anwender auf einer solchen Site sein.

Infektionsrisiko

Das Herunterladen unbekannter Dateien ist immer mit einem Risiko verbunden – schließlich wissen Sie nicht, ob man Ihnen Spyware oder Viren unterjubeln will. Doch auch auf der Site selbst können Gefahren lauern. Auch hier gibt es zwischen einem und fünf Achtung-Zeichen.

gar nicht herauszubekommen. Zwar müssen bei den gängigen Top-Level-Domains wie .de, .net, .com oder anderen die Betreiber als Verantwortliche in einem Verzeichnis geführt werden. Im Fall der gefährlichen Websites stehen hier aber oft nur die Namen von Strohmännern oder Firmen, die im Auftrag des Betreibers handeln.

Die Betreiber zwielichtiger Sites versuchen oft, Anwender abzuzocken. Das geht beispielsweise über Spyware, die den Rechner ausspioniert und auch protokollieren kann, welche Daten Sie beim Internet-Banking eintippen. Ein anderer Trick sind Abzock-Abos. Wir haben mehrfach erlebt, dass Sites ein Update nachinstallieren wollten, etwa für Flash-Player oder Acrobat Reader. Statt zum Software-Hersteller wurden die Anwender aber auf Bezahldienste umgeleitet, wo sie erst einmal ihre Adresse angeben sollten und bei dieser Gelegenheit unbemerkt ein Download-Abo abschlossen. Kostenpunkt: zwischen 100 und 200 Euro, je nach Vertragsgestaltung.

Ebenfalls unter „Abzocke“ zu verbuchen sind Sites wie *http://oneload.org*. Hier wird zwar vor der Anmeldung in großen Buchstaben der Zugang zu Spielen, MP3s, Filmen und Programmen versprochen. Der Slogan lautet „Downloaden bis der Arzt kommt“. Der kommt allerdings höchstens, um den Anwender vor Verzweiflung und Langeweile zu retten. Denn bei näherem Hinsehen erfährt der Kunde, was er hier nur bekommen wird: „Alles zum Thema Filesharing: Anleitungen, Programme, Tools“ – nicht aber die eigentlichen Inhalte, nach denen er höchstwahrscheinlich sucht. Dort taucht auch der wirkliche Name des Dienstes auf: P2P Heute (*www.p2p-heute.com*) – ein Dienst, der schon mehrfach Gegenstand von Rechtsstreitigkeiten und Beschwerden der Verbraucherzentralen war.

Usenet: Legale und illegale Inhalte In Nachrichtengruppen

Etwas anders sieht es etwa bei *www.alphaload.de*, *www.usenext.de* und *www.firstload.de* aus. Hierbei handelt es sich um Zugänge zum Usenet, wo in Nachrichtengruppen überwiegend legale Downloads, aber auch illegale Inhalte aus dem Audio-, Video- und Software-Bereich zu finden sind.

Allerdings ist diese Quelle illegaler Inhalte auch nicht weniger gefährlich als andere. Anwender hinterlassen sogar noch eine weitere Spur in Form ihrer Kreditkarten- oder Kontodaten, da ein Bezahlvorgang stattfindet. Das gilt natürlich auch für andere Dienste, für die der Nutzer bezahlt. Beispielsweise stellen Ermittlungsbehörden bei der Schließung solcher Dienste immer wieder auch Datenbanken mit Nutzerdaten sicher. Hier finden sich dann nicht nur die Zugangsdaten, sondern auch gegebenenfalls Postadressen und Bankverbindungen.

Bei den Sites, die wir Ihnen vorstellen, müssen Sie in der Regel für die Benutzung kein Geld bezahlen und sich auch nicht anmelden. Eine Ausnahme bilden lediglich die Musik-Download-Dienste wie *http://mp3fiesta.com* oder *www.mp3sparks.com* (siehe Tabelle auf Seite 86). Downloads bei diesen Diensten kosten Geld. Laut Anbieter sind sie dafür legal: Die Betreiber führen angeblich Gebühren an eine Verwertungsgesellschaft im Ausland ab. Das sehen die Anwälte der Musikindustrie allerdings anders. Strittig ist auch, ob sich hier nur der Anbieter strafbar macht oder auch derjenige, der Tracks herunterlädt. Die deutschen Gerichte haben hierzu bislang keine Klarheit geschaffen. ›

GLOSSAR Gefährliche Websites

Rund um illegale Downloads gibt es einige Abkürzungen und Begriffe, auf die Sie in den Tiefen des Internets stoßen können.

Bit Torrent (BT): Darunter versteht man ein Filesharing-Protokoll, das sich für die schnelle Verbreitung großer Datenmengen eignet. Um es zu nutzen, benötigt man einen Bit-Torrent-Client (Infos unter *www.bittorrent-faq.de*).

Clickhosting-Dienst, auch Sharehoster oder Filehoster: Hier lassen sich ohne vorherige Anmeldung unkompliziert Dateien und Archive ablegen und von anderen Anwendern herunterladen. Diese Dienste wie *www.rapidshare.com*, *http://megaupload.com/de* oder *www.shareplace.com* finanzieren sich meist durch kostenpflichtige Premium-Versionen, die etwa schnelleren Download und größere Datei-Uploads bieten.

Direkt-Downloads (DDL): Hier finden Sie – oft aufgeteilt in mehrere kleine gepackte Dateien – Downloads, die Sie von einem Clickhosting-Dienst herunterladen können.

Keys: Seriennummern, die das Installieren und Freischalten einer Software ermöglichen. Entweder handelt es sich dabei um Seriennummern von Anwendern, die die Software legal erworben haben, oder um künstliche, mit Hilfe eines Key-Generators erstellte Lizenzen.

Usenet: Sammelbegriff für Nachrichtengruppen, die mit Hilfe eines Newsreaders gelesen werden können. In diesen Nachrichten lassen sich auch Teile von Dateien unterbringen, die zusammengefasst eine Software, eine Musik- oder Filmdatei ergeben können.

Warez: Sammelbegriff für illegal verbreitete Software, die meist über das Internet in Umlauf gebracht wird. Analog dazu werden illegal verbreitete Seriennummern als Serialz bezeichnet. Programme, die illegalerweise den Kopierschutz einer Software aushebeln, heißen Crackz.

Spam ausgesperrt: Eine anonyme Mailadresse vermeidet Werbemüll

www.10minutemail.com

Wegwerf-Mailadressen, die Spam verhindern

Breite des Angebots	**groß**
Dubiose Angebote	⚠ ⚠
Infektionsrisiko	⚠

Wer seine Mailadresse verheimlichen will, kann auf 10minutemail setzen. Der Dienst generiert per Knopfdruck eine temporäre Adresse, mit der Sie sich bei einem Dienst anmelden können, dem Sie Ihre Kontaktdaten nicht anvertrauen möchten. Allerdings könnte der Betreiber Ihre IP-Adresse protokollieren. Der Gratis-Dienst überzeugt durch einfache Bedienung und enthält fast keine Werbung.

Nadel im Heuhaufen: Alt.binaries.nl sucht gezielt nach Binary-Gruppen

http://alt.binaries.nl

Suchmaschine für Binary-Gruppen im Usenet

Breite des Angebots	**groß**
Dubiose Angebote	⚠ ⚠
Infektionsrisiko	⚠

Eine beliebte Quelle für Downloads aller Art ist immer noch das Usenet. Suchmaschinen wie *http://groups.google.com* blenden allerdings Nachrichtengruppen aus, in denen Software, Filme und Musik zu finden sind, also Binary-Gruppen. Bei Alt.binaries.nl finden Sie diese Inhalte übersichtlich und ganz ohne Werbung. Zu jeder Fundstelle gibt es eine NZB-Datei als Download-Hilfe.

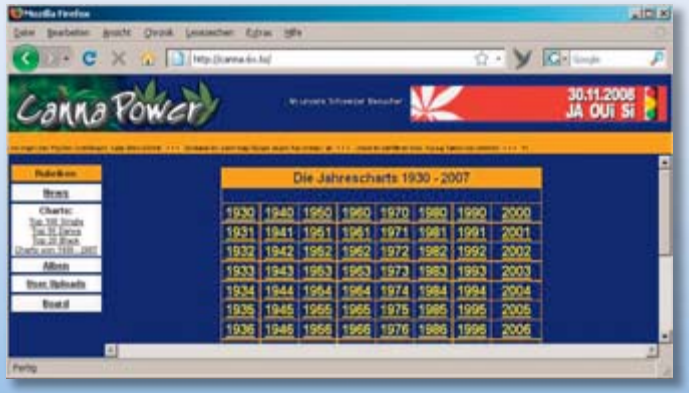
Unkompliziert: Bug Me Not liefert Zugangsdaten für beliebte Sites

www.bugmenot.com

Passwörter für zugangsgeschützte Websites

Breite des Angebots	**gering**
Dubiose Angebote	⚠ ⚠ ⚠ ⚠
Infektionsrisiko	⚠ ⚠ ⚠ ⚠

Jeder hat eine Vielzahl von Passwörtern – auch für Sites, bei denen man gar nichts so Privates tut, als dass ein Passwort gerechtfertigt wäre. Bug Me Not bietet Zugänge zu anmeldepflichtigen Websites aller Art. Allerdings wird der Site Ihr hoher Bekanntheitsgrad zum Verhängnis: Viele Passwörter werden bald, nachdem sie dort auftauchen, von den Betreibern der jeweiligen Sites gesperrt.



Top-Musik: Bei Canna gibt's die deutsche Verkaufshitparade seit 1930

www.canna.6x.to

Großes Musikarchiv mit Einzeltiteln

Breite des Angebots	**groß**
Dubiose Angebote	⚠ ⚠
Infektionsrisiko	⚠ ⚠

Da hat sich jemand richtig Arbeit gemacht: Die deutschen Top 100 eines jeden Jahres seit 1970 sowie Teile aus älteren Hitparaden zurück bis 1930 finden Sie bei Canna. Die Dateien liegen im MP3-Format in unterschiedlicher Qualität als Direkt-Download vor. Außerdem gibt's noch die aktuellen Single-Charts, spezielle Hitparaden wie Dance-Charts sowie einige aktuelle Alben.

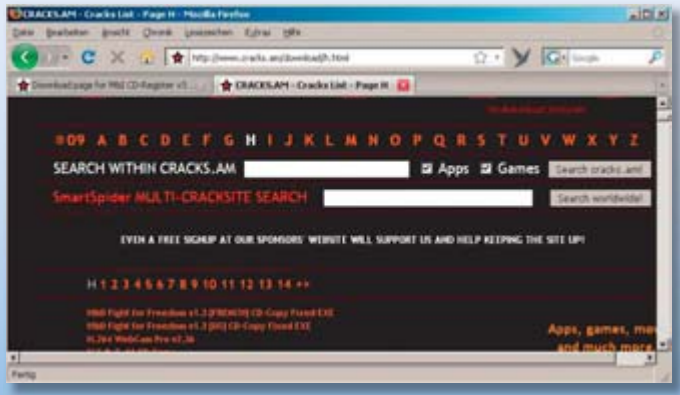
Unwegsam: Charts4you schickt den Besucher in einen Werbedschungel

www.charts4you.org

Musikdateien, Filme und Software per Direkt-Download

Breite des Angebots	**gering**
Dubiose Angebote	⚠ ⚠ ⚠ ⚠ ⚠
Infektionsrisiko	⚠ ⚠ ⚠ ⚠

Rund 2,5 Terabyte Musikalben, Filme, Software und Spiele – alles per Direkt-Download über Clickhoster wie Rapidshare – bietet Charts4you. Allerdings ist der Weg zu den Downloads wegen der vielen Werbung sehr mühsam. Die Qualität der angebotenen Dateien ist gut, und fast alle Dateien sind auch erreichbar. Allerdings handelt es sich beim Gros der Downloads um illegales Material.



Riskant: Viren und Spyware machen Anwendern das Leben schwer

www.cracks.am

Seriennummern, Freischaltcodes und Software-Patches

Breite des Angebots	**groß**
Dubiose Angebote	⚠ ⚠ ⚠ ⚠ ⚠
Infektionsrisiko	⚠ ⚠ ⚠ ⚠

Alles, was man braucht, um Software freizuschalten, findet sich auf dieser Site: Aktivierungscodes, Seriennummern oder Patches, die eine Aktivierung oder eine Seriennummernabfrage umgehen. Dabei gilt: Man hinterlässt seine IP-Adresse und kann somit zur Rechenschaft gezogen werden. Wer dann keine Lizenz der entsprechenden Anwendung nachweisen kann, kommt in Erklärungsnot.

MP3-Downloads: Hier findet man vor allem die aktuellen Charts

www.emp3world.com

MP3-Hits als kostenloser Direkt-Download

Breite des Angebots	**sehr groß**
Dubiose Angebote	⚠ ⚠ ⚠ ⚠
Infektionsrisiko	⚠ ⚠ ⚠

Vor allem für den hitparadenorientierten Musikgeschmack eignet sich Emp3world. Das Portal bietet Direkt-Downloads in 128 oder 192 KBit/s und stellt die gefragtesten Dateien in einer Liste dar. Der Download geht schnell und unkompliziert – keine Weiterleitung auf andere Dienste, keine Eingabe von Kontrollzeichenketten. Einige der zahlreichen Banner führten auf Spyware-Sites.

Informationsquelle: Bei Gulli steht alles Neue aus der Warez-Szene

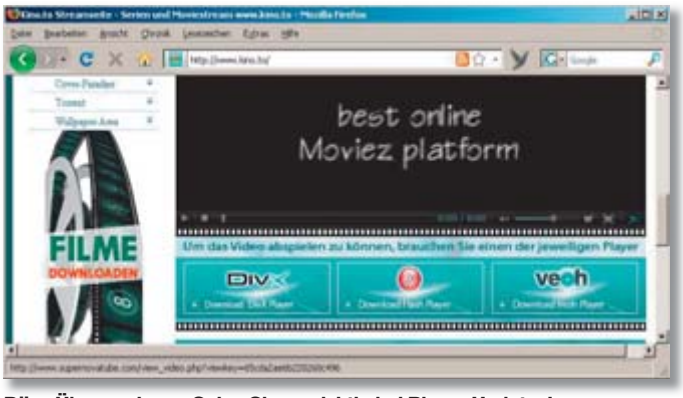
www.gulli.com

Nachrichtenportal und Forum zu Warez und Filesharing

Breite des Angebots	**groß**
Dubiose Angebote	⚠ ⚠ ⚠ ⚠
Infektionsrisiko	⚠

Gulli ist ein Nachrichtenportal, das über Themen wie Downloads, Filesharing und Hacking informiert. Die Site besteht seit über 10 Jahren und ist eine der umfangreichsten Quellen im deutschsprachigen Raum. Im Forum tauschen Anwender Tipps und Tricks aus, Man kann sich gefahrlos informieren, gefährlich ist das Schreiben von Nachrichten (möglicherweise Beihilfe zu Straftat).

›



Böse Überraschung: Seien Sie vorsichtig bei Player-Updates!

www.kino.to

Filme und Fernsehserien als Stream

Breite des Angebots	**gering**
Dubiose Angebote	⚠ ⚠ ⚠
Infektionsrisiko	⚠ ⚠ ⚠

Nicht immer will man einen Film archivieren. Wem es reicht, den Stream auf dem PC-Bildschirm anzuschauen, der ist bei Kino.to richtig. Hier gibt es ausgesuchte Filme als Divx- oder Flash-Stream. Achtung: Falls Ihr Player nicht aktuell ist, updaten Sie nicht über die vorgeschlagene Site *www.mega-downloads.net*. Dort schließen Sie sonst ein wertloses Download-Abo für jährlich 96 Euro ab.

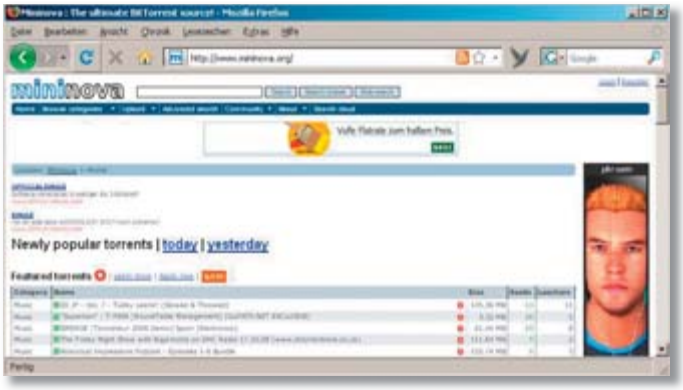
Das passende Deckblatt: Die Datenbank enthält knapp 3 Millionen Cover

http://mega-search.net

Suchmaschine für Cover von CDs, Videos und Spielen

Breite des Angebots	**groß**
Dubiose Angebote	⚠ ⚠
Infektionsrisiko	⚠

Bei Megasearch lagern Cover von Audio-CDs, Videos und Spielen zum Ausdrucken. Die Metasuchmaschine kennt und durchsucht 450 Cover-Datenbanken. Der Störfaktor Werbung schwankt je nach Quelle. Die hohe Zahl von knapp 3 Millionen Dateien kommt durch doppelte Einträge zustande. Außerdem sind Frontcover und Booklet meist als mehrere Dateien abgelegt.



Umfangreich: Bei Mininova gibt's Torrent-Dateien zu vielen Downloads

www.mininova.org

Bit-Torrent-Suchmaschine

Breite des Angebots	**sehr groß**
Dubiose Angebote	⚠ ⚠ ⚠ ⚠
Infektionsrisiko	⚠ ⚠

Es gibt eine Vielzahl von Sites, auf denen man nach Bit-Torrent-Dateien suchen kann. Ein besonders umfangreiches und einfach zu bedienendes Angebot ist Mininova. Die Downloads sind nach Kategorien aufgeschlüsselt: Von Musik über Filme und Software bis hin zu E-Books und Mangas ist alles vertreten. Der Schwerpunkt liegt auf englischsprachigen Inhalten.

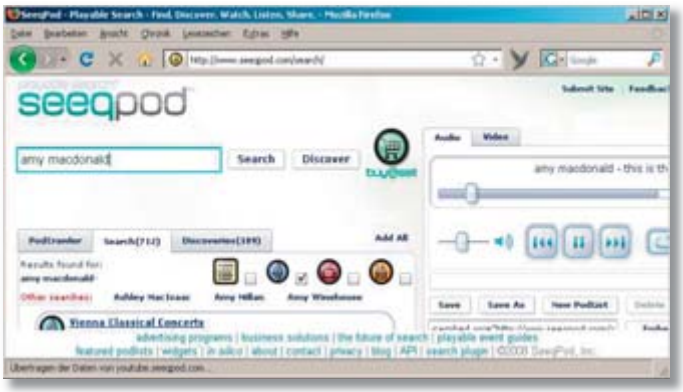
Von Spiegel bis Chip: Download von aktuellen Zeitschriften als illegale PDFs

www.pressefreiheit.ws

Zeitschriften-PDFs als kostenloser Download

Breite des Angebots	**groß**
Dubiose Angebote	⚠ ⚠ ⚠ ⚠ ⚠
Infektionsrisiko	⚠ ⚠ ⚠ ⚠

Viele deutschsprachige Zeitschriften – von Spiegel über Focus bis zu Chip und PC-WELT – finden sich auf dieser Site als illegale Gratis-PDFs. Die Dateien werden eingescannt oder stammen aus den Premium-Shops der Verlage. Ein Schad-Script auf der Site fordert den Anwender auf, seinen Adobe Reader zu aktualisieren. Wer darauf klickt, landet auf einer Site mit Bezahl-Downloads.



Jukebox: Seeqpod spielt Musik-Streams ab und bettet sie in Websites ein

www.seeqpod.com

Großes Musikarchiv mit Einzeltiteln

Breite des Angebots	**groß**
Dubiose Angebote	⚠ ⚠
Infektionsrisiko	⚠ ⚠

Seeqpod greift auf Musik-Sites im Internet zu und spielt diese Titel in einem eigenen Player im Browser ab. Der Anwender stellt sich sein Musikprogramm einfach über die Suchfunktion zusammen und verschiebt die Tracks nach rechts in die Abspielliste. In unseren Tests waren nicht alle Tracks abspielbar. Über eine zusätzliche Recording-Software lassen sich die Titel aufzeichnen.

Für TV-Junkies: Hier finden sich deutschsprachige Folgen von Serien

www.serienfreaks.to

Folgen von TV-Serien und -Shows per Direkt-Download

Breite des Angebots	**groß**
Dubiose Angebote	⚠ ⚠ ⚠
Infektionsrisiko	⚠ ⚠

Serienfreaks ist eine deutsche Community, die Folgen von Fernsehserien per Direkt-Download ins Netz stellt, aber auch Dokumentationen sowie Fernsehshows anbietet. Etwas irreführend ist die Werbung für „kostenlose Usenet-Downloads“ – hierbei handelt es sich um den Bezahldienst Alphaload. Lange Zeit war die Site unter Serienfreaks.tv zu erreichen, die Domain wurde aber entwendet.

Polizei-Aktion: 2006 wurde der Server geschlossen – jetzt ist er wieder da

www.thepiratebay.org

Umfangreichstes Bit-Torrent-Angebot der Welt

Breite des Angebots	**sehr groß**
Dubiose Angebote	⚠ ⚠ ⚠ ⚠ ⚠
Infektionsrisiko	⚠ ⚠ ⚠ ⚠

The Piratebay (TPB) wird von einer schwedischen Gruppe betrieben und ist die wohl umfangreichste und bekannteste Quelle für Torrent-Downloads aller Art. Bei TPB finden sich viele aktuelle Filme, Musikdateien und Programme. Die meisten Dateien sind gut dokumentiert. Berühmtheit erlangte die Site 2006, als die schwedische Polizei die Server vorübergehend beschlagnahmte.

Musik & Co.: Sehr umfangreiche Quelle für deutschsprachige Torrents

www.torrent.to

Torrent-Downloads von Musikdateien, Filmen und Software

Breite des Angebots	**sehr groß**
Dubiose Angebote	⚠ ⚠ ⚠ ⚠ ⚠
Infektionsrisiko	⚠ ⚠ ⚠ ⚠

Bei Torrent.to gibt es ein umfassendes Angebot aktueller Bit-Torrent-Dateien zu Software, Musikalben, Filmen und Fernsehsendungen. Der Anteil an illegalen und dubiosen Angeboten ist hoch. Daher wurde das Angebot bereits mehrfach mit juristischen Mitteln vom Netz genommen. Die Betreiber haben aber immer wieder neue Provider im Ausland gefunden. Die Site ist recht werbelastig.

› IM ÜBERBLICK 50 gefährliche Websites

Internet-Adresse	Inhalt des Angebots	Breite des Angebots	Dubiose Angebote	Infektionsrisiko	Sprache	Bemerkungen
www.10minutemail.com	Wegwerf-Mailadressen	groß	▲▲	▲	Deutsch	wechselt in regelmäßigen Abständen die Domain
http://allseek.info	Cracks, Seriennummern, Freischalt-Patches	groß	▲▲▲▲▲	▲▲▲▲	Englisch	sehr umfangreiches Angebot
http://alt.binaries.nl	Suchmaschine für Binaries-Newsgroup	groß	▲▲	▲	Englisch	durchsucht über 2200 Newsgroups
www.astalavista.com	Klassiker unter den Cracks- und Serials-Sites	gering	▲▲▲▲▲	▲▲▲▲	Englisch	viel störende Werbung und mittelmäßige Inhalte
www.binsearch.info	Suchmaschine für Binaries-Newsgroup	groß	▲▲	▲	Englisch	durchsucht gezielt die populärsten Gruppen
www.bitreactor.to	Torrents zu Filmen, Musik, Software, Spielen	groß	▲▲▲▲	▲▲▲▲	Deutsch	Gratis-Torrents und kostenpflichtige (Usenet-)Downloads
www.bugmenot.com	Passwörter zu vielen Websites	gering	▲▲▲▲	▲▲▲▲	Englisch	Bewertungssystem der Passwörter
http://canna.6x.to	Deutsche Top-100-Charts-Musik seit 1930, Musikalben	sehr groß	▲▲▲▲▲	▲▲▲▲	Deutsch	Download über Clickhoster
www.charts4you.org	Musik, Filme, Programme per Clickhoster	gering	▲▲▲▲▲	▲▲▲▲	Deutsch	extrem nervende umfangreiche Werbung
http://collectr.net	Suchmaschine für Videos, Musik, Software und Spiele	gering	▲▲▲▲	▲▲▲▲	Deutsch	Downloads teilweise defekt oder veraltet
www.crackfind.com	Cracks, Seriennummern, Freischalt-Patches	groß	▲▲▲▲▲	▲▲▲▲	Englisch	auch Downloads und Torrents
http://cracks.am/	Cracks, Seriennummern, Freischalt-Patches	groß	▲▲▲▲▲	▲▲▲▲	Englisch	viel nervende Werbung
http://ddl-search.biz	Direkte Downloads: Filme, Musik, Software, Spiele	gering	▲▲▲▲	▲▲▲▲	Deutsch	ausschließlich Links, viele nicht mehr funktionierend
www.dreamworld.vg/ulc/index.php?directory=Keys	Upload-Center für TV- und Sat-Receiver	groß	▲▲▲▲	▲▲▲▲	Deutsch	auch Inhalte, die Verschlüsselung aufheben
www.ebookdatenbank.info	Sammlung deutschsprachiger E-Books und Zeitschriften	gering	▲▲▲▲	▲▲	Deutsch	wird nicht mehr aktualisiert
www.emp3world.com	MP3-Portal mit aktuellem Angebot	sehr groß	▲▲▲▲	▲▲▲	Englisch	Download mit „Speichern unter“, enthält Spyware
www.gamecopyworld.com	Datenbank zum Erstellen von Kopien von Computerspielen	gering	▲▲▲▲	▲▲▲	Englisch	auch Tutorials und Cracks
www.gsm-free.com	Informationen zu Handy-Hacking, Software für Handys	gering	▲▲▲	▲▲▲▲	Deutsch	umfangreiches Forum
www.gulli.com	Foren und Nachrichten zu Hacking, Downloads, Filesharing	groß	▲▲▲▲	▲	Deutsch	sehr umfangreich und aktuell
www.hoerbuch.in	Hörbücher zum Download	gering	▲▲▲▲	▲▲▲	Deutsch	Downloads per Clickhoster
www.house-of-usenet.org/	ausführliches Forum zum Thema Usenet und Downloads	groß	▲▲▲	▲	Englisch	Anmeldung erforderlich
http://isohunt.com	Bit-Torrent-Suchmaschine	gering	▲▲▲	▲▲	Englisch	nicht nur für ISO-Dateien
http://kino.to	Filme als Streaming-Dateien anschauen	gering	▲▲▲	▲▲▲▲	Deutsch	aktueller Browser und aktueller Player erforderlich
www.lm.x2.to/	Musik, Filme, Programme per Clickhoster	gering	▲▲▲▲	▲▲▲	Deutsch	mit Top-Listen der beliebtesten Downloads
http://mega-search.net	CD-Cover-Suchmaschine	groß	▲▲	▲	Deutsch	knapp 3 Millionen CD-Cover verfügbar
www.mininova.org	Bit-Torrent-Suchmaschine	sehr groß	▲▲▲▲	▲▲	Englisch	auch als RSS-Feeds verfügbar
http://moviez.to/ddl	Musik, Filme, TV-Serien und Software	groß	▲▲▲▲	▲▲▲▲	Deutsch	mit Forum
http://mp3fiesta.com	kostenpflichtige Musik-Downloads	sehr groß	▲▲▲	▲▲▲	Englisch	Bezahlung in australischen Dollar
www.mp3sparks.com	kostenpflichtige Musik-Downloads	sehr groß	▲▲▲	▲▲▲	Englisch	Nachfolger von Allofmp3
http://mp3db.ru	Musikalben zum Download	groß	▲▲▲	▲▲▲	Englisch	auch ausgefallene Musik
www.mybittorrent.com	Bit-Torrent-Suchmaschine	groß	▲▲▲	▲▲	Deutsch	übersichtlich, mit Qualitäts-Rating
www.omemo.com	Anonymes Dateihosting	groß	▲▲▲	▲	Englisch	verschlüsselte dezentrale Datei-Ablage
www.passwordoutlet.com	Passwörter zu Websites (Hacking, Filme und mehr)	gering	▲▲▲▲	▲▲▲▲▲	Englisch	unübersichtlich und viel Werbung
www.pressefreiheit.ws	aktuelle Zeitschriften als PDF-Download	groß	▲▲▲▲▲	▲▲▲▲	Deutsch	ausschließlich deutschsprachig, sehr aktuell
http://saugstube.to	Emule- und Torrent-Downloads aller Art	groß	▲▲▲▲	▲▲▲▲	Deutsch	ziemlich viel Werbung
www.seeqpod.com	Musiksuchmaschine	groß	▲▲	▲▲	Englisch	Tracks lassen sich in eigene Site einbetten
http://serienfreaks.to	Fernsehserien zum Download	groß	▲▲▲	▲▲▲	Deutsch	Downloads per Rapidshare & Co.
www.slyck.com	umfassende Infos zu Filesharing und Warez	groß	▲▲▲▲	▲▲	Englisch	gute Anleitungen („Guides“)
www.speckly.com	Bit-Torrent-Suchmaschine	gering	▲▲▲	▲	Englisch	auch Ausschluss einzelner Begriffe möglich
www.stream-collector.com	Filme und TV-Serien als Stream anschauen	gering	▲▲▲	▲▲▲	Deutsch	Download über Mitschnitt möglich
www.superlux.mirrorz.com	Forum für Sat-Empfang	groß	▲▲▲	▲▲▲	Englisch	Freischaltung verschlüsselter Inhalte möglich
www.thebugs.ws	Datenbank für Cracks und Serials	sehr groß	▲▲▲▲▲	▲▲▲▲	Englisch	teilweise Spyware
http://thepiratebay.org	Torrents zu Filmen, Musik, Software und Spielen	sehr groß	▲▲▲▲▲	▲▲▲▲	Deutsch	extrem umfangreich, unaufdringliche Werbung
www.torrent.to	Torrents zu Filmen, Musik, Software und Spielen	sehr groß	▲▲▲▲▲	▲▲▲▲	Deutsch	umfangreiches aktuelles Angebot
www.torrentazos.com	Torrents zu Filmen, Musik, Software und Spielen	groß	▲▲▲	▲▲	Spanisch	vor allem englischsprachige Inhalte
www.torrentfly.org	Bit-Torrent-Suchmaschine	groß	▲▲▲	▲▲	Englisch	völlig werbefrei, mit Liste der beliebtesten Suchbegriffe
www.torrentz.com	Bit-Torrent-Suchmaschine	sehr groß	▲▲▲	▲▲	Englisch	sehr übersichtlich und werbefrei
www.ubb-torrent.to	Torrents zu Filmen, Musik, Software und Spielen	gering	▲▲▲▲	▲▲▲▲	Deutsch	Registrierung notwendig, um alle Funktionen zu nutzen
http://woom.ws	Suchmaschine für Videos, Musik, Software und Spiele	groß	▲▲▲▲	▲▲▲▲	Deutsch	ausschließlich Direkt-Downloads von Clickhostern
www.wslabi.com	Versteigerung von gehackter Software	groß	▲▲▲▲	▲▲▲▲	Englisch	Programmierer finden so Software-Schwachstellen

Was Sie im Internet niemals tun sollten

Die sieben Todsünden beim Surfen

Es gibt eine Vielzahl von Gefahren im Internet. Doch wenn Sie ein paar elementare Regeln beachten, ist es nicht weiter schwer, Fallstricken aus dem Weg zu gehen.

Von **Tobias Weidemann**

Gefahren lauern überall – man muss sie rechtzeitig erkennen. Das gilt für berüchtigte Ecken in Großstädten genauso wie für das Internet. Während Ihnen auf dem Wochenendtrip Ihr Reiseführer rät, was Sie besser tun und was Sie besser lassen sollten, ist das im Netz weniger einfach. Manche Abzock-Site tarnt sich hinter einem Routenplaner, und gar nicht so selten kommt ein Trojaner erst dadurch auf den PC, weil Sie einer Site vertraut haben, die vor einer Sicherheitslücke warnt.

Auch wer umsichtig und von Sicherheits-Software geschützt duchs Internet surft, kann sich Probleme einhandeln. Und es gibt Situationen, in denen Sie nur geringe Chancen haben, unbeschadet davonzukommen.

Wir stellen sieben gravierende Fehler vor, die Sie im Internet machen können, und geben Tipps, wie Sie sie vermeiden. Denn wenn Sie eine dieser Todsünden begehen, haben Sie eine Menge Ärger am Hals.

1. Todsünde: Sie surfen auf Sites mit aggressiver Werbung

Manche Websites erschlagen einen geradezu mit animierter Werbung, kaum dass die Internet-Seite aufgerufen ist. Viele Fenster öffnen sich, ein Pop-up für Gratis-SMS hier, ein Sex-Banner dort, Abstimmungen und Rankings drängen sich vor, und die gesuchte Information ist kaum zu finden. Auf solchen Sites müssen Sie besondere Vorsicht walten lassen. Ganz schnell klickt man hier einmal daneben – und ruft im schlimmsten Fall eine Site mit Schad-Software auf.

Eine tückische Variante sind Links, die als gelb unterlegte Hinweise im Fenster der aufgerufenen Site wie Fehlermeldungen des Browsers aussehen. Die Einblendungen wollen Ihnen weismachen, dass sie Systemhinweise Ihres PCs sind. Tatsächlich würden Sie auch hier eine Werbeseite aufrufen. **Tipp:** Führen Sie – zunächst ohne zu klicken – die Maus auf eine solche Meldung, und sehen Sie in der Fußzeile des Browsers nach. Hier erscheint die URL der Seite, die aufgerufen werden würde. Anhand dieser Information können Sie leichter entscheiden, ob Sie dorthin geführt werden wollen. **Achtung:** Gefährlich sind Sites, die den Unterschied zwischen Werbung und gesuchten Inhalten verschleiern wollen – so etwa auf *www.kino.to*: Abgesehen davon, dass beim Aufrufen der Site eine fingierte Virenwarnung aufpoppt und beim Abspielen eines Films der zuvor beschriebene gelb unterlegte Hinweis als vorgetäuschte Warnung erscheint, werden Ihnen Software-Player vorgeschlagen. Ein Klick auf die entsprehenden Buttons, die meist nicht als Werbung erkennbar sind, führt zu einer Bezahl-Site, auf der Sie die Abspiel-Software herunterladen können – und nebenbei ein Abo mit 60 Euro Jahresbeitrag abschließen (*www.99downloads.de*).

HIER LESEN SIE ...

- **warum** Sie nicht alles, was Sie herunterladen können, auch herunterladen dürfen
- **warum** Sie Virenwarnungen manchmal getrost ignorieren können
- **welche** Bezahlmöglichkeiten im Internet mit Vorsicht zu genießen sind und wie Sie sich Klarheit verschaffen
- **wen** Ihre Adresse etwas angeht und wen nicht
- **welche** Angebote Sie besonders kritisch prüfen sollten

Foto: Yang MingQi - Fotolia.com

Werbegewitter: Meiden Sie Sites, die Sie mit Werbung, fiktiven Gefahrenmeldungen und Täuschungsmanövern bombardieren

Tagesaktuelle Betrugsfälle: Bei Escrow Fraud finden Sie eine Datenbank mit mehr als 8000 betrügerischen Websites

2. Todsünde: Sie nutzen Download-links von zwielichtigen Sites

Es scheint einfach zu sein: Datei anklicken und herunterladen – per Filesharing-System oder per Direkt-Download über Rapidshare & Co. Doch es kommt vor, dass statt der kostenlosen Freischaltmöglichkeit für Bezahl-Software ein Trojaner auf der Festplatte landet. Wir haben das mit einem Key-Generator für eine teure Grafik-Software ausprobiert: Von den zehn Dateien, die wir fanden, waren nur drei virenfrei. Und nur eine hätte die Grafik-Software (illegal) freigeschaltet. Schädlingsquote: 90 Prozent!

Um zu signalisieren, dass die angebotenen Programme legal und schädlingsfrei sind, gehen immer mehr Sites dazu über, die Downloads von ihren Anwendern bewerten zu lassen oder ein Trusted-Symbol an vertrauenswürdige User zu vergeben, die Daten zum Download zur Verfügung stellen. Aber auch hier ist Manipulation möglich.

Vorsicht bei Warnmeldungen: Gefährlich sind Sites wie *http://adwarestriker.com* oder *http://spystriker.com*, die Ihnen vorgaukeln, Ihr PC hätte eine Schwachstelle, und Ihnen als Sofortmaßnahme einen Patch oder eine Sicherheits-Software aufdrängen. Tools, die Sie hier erhalten, sind nicht nur kostenpflichtig, sondern bestenfalls nutzlos – im schlechtesten Fall schädlich. Verlassen Sie sich grundsätzlich nur auf Sicherheits-Tools, die seriöse Quellen wie PC-WELT Ihnen empfehlen.

Tipp: Dateien, bei denen Sie nicht sicher sind, ob sie gefährlichen Code enthalten, können Sie zunächst innerhalb einer virtuellen Umgebung (etwa eines Vmware-Systems) aufrufen. Schließen Sie aber an ein solches virtuelles System keine externen Laufwerke (wie USB-Sticks oder externe Festplatten) an, auf die Zugriffe gestattet wären. Verzichten Sie außerdem auf freigegebene Netzlaufwerke und Ordner.

3. Todsünde: Sie geben persönliche Daten auf dubiosen Sites preis

Auf seriösen Sites ist nichts dagegen einzuwenden, persönliche Daten anzugeben – diese dienen im besten Fall nur der Kundenbindung und ermöglichen dem Anbieter eines Dienstes, Ihnen Zusatzinformationen zukommen zu lassen. Prüfen Sie, in welcher Form Ihre Daten verwendet werden. Selbst wenn in den AGB steht, dass nur „Partnerunternehmen“ sie nutzen dürfen, sollten Sie vorsichtig sein. Am sichersten ist es, wenn das Unternehmen Ihre Daten nicht zu Werbe- oder Kundenbindungszwecken nutzt oder dies nur in Zusammenhang mit Ihrem konkreten Anliegen oder Auftrag tut.

Unseriöse Web-Seiten, die etwa bei ihren Download-Offerten ungeniert gegen das Urheberrecht verstoßen, werden keine Skrupel haben, Nutzerdaten zu missbrauchen. Sie müssen also davon ausgehen, dass Ihre Daten weitergegeben werden.

Tipp: Als Faustregel sollten Sie sich fragen, ob der Anbieter überhaupt einen sinnvollen Grund hat, Ihre Adresse oder andere Daten von Ihnen zu erfahren.

Besondere Vorsicht gilt bei Bankdaten: Noch zurückhaltender sollten Sie mit Zahlungsinformationen wie Konto- und Kreditkartendaten sein. Im Internet kursieren Listen mit Bankverbindungen und dazugehörigen Namen. Mit den gestohlenen Daten melden sich Kriminelle bei kostenpflichtigen Diensten an.

Selbst wenn die Gebühr durch den rechtmäßigen Kontobesitzer nach einigen Tagen zurückgebucht und der erschlichene Account gelöscht wird, hatten die Betrüger für einige Zeit die Möglichkeit, den Service kostenlos zu nutzen. ›

So billig sie auch sein mögen: Es lohnt sich nicht, für Programme von dubiosen Download-Sites Geld auszugeben

Die Verbraucherzentrale warnt vor Abzocke

4. Todsünde: Sie vertrauen Sites, die gegen geltendes Recht verstoßen

„Was tun bei einer Hausdurchsuchung?“ ist der Titel eines populären E-Books, das seit Jahren im Internet zirkuliert. Ratsamer ist es jedoch, es gar nicht so weit kommen zu lassen. Und dazu gehört, sich von Websites fern zu halten, deren Geschäftsmodell darauf basiert, gegen geltendes Recht zu verstoßen – sei es in puncto Urheberrecht oder durch Anleitungen zu illegalen Handlungen.

Die Gerichte lassen bei offensichtlich rechtswidrigen Sachverhalten keinen rechtlichen Spielraum zu: Wird beispielsweise auf einer Website mit Kreditkartendaten oder Zugangscodes zu Bezahl-Websites gehandelt, dann ist das definitiv illegal – und Sie sollten keinesfalls auf solche Angebote eingehen, selbst wenn hierbei kein Geld fließt. Anders als bei weniger gravierenden Vergehen, bei denen manchmal keine Daten herausgegeben werden, ist es den Behörden hier möglich, auf die Internet-Provider zuzugehen und über die IP-Adressen die Daten von Anwendern anzufordern. Die Vorratsdatenspeicherung wurde für solche Ermittlungsverfahren geschaffen.

Übrigens: Auch wenn Sie Mail-Mahnschreiben von Firmen erhalten: Bei kleineren Vergehen wie einer Anmeldung mit falscher Identität müssen Sie nicht damit rechnen, dass Ermittlungsbehörden Ihre Daten beim Provider anfordern. Denn erstens bedarf es einer richterlichen Anordnung, um die Identität zu ermitteln, die zu einer IP-Adresse gehört, zum anderen muss hierfür ein „schwerwiegender Schaden“ entstanden sein. Eine einfache Anmeldung (etwa in einem Forum) reicht hierfür nicht aus.

5. Todsünde: Sie nutzen leichtfertig Bezahldienste und Treuhandservices

Im Zusammenhang mit Treuhanddiensten und Online-Bezahlverfahren gibt es vor allem zwei Gefahren:

Der Datenschutz eines Bezahldienstes wird missbraucht: Sie bezahlen etwa eine bei Ebay ersteigerte Ware über Western Union (*www.westernunion.de*) oder Moneygram (*www.moneygram.de*). Mit Hilfe einer Transaktionsnummer und eines vereinbarten Kennwortes kann sich der Empfänger bei diesen Diensten das Geld unbürokratisch in bar ausbezahlen lassen. Dabei wird seine Identität nicht dokumentiert. Wenn Sie nun beispielsweise die Ware nicht erhalten, lässt sich nicht verfolgen, an wen das Geld gegangen ist. Entsprechend betont etwa Western Union, dass ihr Geldtransferdienst nicht für Geschäfte zwischen Unbekannten vorgesehen und geeignet ist.

Der vorgeschlagene Dienst existiert nur kurzfristig oder nur zum Schein: Wenn ein Geschäftspartner den Geldtransfer ausschließlich über einen bestimmten Bezahldienst abwickeln will, sollten Sie misstrauisch werden. Gerade bei teuren Waren kommt es vor, dass ein angeblicher Kaufinteressent eine attraktive Summe bietet, die er über einen bestimmten Treuhanddienst bezahlen will. Doch an Ihr Geld kommen Sie nicht: Entweder ist der Dienst unerreichbar oder der Zugang (und damit das Einziehen des Betrags) funktioniert nicht mehr. Es gibt mittlerweile mehrere tausend obskure Online-Treuhanddienste.

Prüfen Sie deshalb immer als Erstes, ob der vorgeschlagene Dienst bekannt und seriös ist oder ob es bereits in der Vergangenheit etliche Beschwerden gab. Oft werden solche Geldtransfer-Unternehmen nämlich einzig und allein zu Betrugszwecken gegründet und nach kurzer Zeit wieder geschlossen. Eine tagesaktuelle Datenbank mit Screenshots zu allen Diensten finden Sie unter *http://escrow-fraud.com*.

Tipp: Die Abwicklung über einen seriösen Treuhandservice kann gerade bei hochwertigen Waren sinnvoll sein. Bei Ebay-Geschäften sollten Sie unbedingt den Ebay-Treuhandservice nutzen (*http://pages.ebay.de/treuhandservice*).

6. Todsünde: Sie gehen auf allzu verlockende Angebote ein

Im Internet kann jeder alles schreiben und versprechen. Für Sie als Kunde ist es später oft schwierig bis unmöglich, das Versprochene einzufordern. Seien Sie daher nicht zu schnäppchenorientiert, und verlassen Sie sich auf Ihren gesunden Menschenverstand. Vor allem, wenn Sie finanziell in Vorleistung treten müssen, ist Misstrauen angesagt.

Dies gilt beispielsweise für Mobilfunkverträge, bei denen Sie in mehreren Schritten oder zeitversetzt eine Kostenerstattung erhalten sollen. Der Anbieter verspricht bei Abschluss von zwei Verträgen über 24 Monate Laufzeit zum hochwertigen Mobilfunkgerät noch alle möglichen Beigaben, etwa eine Spielekonsole, ein Notebook oder einen MP3-Player. Unterm Strich sollen Ihnen keinerlei Zusatzkosten entstehen. Möglich wird das durch die hohe Provision, die der Provider an den dubiosen Händler zahlt und die dieser zur Begleichung der Grundgebühren sowie für seine Kundengeschenke nutzt. Das kann ins Auge gehen – wenn der Händler zahlungsunfähig wird.

Achtung Gutschein: Ein weiteres Beispiel für eine gewagte Vorauszahlung sind Internet-Auktionen, bei denen Sie Gutscheine für bestimmte Leistungen ersteigern, etwa für Wellness-Wochenenden, Flugreisen oder Hotelaufenthalte. Bis Sie den Gutschein nutzen, arbeiten die Unternehmen mit Ihrem Geld.

Prüfen Sie vor Ihrem Preisangebot die Seriosität des jeweiligen Unternehmens. Hat es, etwa bei Ebay, bereits eine lange Liste von Bewertungen, oder ist es relativ neu am Markt? Checken Sie den Leistungsumfang des Gebotenen ganz genau. Wie hoch wäre der Normalpreis, und wie lange ist der Gutschein gültig? Denn hier liegt die zweite Gefahr: Oft sind solche Gutscheine an freie Kontingente gebunden und dienen zum Auffüllen in weniger frequentierten Zeiten. Die Gutscheine lassen sich im schlimmsten Fall gar nicht oder nicht zum gewünschten Termin einlösen.

Tipp: Lassen Sie besser die Finger von Angeboten, die eigentlich viel zu günstig sind, um wahr zu sein.

7. Todsünde: Sie kaufen Dinge aus illegalen oder unautorisierten Quellen

Schnäppchenjäger finden bei Software-Download-Diensten wie *http://zoomerart.net*, *http://mainstoreonline.com* oder *http://cheapbestoemonline.net* teure Software zum Superbillig-Preis. Diese und ähnliche Händler begründen die Fast-Geschenkt-Preise (bis zu 95 Prozent Rabatt) damit, dass sie sich das Anfertigen des Datenträgers und der Dokumentation ersparen und der Käufer die Software selbst downloaden muss. Angeblich sollen die Angebote auch legal sein, da es sich bei den Programmen um günstige Sammellizenzen, OEM-Lizenzen oder Palettenware aus Konkursen und Massenware aus Versteigerungen handle.

In der Tat werden Sie keinen Support erwarten können, denn dieser Vertriebsweg ist nicht von den Programmanbietern autorisiert. Zudem handelt es sich bei dem Software-Angebot um OEM-Ausgaben von Programmen, von denen es schon seit etlichen Versionen gar keine OEM-Lizenzen mehr gibt, etwa Adobe Photoshop. Also ist auch nicht mit Updates vom Hersteller zu rechnen. Hinzu kommt, dass sich bei den englischen Versionen der Software meist keine deutschsprachige Benutzerführung einstellen lässt. Und nicht zuletzt müssen Sie auf diesen dubiosen Sites mit Kreditkarte bezahlen, ohne zu wissen, wie dort mit sensiblen Daten umgegangen wird.

Grauzone bei ausländischen Downloadanbietern: Kompliziert ist die rechtliche Lage bei Musik-Downloaddiensten wie *www.justmusicstore.com*, *www.goldenmp3.ru*, *www.mp3fiesta.com* oder *www.mp3sparks.com*. Hier streiten sich Juristen und Industrie, ob die im Ausland ansässigen Dienste über das Recht verfügen, Musik an Kunden in Deutschland zu verkaufen, und ob die hierfür nötigen Urheberrechtsabgaben korrekt abgeführt werden. Wer bei den Diensten Musik erwirbt, hat zwar die Dateien auf dem Rechner, und diese werden in der Regel auch abspielbar sein. Aus Sicht der Musikindustrie handelt es sich jedoch nicht um autorisierte und legale Kopien. Alle vier Download-Anbieter berufen sich auf russisches oder ukrainisches Recht und arbeiten daher international in einer Grauzone.

Manche Juristen gehen davon aus, dass der Kunde, ähnlich wie er sich eine Ware aus einem anderen Land mitbringen kann, dies auch bei Musikdateien tun kann und so von günstigeren Preisen im Ausland profitiert.

15 Tipps für sicheres Surfen

Viele PC-Anwender fühlen sich auf unsicherem Terrain, wenn sie im Internet unterwegs sind. Doch sich grundlegend zu schützen ist gar nicht so schwierig: Wir haben 15 einfache Tipps zusammengestellt, mit denen Sie die häufigsten Gefahren ausschließen.

Von **Tobias Weidemann**

Die Gefahr, im Web Opfer von Abzocke und Spionage zu werden, steigt beständig – und viele Anwender können nicht einschätzen, wo wirklich Fallen stecken und was nur eingebildete Risiken sind. Die meisten Nutzer fühlen sich keineswegs sicher, wenn sie sich im Internet bewegen. Das bestätigt auch Eva Heil, Geschäftsführerin des Internet-Dienstes GMX: „Auch wir bemerken in unserer täglichen Arbeit, dass Anwender sich einerseits sehr wohl der Risiken bewusst sind, andererseits aber mitunter relativ leichtfertig mit ihren persönlichen Daten umgehen, etwa bei der Auswahl von Passwörtern oder der Veröffentlichung ihrer privaten Daten im Internet."

Viel Schutz mit wenig Aufwand: Dabei ist es gar nicht so schwer, für alle Ihre Aktivitäten im weltweiten Netz einen recht umfassenden Grundstock an Sicherheit herzustellen. Mit wenig Mühe können Sie bereits eine Sicherheit von rund achtzig Prozent erzielen. Nachfolgend haben wir 15 einfache Tipps zusammengestellt, die Ihnen ein ordentliches Maß an Schutz verschaffen. Damit können Sie sich bei Ihren Ausflügen ins Netz bereits relativ sicher fühlen. Aber: Eine Vollkasko-Versicherung ist das nicht – die wichtigste Regel gilt immer noch: Lassen Sie den gesunden Menschenverstand walten, und seien Sie nicht zu gutgläubig.

1 Schließen Sie möglichst viele bekannte Sicherheitslücken

Setzen Sie unbedingt die aktuellste Version Ihres Browsers ein, die alle bekannten Sicherheitslücken behebt. Ob es sich dabei um den Internet Explorer handelt, um Firefox oder Safari, ist Geschmackssache. Sorgen Sie außerdem dafür, dass eine aktuelle Sicherheits-Suite installiert ist. Die kann auch kostenlos sein, sollte aber regelmäßig mit den neuesten Virensignaturen ausgestattet werden.

2 Halten Sie Ihren Windows-PC automatisch aktuell

Aktualisierungen Ihrer Windows-Installation sollten Sie am besten automatisch über die Auto-Update-Funktion von Windows erledigen lassen. Diesen Dienst erreichen Sie unter XP über „Start, Systemsteuerung, Verwaltung, Dienste". Rufen Sie hier die Funktion „Automatische Updates" auf. Unter Vista klicken Sie auf „Start, Alle Programme, Windows Update" und ändern dort die Einstellungen.

3 Vertrauen Sie nur Hinweisen aus verlässlichen Quellen

Stellen Sie sicher, dass es sich bei Aktualisierungshinweisen nicht um Werbe-Popups eines obskuren Software-Anbieters handelt. Am einfachsten geht das über die Adresszeile Ihres Browsers: Aktuelle Programme liefern in solchen Fällen Sicherheitshinweise oder färben die Adresszeile zur Warnung rot ein.

4 Verzichten Sie auf die Darstellung von Active X

Active-X-Elemente können nahezu beliebige Operationen auf Ihrem PC ausführen – daher ist dieser Scripttyp grundsätzlich ein Sicherheitsrisiko. Firefox unterbindet von vornherein die Darstellung solcher Elemente. In anderen Browsern, etwa dem Internet Explorer, sind sie dagegen verfügbar. Deaktivieren Sie Active-X-Elemente in den Internet-Optionen des IE (unter „Sicherheit, Stufe anpassen“).

5 Setzen Sie auf sichere Passwörter, und loggen Sie sich aus

Verwenden Sie unter keinen Umständen unsichere Passwörter (etwa überall dasselbe Kennwort oder ein Passwort, das Dritte erraten könnten). Mehr Infos zum Thema Passwortwahl finden Sie in unserem Artikel ab Seite 58. Verlassen Sie Online-Dienste immer über den Log-out-Button, und schließen Sie danach das Browser-Fenster. Andernfalls sind Sie nicht regulär abgemeldet. Im schlimmsten Fall kann dann ein anderer Nutzer Ihre Daten ausspionieren und sogar in Ihrem Namen Bank- und andere Geschäfte tätigen.

6 Schützen Sie sich vor Schädlingen und Spionen

Schauen Sie nicht nur darauf, ob Ihr Mailanbieter Faxe oder MMS versenden kann, einen Kalender oder ein Fotoalbum bietet, sondern achten Sie gezielt auf sicherheitsrelevante Funktionen wie einen Virenschutz für Ihre Mails, einen anpassbaren Spam- und Phishingschutz sowie eine sichere SSL-verschlüsselte Verbindung. Falls diese nicht standardmäßig verwendet wird – immer mehr Provider tun dies –, sollten Sie sie explizit einsetzen.

7 Sichern Sie sich die Möglichkeit zur Weiterleitung von Mails

Wenn Sie Ihrem Mailprovider einmal den Rücken kehren wollen, etwa weil Sie der Datensicherheit oder dem Schutz der Privatsphäre nicht mehr vertrauen, ist die Weiterleitungsmöglichkeit auf ein anderes Mailkonto wichtig. Alternativ sollten Sie aber auch bei dem neuen Account eine regelmäßige automatische Abfrage (zum Beispiel alle 2 Stunden) des bisherigen Kontos einrichten können. Prüfen Sie bereits bei der Wahl eines Mailproviders, ob diese Funktionen implementiert sind.

Ein zeitgemäßer Spamschutz, hier bei GMX, lässt sich individuell anpassen und erweitern. Eine hundertprozentige Erkennungsquote wird aber kein Schutz schaffen (Tipp 6)

8 Nutzen Sie mehrere Adressen, und versenden Sie Mails diskret

Um Ihr Mailkonto vor Spam zu schützen, können Sie mit einem Zweitkonto arbeiten. Nutzen Sie eine Adresse für Ihren persönlichen Bekanntenkreis (Kollegen, Freunde, Familie), und verwenden Sie die andere überall dort, wo Sie befürchten, dass Ihre Adresse für Spam missbraucht wird. Denken Sie auch an Ihre Freunde und Bekannte: Mails an einen größeren Empfängerkreis sollten Sie zum Schutz der Empfänger immer nur an eine Adresse (etwa Ihre eigene) schicken. Der große Adressverteiler kann dann per BCC (Blind Carbon Copy) eingefügt werden.

9 Achten Sie darauf, was der Provider mit Ihren Daten tut

Bei der Wahl Ihres Mailproviders sollten Sie auch auf den Datenschutz achten. Wo werden die Nutzerdaten gespeichert, und nach welchem Recht geschieht das? Während etwa Googlemail nach amerikanischem Recht arbeitet und die Mails mindestens zur Darstellung kontextsensitiver Werbung auswertet, speichern Provider wie Web.de oder Freenet Ihre Mails auf deutschen Servern nach deutschem Recht. Hierzulande ist auch die Möglichkeit einer verdachtsunabhängigen Prüfung durch Behörden nicht vorgesehen. Wenn Sie nach dem Lesen der AGB nicht wissen, nach welchem Recht und wo Ihre Daten gespeichert werden, fragen Sie beim Provider an. Er ist verpflichtet, Ihnen hierüber Auskunft zu erteilen.

10 Geben Sie Ihre Daten nur sparsam weiter

Bevor Sie Daten im Internet angeben, überlegen Sie sich gut, ob das wirklich erforderlich ist Wenn Sie sich beispielsweise für einen kostenlosen Newsletter registrieren wollen, braucht der Anbieter weder Ihr Geburtsdatum noch Ihre Kontodaten. In vielen Fällen werden solche Daten im übrigen nicht überprüft – moniert wird lediglich, wenn ein solches Feld leer ist oder ein offensichtlich falscher Wert eingegeben wurde (Geburtsdatum vor 1900).

11 Vorsicht bei sozialen Netzwerken

Soziale Netzwerke wie Facebook, Myspace oder StudiVZ bieten Datensammlern viele Möglichkeiten, an Mailadressen, Wohnortangaben, Telefonnummern, aber auch persönliche Fotos und Informationen zu kommen. Überlegen Sie sich daher sehr genau, welche Daten Sie mit allen Teilnehmern der Community teilen wollen und welche nur einem engeren Kreis zugänglich sein sollen.

12 Nutzen Sie den Privat-Modus Ihres Browsers

Aktuelle Browser bieten einen Privacy-Modus. Ist dieser aktiv, werden keine Cache-Infos, Verlaufslisten und andere Informationen auf dem PC abgelegt. Ein solcher Modus ist nicht nur beim Surfen auf öffentlichen PCs (etwa in der Bibliothek) sinnvoll, sondern kann auch bei gemeinsam genutzten PCs hilfreich sein. ›

Auch kleinere Online-Shops können seriös sein: Wer sich am Trusted-Shops-Logo orientiert hat, profitiert vom Käuferschutzprogramm (Tipp 15)

13 Nutzen Sie möglichst oft eine verschlüsselte Datenübertragung

Achten Sie gerade beim Online-Shopping auf sichere Übertragungswege. Ihre persönlichen Daten, insbesondere Zahlungsdaten und Kreditkarteninformationen, sollten Sie ausschließlich über eine SSL-verschlüsselte Leitung schicken. Sie erkennen diese am Schloss-Symbol neben der Adressleiste (bei älteren Browsern rechts unten im Browserfenster). Beim Klick auf das Schloss neben der Adressleiste erhalten Sie weitere Informationen zur Verschlüsselung.

14 Setzen Sie auf seriöse Anbieter und achten Sie auf eine für den Kunden geeignete Zahlweise

Prüfen Sie die AGB (Allgemeinen Geschäftsbedingungen) des Händlers auf Fallstricke. Werfen Sie zudem einen Blick ins Impressum oder auf die Angaben zur Kontaktaufnahme. Ist eine Rückfrage nur per Mail oder Brief möglich, werden Sie bei Unstimmigkeiten Probleme haben, den Händler zu kontaktieren. Nur wenige Händler bieten Zahlung auf Rechnung an. Die Zahlung per Nachnahme ist sicherer als per Vorkasse oder Kreditkarte. So gehen Sie immerhin sicher, dass Sie ein Paket bekommen. Gerade in Zeiten zahlreicher Insolvenzen ist ein solcher Zahlungsweg zu empfehlen, bei dem das Geld erst bei oder nach der Lieferung fließt. Im Ernstfall geht der Kunde sonst oft leer aus.

15 Achten Sie auf ein digitales Gütesiegel und Käuferschutzprogramme

Neben den bekannten Firmen wie Amazon, Alternate oder Otto-Versand gibt es eine Vielzahl kleinerer Unternehmen, die Ware ebenfalls zu günstigen Preisen anbieten. Solche Unternehmen können sich für das Trusted-Shops-Zertifikat qualifizieren (*www.trustedshops.de*): Dazu müssen sie bestimmte Regeln in Bezug auf Seriosität, Datenschutz und Liefersicherheit einhalten und dem Kunden ein spezielles Käuferschutzprogramm in Kooperation mit einem Kreditversicherungsunternehmen bieten. Hilfreich können auch Käuferschutzprogramme wie die von Ebay oder Amazon Marketplace sein. Hier wird Ihnen im Schadensfall (Sie erhalten beispielsweise keine Ware oder die Ware entspricht nicht den Absprachen) der Kaufpreis erstattet. Im Fall von Ebay ist das Eintreten des Käuferschutzes aber an eine Reihe von Voraussetzungen gebunden (unter anderem Zahlung per Paypal).