[M] Foto: DEFD; Montage: COMPUTERBILD

ARTIKEL-WEGWEISER

- Tarnseiten für Trojaner und Viren Seite 61
- Programm-Knacker und Hacker-Programme Seite 62
- Viren, Trojaner & Co. zum Download Seite 64
- Illegale Filme, Musik und Software in Tauschbörsen Seite 66
- Abo-Fallen im Internet Seite 68
- Raubkopien als Billig-Angebote im Softwareshop Seite 70
- Illegale Billig-Musik aus Russland Seite 71
- Gefährliche Schutzprogramme Seite 72
- So schützen Sie Ihren PC vor gefährlichen Internetseiten Seite 73
- Das Internet-Sicherheitspaket USB für den Speicherstift ab Seite 74

Gegen die Viren, Trojaner und Abo-Fallen der gefährlichsten Internetseiten hilft kein Laserschwert, wohl aber COMPUTERBILD: Möge das Internet-Sicherheitspaket USB immer mit dir sein!

Taschendiebe, Einbrecher und Trickbetrüger gibt's zwar immer noch. Aber der zeitgemäße Ganove treibt sein Unwesen im Internet. Für ihn ist das weltweite Datennetz ein Paradies: Noch nie war es so einfach, Millionen von Opfern zu schröpfen. Kleine und große Kriminelle kapern fremde Computer, spähen Bankdaten aus, nutzen infizierte PCs als Werbe-Schleudern und als Waffen, um Firmen anzugreifen.

Aber wo drohen diese Gefahren? COMPUTERBILD hat die 100 gefährlichsten Internetseiten zusammengestellt und informiert über ihre Inhalte und Risiken.

Natürlich gibt's noch mehr schlimme Angebote, und sicher bekommen Sie öfter mal eine E-Mail von einem Bekannten mit einem Link* zu einer dubiosen Seite. Die würden Sie vielleicht gern mal anschauen. Das ist Ihnen bislang zu gefährlich? Mit einem gewöhnlichen USB-Speicherstift und dem COMPUTERBILD-Sicherheitspaket USB auf Heft-DVD machen Sie Ihren PC zur unverwundbaren Surf-Station (siehe Kasten rechts).

Vor welchen Seiten muss ich mich in Acht nehmen?

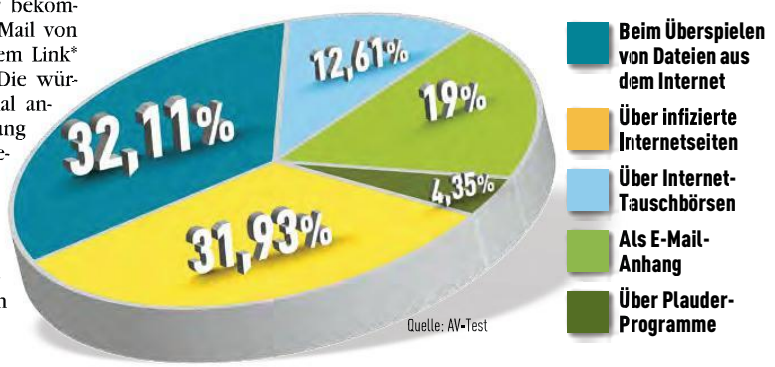
Die größte Gefahr: Schadsoftware, die den Computer zum Teil eines weltweiten Verbrechernetzes („Botnetz") machen. Solche Trojaner* lauern zum Beispiel auf Tarnseiten (siehe rechte Seite), in Software-Knackprogrammen (Seite 62), in Tauschbörsen (Seite 66) und angeblichen Schutzprogrammen (Seite 72). Urheber und Verbreiter sind kriminelle Banden, denen es um Profit geht: Gekaperte und fernsteuerbare Computer von arglosen Nutzern sind viel wert.

Viele Nutzer werden aber auch selbst zum Täter – ohne es zu ahnen. Mit dem Einkauf bei illegalen Software-und Musik-Shops machen sie sich strafbar: Hier werden Raubkopien gehandelt (Seite 70 und 71). Außerdem lauern immer neue Abzocke-Seiten im Netz, die Nutzer mit Versprechungen hereinlegen und dann mit Zahlungsaufforderungen unter Druck setzen (Seite 68).

Wie kann ich mich vor gefährlichen Seiten schützen?

- Erste Pflicht: ein gutes Internet-Sicherheitspaket auf dem PC.
- COMPUTERBILD zeigt, wie Sie die 100 gefährlichsten Internetseiten in Ihrem Internet-Zugriffsprogramm ganz einfach sperren (Seite 73). So können Sie auch nicht zufällig auf den Seiten landen.
- Nutzen Sie für Ausflüge auf dubiose Seiten das Internet-Sicherheitspaket USB (siehe Kasten).

Verbreitungswege von Computerschädlingen



Surf-Versicherung

Mit dem Internet-Sicherheitspaket USB können Sie jede Internetseite gefahrlos besuchen. Die Software funktioniert mit jedem USB-Speicherstift ab 1 Gigabyte. Das Programmpaket gibt's auf Heft-DVD und unter Webcode **10272**[1], die Anleitung ab Seite 74. Wenn Sie noch keinen USB-Stift haben: Mit der Aktion bekommen Sie ein 2-Gigabyte-Modell gratis!

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 158/159.

[1]Wie die Webcodes funktionieren, steht auf Seite 18.

Tarnseiten für Trojaner und Viren

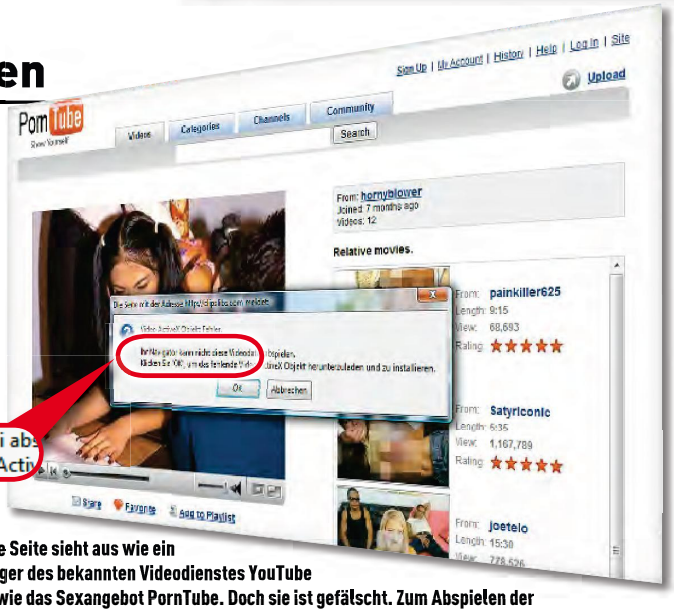
Mit der Schlagzeile „Das Top-Model als Popp-Model“ löste eine Zeitungsmeldung vor Kurzem eine gewaltige Suchwelle aus: Im Internet sei ein Sexvideo mit Model-Sternchen Gina-Lisa aufgetaucht. Einige Kriminelle sprangen auf den Zug auf, kauften Anzeigen bei Google und leiteten so den Ansturm auf ihre Internetseite. Dort sollte es aber nur mit Spezialsoftware was zum Gucken geben. Wer das Programm überspielte, bekam statt pikanter Aufnahmen den fiesen Trojaner „Zlob“ auf den PC.

DAS DROHT

- Unbemerkte Installation von Schadsoftware
- Kriminelle können die Kontrolle über Ihren Computer bekommen
- Per Tastatur-Protokollprogramme werden heimlich persönliche Daten geklaut
- Pornografische Fotos und Videos

Warum sind diese Seiten so gefährlich?

Weil die Gauner mit der Neugierde und Sensationslust der Internetnutzer spielen. Sie beobachten die Internet- und Nachrichtenlage vor allem in Europa und den USA. Mit angeblichen Infos zu Trendthemen wollen sie möglichst viele Besucher auf ihre Internetseiten locken. Weil das recht hohen Aufwand erfordert, muss der Ertrag stimmen: Entsprechend hochgerüstete und gefährliche Schadprogramme auf den Seiten sollen möglichst viele PCs für kriminelle Zwecke nutzbar machen. Vor allem unzählige Pornoseiten sind verseucht – schließlich ist das Thema im Internet beliebt.



Diese Seite sieht aus wie ein Ableger des bekannten Videodienstes YouTube und wie das Sexangebot PornTube. Doch sie ist gefälscht. Zum Abspielen der Videos soll eine Software heruntergeladen werden – inklusive Schädling.

Entwickelt von echten Experten, kommen oft sogenannte Drive-by-Schädlinge zum Einsatz. Das sind Trojaner, die sich allein beim Besuch einer Internetseite installieren. Einfallstore sind etwa Sicherheitslücken im Internet-Zugriffsprogramm. Wird so ein Schädling nicht abgefangen, können Hacker übers Internet weitere Schadprogramme aufspielen, Daten ausspionieren oder den Computer heimlich zum Versenden von unzähligen Werbe-E-Mails nutzen.

Auf welchen Seiten lauern die Gefahren?

Die Gefahr geht nicht nur von Schmuddelseiten aus. Hacker nutzen auch Sicherheitslücken namhafter Internetseiten und schleusen dort Schadcodes ein. So wurde vor Kurzem die Internet-Ticketbörse Eurotickets hop infiziert. Wer Eintrittskarten kaufen wollte, fing sich einen Trojaner ein. Auch das Videoportal YouTube wurde schon zur Verbreitung von Viren missbraucht. Hier tarnte sich ein Trojaner als ein Video.

Eine andere raffinierte Methode: Kriminelle bauen bekannte Internetseiten, wie YouTube oder MySpace, einfach nach und setzen Schädlinge auf die Seite. Arglose Nutzer werden zum Beispiel über Plauderräume (Chats) und Internetforen zu den gefährlichen Imitaten gelockt.

Wer steckt hinter den fiesen Trick-Angeboten?

Die Zeiten haben sich geändert: Inzwischen treiben nicht mehr Hacker und Jugendliche mit Programmierwissen („Script Kiddies“) ihr Unwesen, indem sie Viren zum Spaß oder für Ruhm, Ehre und Nervenkitzel entwickeln. Die Strafen in vielen Ländern wirken auf den Einzelnen zu abschreckend. Stattdessen bringen zunehmend Kriminelle Viren und Trojaner in Umlauf. Sie haben das Internet als lukrative Verdienstmöglichkeit entdeckt.

Mittlerweile hat sich eine gut organisierte und professionelle Verbrecherszene entwickelt, die mit technischem Detailwissen Sicherheitslücken aufspürt. Denn seit Internutzer nicht mehr blauäugig jeden E-Mail-Anhang öffnen, sind immer neue Tricks notwendig, die auf möglichst vielen Computern funktionieren sollen. Die PCs werden gekapert, um sie dann auszuspähen und für weitere Aktionen zu missbrauchen.

Lockvogel BitTorrent-Tauschbörse: Diese Seite verspricht ein Gratis-Programm zum schnellen Überspielen von Daten aus der Tauschbörse. Dahinter lauert aber ein Schädling.

Trittbrettfahrer: Viele Internetnutzer suchten nach einem angeblichen Sexvideo von Gina-Lisa, einer Kandidatin von Germanys Next Topmodel. Gauner leiteten sie auf eine verseuchte Seite.

Die schlimmsten Tarnseiten mit Trojanern und Viren

Adresse	Inhalte und Gefahren
www.fevertube.com	Die Seite wirbt mit Nacktvideos von Prominenten. Im notwendigen Video-Codec lauert ein Virus.
www.girls-forever.com	Lockt mit Pornobildern, untersucht das Internet-Zugriffsprogramm auf Sicherheitslücken.
www.kassperskylabs.cn	Nicht zu verwechseln mit Kaspersky.com! Sucht nach Sicherheitslücken und installiert Schadsoftware.
www.magicpornotube.net	Sex-Videoportal. Auch hier bekommt man schnell einen Trojaner untergeschoben.
www.adultan.com	Wirbt mit kostenlosen Pornofilmchen. Das Programm zum Abspielen enthält aber einen Trojaner.
www.nudeteens.in/3	Lockt mit nackten Tatsachen, schleust Trojaner ein.

Adresse	Inhalte und Gefahren
www.astalavista.box.sk	Populäres Hackerforum, das viele Links zu gefährlichen Programmen bereitstellt.
www.stepbystepbg.org	Die versprochenen Tipps zum Erlernen fremder Sprachen gibt's hier nicht. Dafür einen Trojaner.
www.thetextdesk.com	Diese Seite bietet eine Handy-Software zum Herunterladen an, die aber Schadsoftware enthält.
www.hqticket.com	Das Angebot wirbt mit Gratis-Musik, -Filmen und -Spielen. Der Zugang: ein virenverseuchtes Programm.
www.web-money.cn/arm/	Ein Dienst für Online-Bezahlung, der automatisch eine Software installieren möchte – mit Trojaner.
www.pokerfinds.com	Pokerseite, die Sicherheitslücken im Browser nutzt.

Programm-Knacker und Hacker-Programme

Es ist so einfach, so verlockend: Schnell die Testversion des teuren Programms von der Herstellerseite runterladen, parallel aus einer illegalen Quelle das passende Knackprogramm überspielen und die Kauf-Software damit freischalten. Schon hat man die Vollversion für lau. Das ist aber nicht nur strafbar, sondern auch gefährlich: Oft nisten sich mit den Knackern Schädlinge auf dem Computer ein!

DAS DROHT
- Fiese Schadprogramme aller Art in Cracks & Co.
- Botnetz-Trojaner öffnen den PC für die Spam-Mafia
- Pornografische Bilder
- Schadensersatzklagen der Software-Hersteller (Rechteinhaber)

Was wird auf den Internetseiten angeboten?

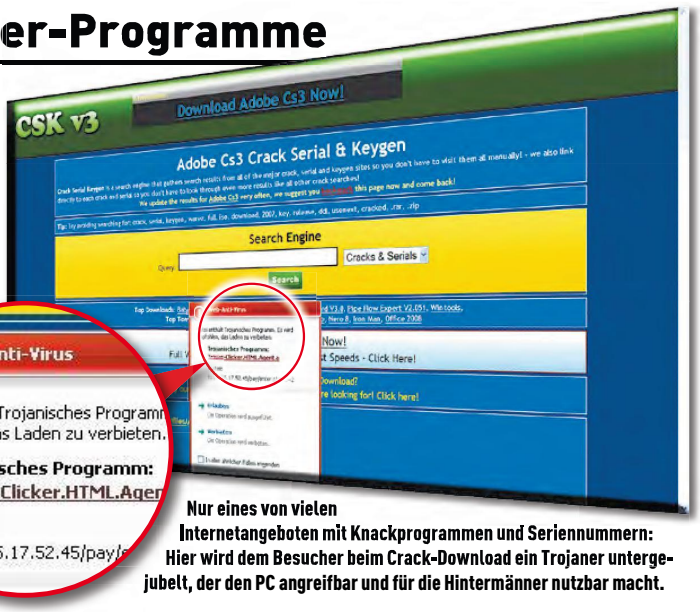
Jegliche Arten von Hilfsmitteln, mit denen sich Raubkopien besorgen und herstellen lassen:

- **Serials/Serialz:** Das ist der Codename für Seriennummern. Mit ihnen lassen sich Programmkopien installieren oder Testversionen zur Vollversion aufrüsten. Serialz werden entweder direkt auf den illegalen Internetseiten angezeigt, oder sie lassen sich als Textdatei auf den PC überspielen.
- **Cracks/Crackz:** Dahinter stecken eine oder mehrere Dateien, die eine raubkopierte Software so verändern, dass sie nutzbar wird. Dazu wird zum Beispiel die Seriennummern-Kontrolle deaktiviert, die Startdatei des Programms gegen eine manipulierte Version ausgetauscht. Spätestens wenn die geknackte Software aktualisiert werden soll, kann es Probleme geben. Dann ist ein neuer Crack nötig.
- **Keygens**: Das ist die Abkürzung für Schlüsselgeneratoren („Key“ = Englisch für „Schlüssel“). Diese kleinen Programme berechnen gefälschte, aber funktionierende Seriennummern zum Freischalten von Software.

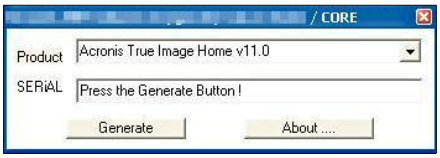
Woher kommen die Cracks und Seriennummern?

Cracks stammen meist von raubkopierten Programmversionen der sogenannten Release- oder Warez-Szene. Die Mitglieder analysieren Software und entwickeln passende Knack-Methoden. Manchmal gibt es im Internet Cracks, bevor das betreffende Programm im Laden steht.

Vielen Mitgliedern der gut organisierten Gruppen geht es um Ruhm und Anerkennung in den eigenen Reihen: Wer kommt am schnellsten an aktuelle Software? Wer hat eine neue Software zuerst geknackt? Einzelne Gruppen-Mitglieder beschaffen die Originalprodukte so früh wie möglich, etwa aus DVD-Presswerken. Andere sind für das Knacken von Kopierschutzmaßnahmen zuständig. Um Key-Generatoren zu erstellen, prüfen sie die Logik der Seriennummern einer Software und automatisieren mit einem Programm die „Produktion“ von gültigen Nummern. In meist geheimen Internet-Foren und Plauderräumen tauscht sich die Szene aus.



Nur eines von vielen Internetangeboten mit Knackprogrammen und Seriennummern: Hier wird dem Besucher beim Crack-Download ein Trojaner untergejubelt, der den PC angreifbar und für die Hintermänner nutzbar macht.



Seriennummern per Mausklick: Ein Programm errechnet für Software der Firma Acronis gültige Nummern.

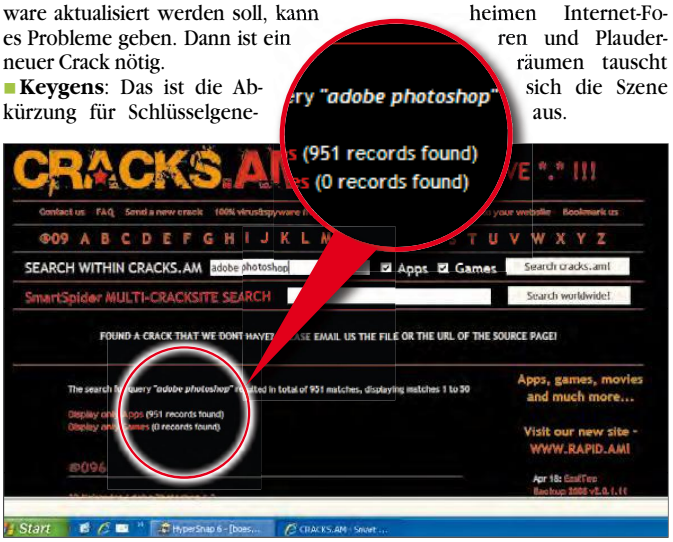
Wer steckt hinter den Crack-Seiten?

Selten die Programmierer der Warez-Szene selbst. Nur einige Mitglieder halten den Kontakt zu Betreibern der „kommerziellen“ Crack-Seiten. Diesen Gruppen geht es um handfesten Profit: Sie fügen den Cracks und Seriennummern-Dateien Trojaner hinzu, stellen sie auf ihr Internetangebot. Bei den Suchmaschinen kaufen sie beliebte Begriffe wie „Cracks“ oder „Serialz“ – schon tauchen ihre Seiten in den Ergebnislisten ganz oben auf. Viele setzen noch auf den Sex-Faktor, bestücken ihre Seiten mit pornografischen Fotos, um Interessenten anzulocken.

Klickt ein Nutzer auf einen Crack-Link*, kommt das Knackprogramm zwar auf den Computer – damit kein Verdacht aufkommt. Gleichzeitig hat sich der Nutzer allerdings einen Trojaner* eingefangen. Das ist der Profit der dunklen Warez-Szene: Viele infizierte Computer auf der ganzen Welt. Kriminelle können so die PCs fernsteuern und zum Teil eines Botnetzes machen. Gauner versenden über solche Computer und deren E-Mail-Anschluss massenhaft Werbe-Nachrichten (Spam). Oder sie fangen per Lauschprogramm (Keylogger) eingetippte Bank- und Kreditkartendaten ab.

Beispiel www.serialz.to: eine riesige Sammlung mit rund 80 000 Seriennummern zum Herunterladen. Die Serialz-Software wird dem Besucher schmackhaft gemacht: „Hier kannst du die beste Serialz-Sammlung der Welt herunterladen. Nach dem Download benötigst du lediglich die bei uns regelmäßig erscheinenden zweiwöchentlichen Updates.“ Stimmt – aber mit der Software holt man sich auch ein Schnüffelprogramm auf den PC.

Die Hintermänner der Crack-Seiten verschleiern ihre Identität. So



Die Crack-Suchmaschine www.cracks.am findet allein 951 höchst illegale Knackprogramme für verschiedene Versionen der Bildbearbeitungs-Software Adobe Photoshop. Es ist ungewiss, wie viele der Dateien mit Viren und Trojanern verseucht sind.

Bei www.serialz.to gibt's eine Datenbank mit Zehntausenden Seriennummern zum Gratis-Herunterladen und mit regelmäßigen Aktualisierungen. Achtung: Zusammen mit der Datenbank wird Werbe- und Spionage-Software installiert.

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 158/159.

nutzen sie zum Beispiel für die Registrierung ihrer Internetadressen spezielle Anonymisierungsdienste, die in ihrem Namen die Adressen anmelden.

Was sind „Hacker-Tools“?

Das sollen Programme sein, mit deren Hilfe jeder zum Profi-Knacker werden kann. Flavio Riberio, Betreiber der Seite www.hackpalace.com, brüstet sich etwa damit, „mehr als 400 Megabyte Daten zum Thema Hacking“ gesammelt zu haben – natürlich nur zu „Forschungszwecken“. Auf solchen Hack-Seiten gibt es neben schwer verständlichen Hack-Anleitungen, die sehr gute Computerkenntnisse voraussetzen, mitunter auch Passwortknacker oder Software zum Belauschen von Computer-Netzwerken (Sniffer).

Solche Programme sind ungefährlich. Sie können sogar nützlich sein. Etwa, wenn man selbst mal sein eigenes Computer-Passwort vergessen hat. Gefährlich wird’s, wenn „Hacker-Tools“ in die falschen Hände geraten und etwa zum Ausspionieren von Kollegen oder Nachbarn missbraucht werden.

Manche dieser Hacker-Seiten bieten sogar funktionstüchtige Virenbaukästen und komplette Trojaner-Sammlungen zum Download an (mehr dazu auf Seite 64).

„Hacker-Spider“ verspricht Werkzeuge für den Profi-Hacker. Als Zugang dient eine Software – ein teurer Dialer für Modem- und ISDN-Nutzer. Wer den Zugang per DSL wählt, merkt die Abzocke schnell: 12,50 Euro für sechs Minuten, zahlbar per Vorkasse-Karte.

Die schlimmsten Seiten mit Cracker- und Hacker-Werkzeugen

Adresse	Inhalte und Gefahren
www.easycracks.net	Crack-Suchmaschine, „täglich aktualisiert“, Links* sind mit Trojanern verseucht
cracks.thebugs.ws	Crack-Downloads funktionieren, die Links sind allerdings trojanerverseucht
www.icracks.net	Wer sich Knackprogramme von dieser Seite überspielt, bekommt einen Trojaner untergeschoben.
www.anycracks.com	Auch auf dieser Seite lauern Trojaner hinter den Crack-Links.
www.keygen.name	Jede Menge Cracks, Serials und Nummern-Generatoren, beim Download wird ein Trojaner installiert.
www.serialz.to	Datenbank mit rund 80 000 Nummern zum Download, die Spionage- und Reklame-Software installiert.

Adresse	Inhalte und Gefahren
www.crackportal.com	Mehr als 100 000 Knackprogramme zum Herunterladen, infizierte Download-Links
www.serialsbox.com	Hier droht beim Überspielen von Dateien eine Infektion mit dem Trojaner „Zlob“
www.keygen.us	Seriennummern-Generatoren und Cracks zum Herunterladen, alle Links sind verseucht.
www.seriall.com	Wer sich Knackprogramme von dieser Seite überspielt, bekommt den „Small“- Trojaner untergeschoben.
www.hackpalace.com	„Sicherheits-Seite“ mit Hack-Anleitungen, Passwortknackern, Lauschprogrammen und vielem mehr
www.hackingstore.de www.hacker-spider.at.nr	Angeblich bekommt man hier Hacker-Software, es wird aber ein Einwahl-Abzock-Programm installiert.

Viren, Trojaner & Co. zum Download

Ganz unverblümt kommen Hacker in ihren Internet-Foren zur Sache, wenn's um das Ausnutzen von Sicherheitslücken geht: „Ich bin ein Neuling beim Hacken. Jetzt wollte ich mal fragen, wie ich mir meinen eigenen Trojaner selber programmieren kann", schreibt zum Beispiel „OverKiller" in einer Diskussionsgruppe.

Ein richtiger Hacker zu werden, ist heute nicht mehr allzu schwer.

DAS DROHT

- Fatale Experimente: Bei kleinsten Fehlern gefährden Sie sich und andere.
- Gefährliche Neugier: Virenbaukästen sind selber Schädlinge.
- Geldstrafe droht: Wer Viren verbreitet, macht sich strafbar.

Denn Lernmaterial in Form von Wissen und Viren steht für „OverKiller" und andere Nachwuchs-Hacker massenweise im Internet bereit: auf sogenannten Virii-Seiten.

Was findet man auf den Virii-Seiten?

„Virii", der lateinische Plural von „Virus", ist der Szene-Ausdruck für Schadprogramme. Hunderte solcher Programme gibt's auf einschlägigen Internetseiten zum Überspielen für jedermann. Außerdem finden Hacker hier Programmcodes von Viren zum Heim-Studium oder Baukästen, mit denen Sie selber Viren erzeugen können. Beides ist extrem gefährlich: Wer sich nicht auskennt, fängt sich selbst einen Virus ein. Auf Seiten wie Phreak.org gibt's Viren als direkt ausführbare Dateien. Ein falscher Klick, und der Virus startet gleich nach dem Überspielen.

Und in den sogenannten Virus-Construction-Kits (Virenbaukästen) stecken oft selbst Schädlinge, die beim Start des Baukasten-Programms aktiv werden. Besonders fies: www.freewebs.com/green-hell. Hier werden angeblich vom Programmierer selbst geschriebene Viren angeboten. Tatsächlich aber steckt in jedem Programm die gleiche Schadsoftware, die auf dem PC eine Hintertür für weitere Schadprogramme öffnet. Das Sprichwort „Wer anderen eine Grube gräbt, fällt selbst hinein", gilt auch für den „Virus Wizard". Hinter dem Virenbaukasten verbirgt sich ein sogenannter Dropper. Das ist ein Programm, das weitere Schädlinge in Windows einschleust.

Getarnt: Wer diesen angeblichen Virenbaukasten installiert, holt sich in Wahrheit einen Dropper. Das ist ein Programm, das wiederum andere Schadprogramme installiert, zum Beispiel den Trojaner Dldr.Apropo.G.

Wer steckt hinter den Virii-Seiten?

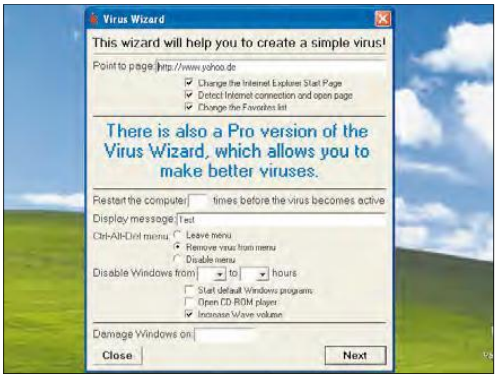
Einerseits sind es Idealisten, die auf die Sicherheitslücken von PC-Systemen hinweisen wollen. So wenigstens liest es sich auf den Eingangsseiten der Virii-Angebote. Einige betrachten sich als „Künstler", die nach Herausforderungen suchen. Es gelte, neue Techniken zu erlernen, schreibt etwa das aus Polen veröffentlichte Magazin Hakin9.

Aber natürlich gibt's auch Hacker, die nur von krimineller Energie angetrieben werden. Selbst bei vermeintlich ehrenhaften Seiten bleibt ein schaler Beigeschmack: Auch wenn die auf den Seiten vorhandenen Viren schon bekannt sind und es Gegenmittel gibt, schafft das hier verbreitete Wissen die Basis für noch gemeinere Viren.

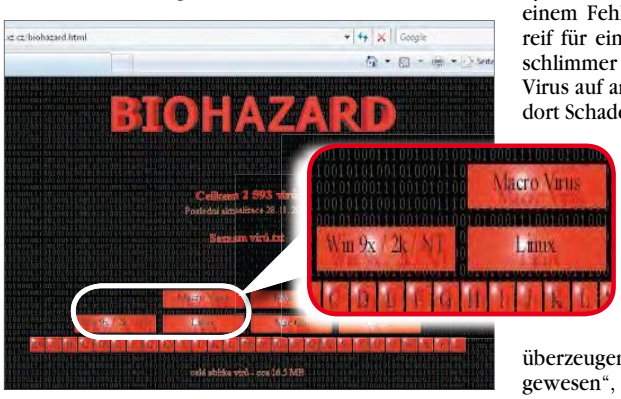
Welche Konsequenzen drohen, wenn ein Virus freikommt?

„Es kann immer passieren, dass man sich verklickt und aus Versehen das Virus startet", schreibt „TankyFranky" in einem Viren-Forum. Nach so einem Fehlklick ist der eigene PC reif für eine Neuinstallation. Noch schlimmer wird's, wenn sich der Virus auf andere PCs überträgt und dort Schaden anrichtet.

„Wenn man vorsätzlich Schadprogramme in andere PCs einschleust, drohen Geld- oder Freiheitsstrafe", sagt Rechtsanwalt Stefan Kramer. „Da wird's auch schwierig, einen Staatsanwalt davon zu überzeugen, es wäre ein Versehen gewesen", so Kramer. „Es genügt schon, dass so etwas fahrlässig geschieht."



Zu spät: Wurde der Virus Wizard gestartet, ist auch der Trojaner bereits auf der Festplatte installiert und bereitet Angriffe vor.



Auf der Seite von Biohazard sind die Schädlinge säuberlich nach Betriebssystemen sortiert. Sogar seltene Linux-Viren gibt's hier.

Die schlimmsten Seiten mit gefährlichen Viren

Adresse	Inhalt
www.biohazard.xz.cz	Virensammlung aus Tschechien
www.hackpalace.com/virii/indexe.shtml	Umfangreiche Virensammlung
www.phreak.org/html/virii.shtml	Viren und Virengeneratoren zum Download. Viele können direkt gestartet werden.
vx.netlux.org	Große Sammlung von Virenbaukästen
www.rigacci.org/comp/virus/	Kleine, aber sehr gefährliche Virensammlung
www.worst-viruses.2ya.com/	Viren und Virenbaukästen zum Download
vx.org.ua/delphi/	Virensammlung und Quellcodes von Viren in der Programmiersprache Delphi
members.fortunecity.com/acid_knight/virii.html	Chaotisch strukturierte Virensammlung
www.pugnax.co.uk/code	Quellcode für einige Viren als „Lernmaterial"

Adresse	Inhalt
www.textfiles.com/virus/	Umfangreiche Anleitungen zur Virenerstellung
membres.lycos.fr/gatesbillou/	Virengeneratoren zum Download
www.freewebs.com/green-hell/	Viren zum Download mit versteckten Trojaner. Wer die Dateien überspielt, wird ausspioniert.
vxchaos.2hell.com/	Umfangreiche Sammlung von Viren, Trojanern und anderer Software mit ähnlichen Inhalten
www.geocities.com/randy027dsz36/	Virengenerator zum Download. Enthält „Dropper" zum Installieren weiterer Schadprogramme!
web.tiscalinet.it/dec_spiderman/home.htm	Viren und Quelltexte, Seite auf Italienisch
www.nvkz.kuzbass.net/as/	Umfangreiche Virensammlung auf Russisch
el-killer.chez-alice.fr/Virii.htm	Kleinere Sammlung wirkungsvoller Viren

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 158/159.

Illegale Filme, Musik und Software in Tauschbörsen

Alltag in einem Tauschbörsen-Forum: Stolz berichtet Nutzer „Nightelf“ über seine Erfolge: „Von der UBR-Crew gibt es bis heute circa 151 Film-Releases im Netz, immer in guter Qualität. Es erscheint immer ein Release die Woche.“ Prompt bedankt sich Forum-Mitglied „samurai05“ artig für das neueste Film-Angebot…

Was sich harmlos anhört, ist ein illegales Hobby: Die „UBR-Crew“ ist eine Raubkopierer-Gruppe, „Film-Releases“ sind Veröffentlichungen im Internet – natürlich illegal.

DAS DROHT
- Schadsoftware aller Art
- Fast ausschließlich raubkopierte Musik und Filme – die Nutzung ist strafbar
- Internet-Ermittler können Nutzer relativ leicht identifizieren
- Pornografische Bilder und Videos

Wie funktioniert die Tausch-Szene?

Gehandelt werden Filme und Musik über Tauschbörsen-Netze wie Bittorrent und Gratis-Speicherplatzanbieter wie Rapidshare. Die Nutzer verteilen die Links* zu den Raubkopien auf einschlägigen Internetseiten, in Foren und privaten E-Mails. Im Angebot sind aktuelle und ältere Kinofilme in TV- oder DVD-Qualität, Musik von Tausenden Interpreten bis hin zu Profiprogrammen samt Seriennummer zum Freischalten.

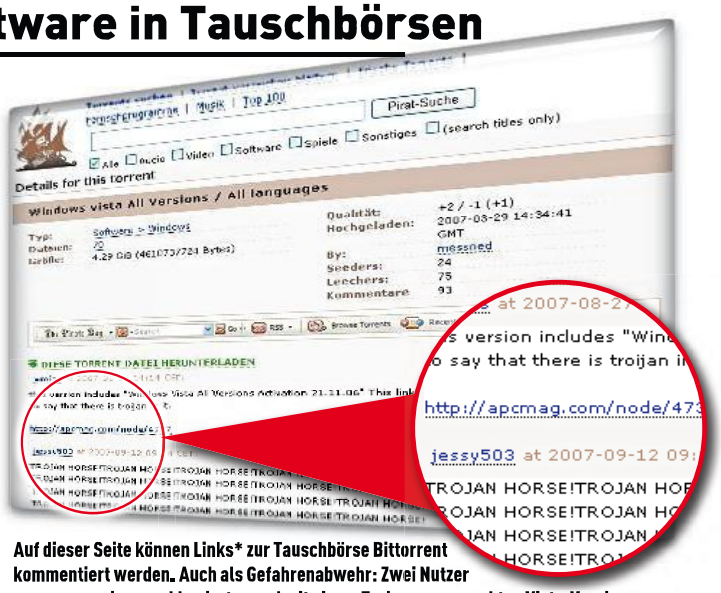
Für das Bittorrent-Netzwerk ist eine Überspiel-Software notwendig. Jeder, der damit Musik oder Filme herunterlädt, bietet sie gleichzeitig im Netzwerk an. So entsteht ein weltweites Netz aus vielen Quellen, einen zentralen Computer mit der Tauschware gibt es nicht. Dateien bei Rapidshare lassen sich dagegen ohne Hilfsmittel mit einigen Klicks überspielen („Direct Downloads“).

Die meisten Tauscher sind Privatpersonen, etwa Filmfans und Musikliebhaber, denen Originale zu teuer sind. Tauschen ist aber kein Kavaliersdelikt: Sobald sie illegale Kopien anbieten, machen sie sich strafbar. Die Benutzung von Tauschbörsen und Internetfestplatten ist nur legal, solange legale Dateien getauscht werden. Etwa eigene Bilder, Videos oder Gratis-Software.

Wer steckt hinter den Tauschseiten?

Die Betreiber von Seiten mit Tauschbörsen-Links wie „Goldesel“ oder „Saugstube“ sind nur schwer oder gar nicht zu ermitteln. Die Computer stehen mal in den Niederlanden, mal in Rumänien. Die Verantwortlichen bleiben anonym. Dabei sehen sich die meisten Betreiber nur als Link-Vermittler und nicht als Raubkopierer. So steht etwa auf der Goldesel-Startseite: „Auf dieser Seite sind lediglich Links zu einer Tauschbörse. Das Programm sucht dann selber danach und wir haben dann damit nichts mehr zu tun!“

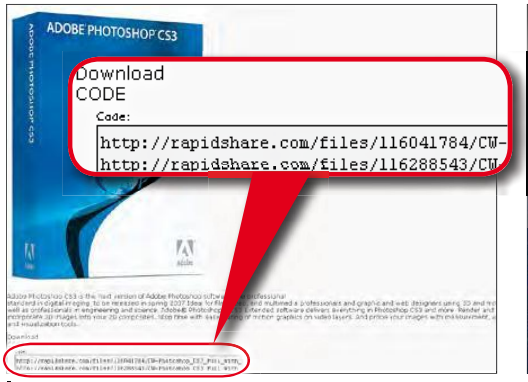
Letztendlich geht’s aber ums Geld: Die Tauschseiten sind mit Reklame gepflastert, vor allem mit jeder Menge Erotik-Werbung. Klicks auf Bilder und Banner lassen die Kassen klingeln. Wer jedoch der Werbung folgt, gelangt schnell in gefährliche Ecken des Internets.



Auf dieser Seite können Links* zur Tauschbörse Bittorrent kommentiert werden. Auch als Gefahrenabwehr: Zwei Nutzer warnen vor einer raubkopierten und mit einem Trojaner verseuchten Vista-Version.

Welche Gefahren lauern in Tauschbörsen?

- **Schadsoftware:** Immer wieder versuchen Kriminelle, über Tauschbörsen mit Viren und Trojanern verseuchte Daten unters Volk zu bringen. Vor allem Knackprogramme für Software sind gefährlich. Zwar gibt’s auf vielen Tauschseiten eine Art Kontrolle, indem infizierte Dateien gemeldet und die Links entfernt werden. Doch selbst in kurzer Zeit klicken viele Nutzer auf die versprochenen Filme oder Spiele und laden sich die Dateien herunter.
- **Strafverfolgung:** Bei Tauschbörsen haben Ermittler leichtes Spiel: Sie bieten Musik an und protokollieren, welche Internetnummern (IP-Adressen) die Dateien heruntergeladen haben. Damit stellen sie Strafanzeige und warten, bis die Internetanbieter die Namen der betreffenden Kunden preisgeben müssen. Die bekommen dann mindestens eine kostenpflichtige Unterlassungserklärung.



Im Forum dieser Seite gibt’s unter anderem Links zu geknackter Profi-Software wie Adobe Photoshop CS3. Die Programme lagern auf Rapidshare-Internetcomputern.

Auf vielen Tauschseiten prangt Porno-Werbung. Im schlimmsten Fall wird der PC mit Schadsoftware infiziert, Sicherheitslücken in Videoprogrammen bieten die Angriffsflächen.

Die schlimmsten Seiten mit illegalen Filmen, Songs und Software

Adresse	Inhalte und Gefahren
www.mininova.org	Umfassende Suchseite für das Bittorrent-Netzwerk, englische Filme und Software als Raubkopien
www.sceneload.to	Jede Menge Tauschbörsen-Links zu illegalen Filmen, Musik, Software, Hörspielen, Pornografie
www.serienjunkies.org	Deutsche Seite mit Bittorrent-Links, hier lagern fast ausschließlich Links zu kopierten TV-Serien aller Art
www.hoerspiele.to	Deutsche Seite mit Download-Links zu Hörbüchern und Hörspielen im MP3-Format. Achtung: illegal!
www.dimeadozen.org	Bittorent-Links zu Videos mit illegalen Konzertmitschnitten, Registrierung erforderlich
www.saugstube-torrent.to	Links zu Musik, Software, Filmen und Spielen im Bittorrent-Netzwerk, viel aggressive Porno-Werbung

Adresse	Inhalte und Gefahren
www.ddl-search.com	Suchseite für illegale „Direct Downloads“ bei Internetfestplatten-Diensten wie Rapidshare
www.oxygen-warez.com	Links zu raubkopierten Filmen, Musik, Programmen bei Rapidshare und anderen Speicherplatz-Anbietern
www.goldesel.6x.to	Jede Menge illegale Kopien von Filmen, Spielen und Musik, täglich kommen 40 bis 60 Links hinzu
www.ddl-warez.org	Deutsche Seite mit den neuesten direkten Download-links zu Raubkopien bei Rapidshare
www.usenext.de	Kostenpflichtiger Zugang zu Nachrichtengruppen mit Raubkopien; Anbieter rechnet Datenvolumen ab
www.firstload.de	Kostenpflichtiger Newsgroup-Zugang mit eigener Software für illegale Dateiangebote

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 158/159.

Abo-Fallen im Internet

Sandra W. ist einem Internet-Abzocker in die Falle gegangen: „Ich hatte es eilig, wollte zu einem Geschäftstermin nach Bremen“, erklärt sie. Ein paar Klicks in einer Suchmaschine, schon landet sie auf den Seiten von Routenplaner-server.com und gibt ihre Adresse ein. „Ich habe mir nichts dabei gedacht, es waren keine Informationen darüber zu sehen, dass die Routenplanung Geld kostet.“

DAS DROHT

- Ein falscher Klick, schon sind Sie in der Abo-Falle.
- Horrende Rechnungen und einschüchternde Mahnschreiben.
- Im schlimmsten Fall hilft nur noch der Gang zum Anwalt.

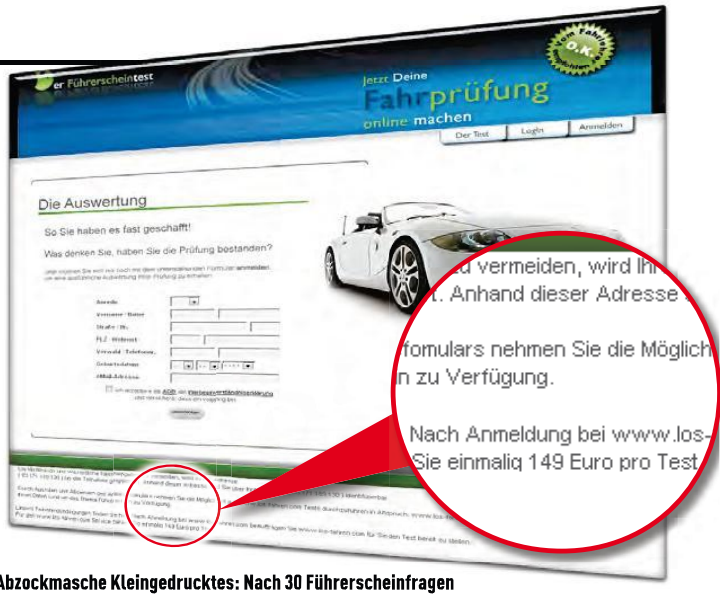
Dann schnappt die Falle zu. Erst kommen Rechnungen, später folgen Mahnungen. 107 Euro und 10 Cent soll die Grafikdesignerin bezahlen, so das Mahnschreiben der Münchener Anwältin Katja Günther. Zum Abopreis von 59,95 Euro kommen noch Mahnkosten, Verzugszinsen und natürlich 39 Euro für die „Inanspruchnahme“ der Anwältin hinzu. Ein gutes Geschäft für Anbieter und Anwältin. Das ist die linke Tour der Abo-Abzocker im Internet: Fallen stellen, täuschen, Druck machen, bis das Opfer zahlt.

Wie wird abgezockt?

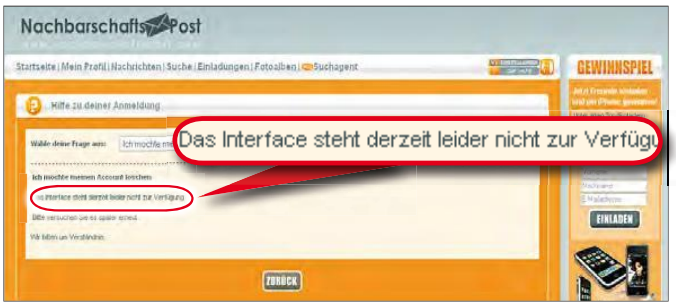
Abo-Abzocker setzen auf die Leichtgläubigkeit der Nutzer, auf Spieltrieb oder Eile. Wer wie Sandra W. schnelle Infos braucht, liest nicht jeden Satz im versteckten Kleingedruckten einer Seite, sondern gibt die eigene Adresse ein und klickt auf „Weiter“, um möglichst flott zum Ergebnis zu kommen. Die Abzocker bieten in der Regel einfache Dienstleistungen und Informationen: Kochrezepte, Referate, Routenplanung oder die „Berechnung“ der Lebenserwartung. Auch SMS-Versand oder einfache Spielereien stehen auf dem Programm der Fallensteller.

Doch es gibt auch immer wieder neue Variationen der Masche. Opfer werden zum Beispiel gezielt per SMS oder E-Mail in die Abofalle gelockt. Die Seite Online-girlies.com zum Beispiel verschickt E-Mails mit dem Hinweis, dass auf der Internetseite angeblich Nacktbilder des Empfängers veröffentlicht worden sind. Wer sie entfernen möchte, solle doch bitte die Seite anwählen und sich registrieren. Kostenpunkt: 98 Euro.

Per SMS sucht auch nachbarschaftspost.com nach Kunden. Angeblich sei eine Nachricht eingegangen und man müsse sich nur registrieren, um die Post abzurufen. Nach Eingabe von Handynummer, Namen und Vornamen sitzt das Opfer in der Falle: 216 Euro werden fällig. Ebenfalls neu: ein Führerscheintest. Hier beantwortet das Opfer 30 Fragen aus der Führerschein-Theorieprüfung. Das Ergebnis gibt’s nur gegen Eingabe der eigenen Adressdaten. Die Kosten betragen 149 Euro.



Abzockmasche Kleingedrucktes: Nach 30 Führerscheinfragen muss das Abzockopfer seine Adresse eingeben. Dass er außerdem 149 Euro zahlen soll, ist tief im Kleingedruckten versteckt.



Noch eine Abzockmasche: Die Seite Nachbarschaftspost.com lockt damit, dass man das Angebot auch online widerrufen kann. Der entsprechende Bereich auf der Seite ist aber angeblich außer Betrieb.

Wer steckt hinter den Abofallen?

Dubiose Firmen mit wechselnden Namen. Als Betreiber von routenplaner-server.com zum Beispiel nennt die Münchener Anwältin in ihren Schreiben die „NetContent Ltd.“. Im Impressum der Seite steht aber inzwischen die „Online Content Ltd.“. Die Spur der Firma führt nach Großbritannien. Dort ist sie auf den Namen der 22-jährigen Katarina Dovcová aus der Slowakei registriert. „Ich gehe davon aus, dass das ein Strohmann ist“, sagt Tim Peters von der Verbraucherzentrale Hamburg e.V. Denn die Konten liegen immer bei deutschen Banken.

Häufig stößt man im Impressum der Abo-Seiten auf die Andreas & Manuel Schmidtlein OHG. Die Brüder betreiben zahlreiche Portale wie Hausaufgaben-heute.com, Ge-

Die schlimmsten Abo- und Abzock-Seiten

Adresse	Beschreibung
www.los-fahren.com	Führerscheintest. Das Ergebnis gibt’s gegen Eingabe der eigenen Adresse – und 149 Euro.
www.nachbarschaftspost.com	Nachbarschaftsnetzwerk und Kontaktbörse. Schickt SMS an das Opfer, um es auf die Seite zu locken.
www.online-girlies.com	Porno-Seite. Verschickt E-Mails, in denen behauptet wird, dass dort pikante Fotos des Opfers zu sehen sind.
www.wie-anziehend-bist-du.de	Seite mit Persönlichkeitstests. Kunde verzichtet beim Anmelden angeblich auf sein Widerrufsrecht.
www.mega-downloads.net	Lockt mit Gratis-Software. Anzeigen verweisen auf teure Unterseiten. Kosten: 96 Euro.
www.ihre-Rezepte.de	Rezeptdatenbank mit versteckten Kostenangaben im Kleingedruckten.
www.smsfree100.de	Angeblicher Gratisversand von SMS. Nach der Eingabe der Adressdaten kommt die Rechnung.
www.vorlagen-land.de	Datenbank mit Vorlagen für Büroprogramme. Lockt mit Gewinnspiel zur Adresseingabe.
www.sudoku.de	Sudoku-Rätsel, angeblich auch mit einem Programm, mit dem sich eigene Rätsel erstellen lassen.
www.grafik-archiv.com	Bilderdatenbank, lockt mit animierten Grafiken. Kosten im Kleingedruckten

Adresse	Beschreibung
www.kochrezepte-download.de	Rezeptdatenbank. Kosten im Kleingedruckten: 59,95 Euro. Lockt mit einem Gewinnspiel zur Anmeldung.
www.every-game.com	Computerspiele zum Download. Kosten im Kleingedruckten. Lockt mit Gewinnspiel.
www.routenplaner-server.com	Streckenplaner. Lockt mit Gewinnspiel. Kosten im Kleingedruckten versteckt.
www.astrologie-server.com	Horoskope, etwa zu Liebe, Partnerschaft oder Beruf. Lockt mit Gewinnspiel. Kosten: 79,95 Euro.
www.gehalts-rechner.de	Berechnet das Netto-Gehalt. Nach Eingabe der Finanzdaten muss man sich registrieren.
www.hausaufgaben-server.com	Hausaufgaben, Referate und Lerntipps. Lockt mit Gewinnspiel. Kosten im Kleingedruckten.
www.online-flirten.de	Partnersuche und Flirtseite mit angeblich über 23 000 Einträgen. Lockt mit Gutschein und Gewinnspiel.
www.condome.tv	Kondom-Abonnement angeblich zum kostenlosen Test. Widerrufsrecht erlischt bei Zustimmung.
www.genealogie.de	Namens- und Ahnenforschung. Angeblich eine wissenschaftliche Datenbank.
www.meine-wunderbare-katze.com	Katzen-Shop mit teurer Clubmitgliedschaft. Kunden werden mit individuellen Ansteckern gelockt.

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 158/159.

dichte.de oder p2p-heute.com. Wer hier seine Daten eingibt, um das Angebot zu „testen“, erhält nach kurzer Zeit ein Abo. Kosten: 168 Euro.

Wieso funktionieren die Tricks der Abzocker?

Abo-Abzocker weisen zwar meist auf die Kosten hin. Nur geschieht das in der Regel so, dass kaum ein Kunde die Informationen genau liest und versteht. Grundsätzlich stehen die Bedingungen im Kleingedruckten, oft versteckt unterhalb des sichtbaren Bereichs einer Seite oder bewusst unleserlich gestaltet mit grauem Text auf weißem Untergrund oder Schwarz auf Grau.

Häufig – etwa bei p2p-heute.com – sind die Bedingungen auch nicht als Text auf einer Seite hinterlegt, sondern als Bilddateien. Wer die Textdarstellung vergrößern will, um die Teilnahmebedingungen bequemer zu lesen, scheitert. Denn Grafik-Texte lassen sich nicht größer darstellen.

Neueste Verschleierungsmasche: Wie-anziehend-bist-du.de zeigt zwar den Preis deutlich an, aber dafür verzichtet der Kunde auch gleich auf sein Widerrufsrecht, wenn er die AGB akzeptiert.

Sitzen die Opfer in der Falle, folgt der Druck. Erst Mahnungen, dann meldet sich in der Regel ein Inkassobüro und später ein Anwalt. Auch im Fall von Sandra W.: „Themenschwerpunkt Strafrecht“ steht einschüchternd im Adressfeld des Schreibens der Anwältin. Unten auf der Seite findet sich ein Hinweis, dass Daten über versäumte Zahlungen an die Schufa weitergeleitet würden. Das muss man sich nicht bieten lassen. Mit einem Musterschreiben, in dem man die Forderungen bestreitet, kann man sich wehren. Das empfiehlt auch Tim Peters von der Verbraucherzentrale Hamburg. „Erst wenn ein gerichtlicher Mahnbescheid ins Haus flattert, müssen Sie reagieren und binnen zwei Wochen Einspruch einlegen. Doch dazu kam es bislang in keinem mir bekannten Fall.“

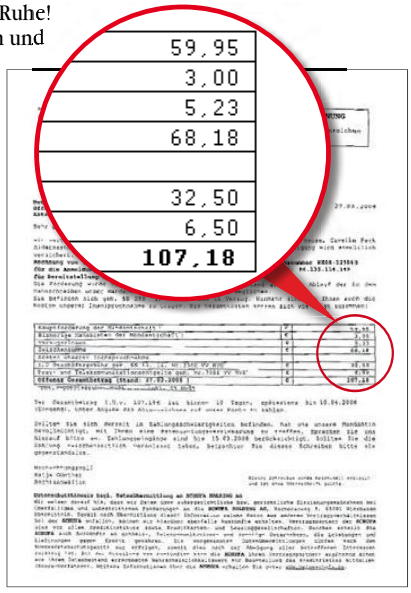
Wie kommen Sie aus der Abo-Falle wieder raus?

Ganz wichtig: Bewahren Sie Ruhe!

- Ignorieren Sie Rechnungen und Mahnungen.
- Reagieren Sie auf ein Anwaltsschreiben mit einem Formbrief. Beispiele und weitere Infos gibt’s unter ➔① und ➔②.
- Falls doch ein gerichtlicher Mahnbescheid kommt, sollten Sie möglichst schnell einen eigenen Anwalt einschalten.

Internet: ➔① www.vis.bayern.de/recht/handel/vertragsarten/abo-fallen.htm
➔② www.rotglut.org

Abzockmasche Widerrufsrecht: Mit dem Akzeptieren der allgemeinen Geschäftsbedingungen (AGB) verzichtet das Opfer auch gleich auf das Widerrufsrecht. Das ist rechtlich nicht zulässig!



Die Standard-Mahnung der Münchner Anwältin. Zu den Abo-Kosten addiert sie ihre Gebühren. Solche Schreiben können Sie ignorieren.

Raubkopien als Billig-Angebote im Softwareshop

Das komplette Microsoft-Office-2007-Programmpaket für nur 79,95 statt 849 Euro? Wem das nicht spanisch vorkommt, den haben die Profi-Raubkopierer schon fast am Haken. Doch wer auf solche Werbe-E-Mails (Spam) hereinfällt, kauft illegale Software.

DAS DROHT
- Strafverfolgung wegen Nutzung illegaler Kopien
- Missbrauch der Kreditkartendaten
- Defekte Aktualisierungsfunktionen der illegalen Programme
- Schadensersatzklagen der Rechteinhaber

Was wird beworben?

Teure Software zu Schleuderpreisen. Damit können die Shop-Betreiber schnell viel Geld verdienen. Im Angebot sind zum Beispiel die Produkte von Microsoft (Windows, Office), Adobe (Creative Suite) und Corel (Graphics Suite).

Bei diesen Preisen ist klar: Die Shops verkaufen Raubkopien, die nur mit Knackprogrammen (Cracks) und geklauten oder gefälschten Seriennummern funktionieren. Hat der Kunde per Kreditkarte bezahlt, kann er die Dateien direkt auf die Festplatte* herunterladen. Häufig bekommt er auch CD- oder DVD-Abbilder („Images"), die er erst auf einen Rohling brennen muss.

Mit professionell gestalteten Seiten, Warenkorb-Funktion und Support-Formular täuschen die Shops Seriosität vor. Einige sind sogar auf Deutsch – zumindest teilweise. Als Begründung für die Billig-Preise verweisen viele Anbieter auf die fehlende Verpackung und das fehlende Handbuch. Häufig preisen sie ihre Ware als „OEM-Software" an. Das sind Programme, die in der Regel nur mit PCs verkauft werden dürfen.

Was passiert, wenn man Programme bestellt?

COMPUTERBILD hat testweise anonym einige Programme geordert:

- Zwei Einkaufsversuche scheiterten nach der Eingabe der Kreditkartendaten mit Fehlermeldungen. Die ungewisse Gefahr: Möglicherweise sind die Betreiber nur an den Kreditkartendaten interessiert.
- Bei einem Shop gab's auch statt Software eine Fehlermeldung. Dennoch wurde der Kaufbetrag von der Kreditkarte abgebucht: 100 Dollar (rund 64 Euro) für ein Office-Paket.
- Drei Bestellungen klappten. Die Tester konnten je ein Virenschutzprogramm von McAfee (9,50 Euro) und Symantec (11,50 Euro) sowie Windows Vista (51,15 Euro) kaufen und auf den PC überspielen. Der anschließende Virencheck war negativ: Beim Download kamen keine Schädlinge auf den PC.

Dann der Funktionstest: Mit den Schutzprogrammen gab's keine Probleme. Die per Freischalt-Crack aktivierte Vista-Kopie verlangte nach Installation des Service Packs 1 eine erneute Aktivierung. Der Crack funktionierte aber nicht mehr, die illegale Vista-Kopie ist also nutzlos.

Einer der bestgemachten illegalen Shops: Euro Software sieht professionell aus, das Angebot ist groß, und die Programme sind spottbillig. Per Spam-Mails wird der Shop beworben (Bild unten links). Achtung: Verkauft werden Raubkopien.

Wer steckt hinter den illegalen Angeboten?

Beispiel Euro Software und Soft Sales: Hinter den Shops steckt der in den USA bereits verurteilte Spammer Leonid Kuvayev. Auf der Anti-Spam-Seite „Spamhaus" beschreiben ihn ehemalige Angestellte als jemanden, „der für Geld alles tut" und ins schmutzige Geschäft mit Kinderpornografie verstrickt ist. Kuvayevs Masche: Er wirbt mit Spam-Mails für seine illegalen Aktivitäten vom Raubkopie-Handel über Online-Apotheken und Internet-Casinos bis zum knallharten Porno. Seine Internetangebote betreibt er vor allem auf Computern in Südamerika, China und Russland – überall dort, wo harte Dollar mehr zählen als legale Inhalte.

Warum Kriminelle wie Kuvayev schwer zu fassen sind, erklärt Christine Ehlers, Sprecherin der Gesellschaft zur Verfolgung von Urheberrechtsverletzungen (GVU): „Sitzen die Anbieter im Ausland, ist die Rechtslage unsicher und die Strafverfolgung sehr schwierig."

Damit internationale Strafverfolger ihm nicht zu Leibe rücken können, steuert Kuvayev seine Aktivitäten mit Hilfe sogenannter Bot-Netze. Das sind Armeen fremder Computer, die per Virus gekapert wurden. Über die PCs der ahnungslosen Nutzer verschickt er dann die Werbe-E-Mails zu seinen Shops.

In schlechtem Deutsch verfasste Reklame-Mails (Spam) preisen immer wieder billige Software an. Viele verweisen auf die Shops von Soft Sales und Euro Software (Bild oben).

Der COMPUTERBILD-Testeinkauf schlug bei mehreren Shops fehl, unter anderem bei Soft Sales. Verdächtig: Fehlermeldungen erschienen immer erst nach der Eingabe der Kreditkartendaten.

Die schlimmsten Seiten mit Raubkopien

Adresse	Inhalte und Gefahren
www.aesofta.com	Eine von vielen Adressen zum Raubkopien-Shop Euro Software von Leonid Kuvayev, Werbung per Spam.
www.zoomerart.net	Etwas anderes Angebot, aber gleiches Bestellsystem wie unter austein.com.
www.austein.com	Billig gemachter Shop, Raubkopien werden als günstige „OEM-Software" verkauft.
www.mainstoreonline.com	Wer bei www.austein.com einkauft, landet im Bestellprozess in diesem Shop; nahezu identisches Angebot.

Adresse	Inhalte und Gefahren
www.cheapbestoemonline.net	Shop „Soft Sales", Bestellung brach nach Eingabe der Kreditkartendaten ab.
www.adobemasters.com	„Online OEM Soft Store" nicht nur mit Programmen von Adobe, Werbung mit 80 Prozent Erspanis.
www.vip-soft.us	Gleiche Masche wie bei Soft Sales, die Bestellung brach nach Eingabe der Kreditkartendaten ab.
www.ldkueekadernau.com	Der Raubkopien-Shop „Downloadable Software", für den in verschiedenen Spam-E-Mails geworben wird.

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 158/159.

Illegale Billig-Musik aus Russland

Geht's nur um die Preise, können iTunes, Musicload & Co. einpacken: Während in den etablierten Musik-Shops ein heruntergeladener Song 99 Cent kostet, gibt's in Internet-Shops wie LegalSounds und MP3fiesta fürs gleiche Geld das komplette Album. Was alles andere als legal ist …

DAS DROHT

- Strafverfolgung wegen Nutzung illegaler Kopien
- Missbrauch Ihrer Kreditkartendaten
- Schadensersatzklagen der Rechteinhaber

Wie funktioniert die Musik-Masche?

Es gibt viele illegale Shops für MP3-Musik. Viele Betreiber sitzen in Russland. Ihre Masche:

- Die Angebote – in englischer, oft auch deutscher Sprache – sehen professionell und seriös aus.
- Die Preise liegen so weit unter den sonst üblichen, dass die Versuchung für jeden Musikfan groß ist: Ein Titel kostet je nach Anbieter zwischen 9 und 20 Cent, ein ganzes Album 1 bis 2 Euro.
- Viele Shops bieten über zwei Millionen Songs an. Dazu gehören aktuelle Alben, aber auch ältere Titel – wie bei iTunes & Co.
- Mit Hinweisen auf rechtmäßige Verträge mit örtlichen Rechte-Verwertungsgesellschaften und Gebührenzahlungen wird der Eindruck erweckt, das Angebot sei legal und alles in Ordnung.
- Viele Shops bieten per Klick die aktuelle Chartmusik westeuropäischer Länder und der USA an.

Für die Bezahlung akzeptieren die Shops vor allem Kreditkarten. Nach der erforderlichen Registrierung muss der Musikfan in der Regel sein Benutzerkonto zunächst mit 10 bis 100 Dollar aufladen. Der Kauf einzelner Songs ist fast nie möglich.

Billig-MP3-Shops wie Soundike.com unterbieten die Preise bekannter Angebote wie iTunes: 1,44 Dollar (rund 0,92 Euro) für ein ganzes Album. Der Shop aus Moskau hält rund 100 000 Titel bereit, bei anderen Anbietern sind es sogar über zwei Millionen Songs. Einen Kopierschutz gibt's – natürlich – nicht.

Wer steckt hinter den Musik-Downloads?

Das bleibt meist unklar. Ein Impressum mit Kontaktdaten, wie es auf deutschen Seiten üblich ist, gibt es nur selten. Auch ein Blick in die Registrierungsdaten der Internetadresse hilft nicht. So wurde zum Beispiel www.MP3fiesta.com von einer „Istok Company Ltd." registriert. Die Firma soll in Kiev ansässig sein, ist im offiziellen Firmenregister für Ltd.-Unternehmen aber nicht eingetragen. So bleiben die Hintermänner anonym. Experten der Musikindustrie wissen: Einige Shops gehören zur organisierten Kriminalität.

Es gibt aber auch Anbieter wie www.mp3search.ru, die sich nicht verstecken. Sie verweisen jedoch ebenfalls ausschließlich auf Verträge mit Verwertungsgesellschaften. Lizenzen von internationalen Plattenfirmen haben sie nicht – verkaufen deren Musik aber trotzdem. Deshalb gilt: Finger weg!

Das Kleingedruckte eines Shops: Der Anbieter verweist auf eine „Copyright-Lizenz" der Organisation AVTOR – eine der selbst ernannten Verwertungsgesellschaften in Russland. Weiter heißt es: „Der Kunde übernimmt die Verantwortung."

Das sagt die Urheberrechts-Expertin

COMPUTERBILD fragte Marion Janke, Rechtsanwältin und Urheberrechtsexpertin in Rostock

Musik-Shops wie MP3sugar.com und mp3va.com geben sich einen legalen Anstrich. Zu Recht?
Billig-MP3-Shops berufen sich auf Fantasie-Lizenzabkommen fragwürdiger Organisationen wie „AVTOR". Der Wahrheitsgehalt solcher Behauptungen ist für Laien nur schwer abzuschätzen. Bei den genannten Shops ist es praktisch ausgeschlossen, dass Plattenfirmen und Künstler an den Einnahmen aus Musikdownloads beteiligt sind.

Was raten Sie Musikfans, die sich für solche Shops interessieren?
Verlassen Sie sich keinesfalls auf die Beteuerungen der Anbieter, alles sei legal. Wer bei solchen Billig-Downloads zugreift, kann sich später nicht auf die Versprechungen des Anbieters berufen und muss im Zweifelsfall für Schadensersatzforderungen der Rechteinhaber einstehen.

Die schlimmsten Seiten mit illegaler Billig-Musik

Adresse	Beschreibung
www.lavamus.com	Rund 2,35 Millionen Titel, jeder Song für 15 Cent, zahlbar per Kreditkarte
www.iomoio.com	Rund 900 000 Songs je 15 Cent, jedes Stück kann mehrfach geladen werden
www.mp3skyline.com	Mehr als 2,6 Millionen MP3-Songs (13 Cent) aller Richtungen, einige Titel sind aus dem Radio aufgezeichnet
www.soundike.com	Songs ab 10 Cent, Sprachoption „Deutsch" ohne Funktion, Bezahlung per Kreditkarte
www.soundsbox.com	Chart-Musik, jeder Titel kostet 9 Cent, mit eigenem Download-Manager
www.mp3search.ru	12 Cent pro MP3-Song, führt nach eigenen Angaben Gebühren an eine russische Rechtegesellschaft ab
www.mp3sugar.com	Rund 670 000 Titel für je 18 Cent im Angebot, Betreiber ist die Fantasiefirma „SweetMedia Ltd."

Adresse	Beschreibung
www.musicmp3.ru	MP3s ab 10 Cent pro Titel, laut Internetseite rund 500 000 Titel im Angebot, keine Kreditkartenzahlung
www.mp3ninja.com	Shop aus Lettland der nicht existenten „Digimobi Ltd.", Titel-Preise ab 5 Cent
www.mp3fiesta.com	1,3 Millionen Songs ab 13 Cent, Charts aus den USA und England, Bezahlung per Kreditkarte
www.mp3va.com	10 Cent pro Titel, etwas niedrigere Tonqualität als bei den übrigen Shops, PayPal-Zahlung möglich
www.mp3city.com.ua	Ukrainische Seite mit vielen Chart-Hits, jeder Titel kostet 13 Cent
www.justmusicstore.com	2,1 Millionen MP3-Songs, deutschsprachig, Werbung mit Gratis-Song für Neukunden
www.songboxx.com	MP3-Suchmaschine: durchstöbert gut ein Dutzend dubiose Shops nach Titeln, Interpreten und Alben

Gefährliche Schutzprogramme

Sie tragen Namen wie Win-Antivirus, Malwarealarm oder Spystriker und stehen reihenweise auf Internetseiten zum kostenlosen Überspielen bereit. Doch was klingt wie eine Sammlung von Schutzprogrammen gegen Viren und Spionage, ist in Wahrheit nur ein mieses Geschäft mit der Angst. Denn diese und andere „Sicherheitsprogramme“ geben nur vor, den Computer vor Schädlingen zu schützen. In Wirklichkeit bietet keins davon ausreichende Sicherheit. Im Gegenteil: Viele dieser Programme bringen sogar selber Schädlinge mit!

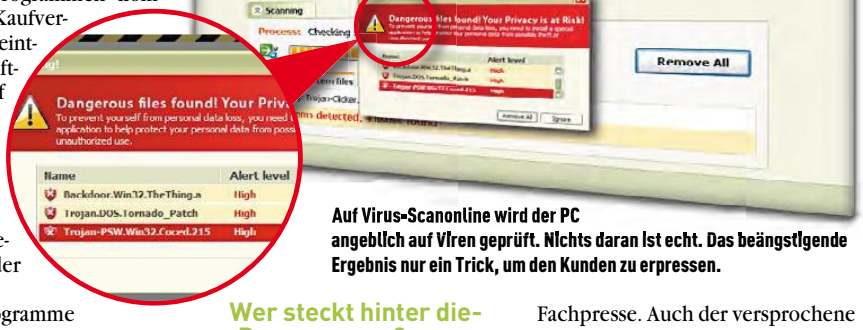
DAS DROHT

- Schädlinge gelangen auf Ihren Computer
- Angebliche Schutzprogramme erpressen mit erfundenen Schädlingen
- Entfernung von Viren und Spionage-Programmen nur gegen Bares

Was machen diese Programme?

Die Masche ist immer ähnlich: Auf einer seriös wirkenden Internetseite wird ein Virenschutz- oder Anti-Spionage-Programm zum kostenlosen Überspielen angeboten. Nach der Installation wird klar:

- Kostenlos ist bloß die Überprüfung. Wird ein Schädling gefunden, kann er nur gegen Geld entfernt werden.
- Damit der Kunde auch ja zahlt, erfinden viele dieser Abzock-Programme Schädlinge und erpressen so zum Kauf der Vollversion.
- Echten Schadprogrammen kommen auch die Kaufversionen der vermeintlichen Schutzsoftware kaum auf die Spur.
- Auch harmlose Dateien (zum Beispiel Cookies) werden zur Bedrohung aufgebauscht, damit der Kunde kauft.
- Einige der Programme gehen sogar so weit, selber Schädlinge auf dem Computer zu installieren. Die werden dann beim Suchlauf natürlich gefunden.
- Ein Teil der Software belästigt den Nutzer mit Werbung und spioniert ihn aus.
- Viele dieser Programme lassen sich nur sehr schwer wieder entfernen.



Auf Virus-Scanonline wird der PC angeblich auf Viren geprüft. Nichts daran ist echt. Das beängstigende Ergebnis nur ein Trick, um den Kunden zu erpressen.

Wer steckt hinter diesen Programmen?

Die Internetseiten kommen meist von Servern in China, der Ukraine oder in Russland. Entsprechend schwer ist es, die Hintermänner zu enttarnen. Die Angaben auf den Internetseiten sind in fast allen Fällen pure Fantasie. Ebenso die Fotos der angeblichen Firmensitze und die angegebenen Auszeichnungen der Fachpresse. Auch der versprochene Kundendienst ist nicht mehr als eine Luftnummer: Auf Anfragen gibt's nur automatisierte Antworten.

Woran erkenne ich, ob ich so ein Programm habe?

Leider ist die Erkennung alles andere als einfach. Denn es gibt mittlerweile über 100 von diesen gefährlichen Programmen (siehe auch COMPUTERBILD 23/2007). Die verbreitetsten finden Sie unten in der Liste. Mit dabei ist zum Beispiel Winantivirus, ein Klassiker der Betrugsprogramme, das sich in immer neuen Versionen bereits seit Jahren auf dem Markt hält.

Allen betrügerischen Programmen ist eins gemeinsam: Es gibt sie nicht beim Händler, sondern nur zum Überspielen von meist englischsprachigen Internetseiten. Wenn Ihr Antiviren- oder Anti-Spionage-Programm von so einer Seite stammt, sollten Sie es sofort entfernen, um ganz sicherzugehen. Verlassen können Sie sich auf die Produkte, die COMPUTERBILD getestet hat. Sicherheitsprogramme, die Ihren Computer wirklich schützen, finden Sie in der Bestenliste auf Seite 139 oder auf Heft-CD/-DVD (Kaspersky Security Suite CBE).

Abzocker: Expert Antivirus findet nur wenige Virentypen, dafür aber Risiken, die keine sind. Das Programm bringt sogar eigene Schädlinge mit, um PC-Nutzer mit Funden zu überzeugen.

Auch seriös gestaltete Internetseiten sind keine Garantie für verlässliche Produkte. MyNetProtector findet immer Bedrohungen – auch auf sauberen Computern.

Die schlimmsten Seiten mit gefährlichen Sicherheitsprogrammen

Adresse	Inhalte und Gefahren
www.winantivirus.com	Der Klassiker unter den Abzock-Programmen. Hält sich seit Jahren in immer neuen Versionen auf dem Markt. Bietet auch gegen Geld keinen ausreichenden Schutz.
www.adwarestriker.com	Hersteller Bulletproof kopiert für seine Schutzprogramme die Schädlings-Datenbanken seriöser Hersteller. Die „Schutzprogramme“ erfinden Schädlinge.
www.expertantivirus.com	Auf dieser Internetseite gibt's ein Antiviren-Programm, das Schädlinge selber mitbringt und Windows-Dateien manipuliert.

Adresse	Inhalte und Gefahren
www.spystriker.com	Hier gibt's ein angebliches Anti-Spionage-Programm. Es erfindet Schädlinge und erpresst zum Kauf der Vollversion. Es bietet keinen ausreichenden Schutz.
http://virus-scanonline.com	Hier wird der PC angeblich übers Internet auf Viren geprüft. Das immer gleiche Ergebnis: Alles verseucht. Die passende „Schutzsoftware“ gibt's zum Überspielen.
www.mynetprotector.com	Das hier angebotenen Schutzprogramm macht den PC nicht sicherer – im Gegenteil: Es macht Windows manipulierbar und erfindet Schädlinge.

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 158/159.

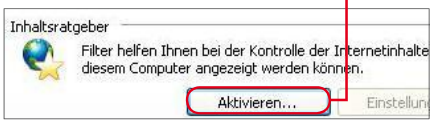
So schützen Sie Ihren PC vor gefährlichen Internetseiten

Das Internet steckt voller schlimmer Seiten. Um Ihre Familie, Ihren Geldbeutel und den Computer vor den übelsten Fallen im Netz zu schützen, hat COMPUTERBILD eine Sperrliste mit über 100 gefährlichen Adressen auf die Heft-CD/-DVD dieser Ausgabe gepackt. In den folgenden Anleitungen erfahren Sie, wie Sie all diese Adressen in einem Rutsch als „schwarze Liste" ins Internet-Zugriffsprogramm übertragen. Diese Internetseiten werden dann künftig automatisch geblockt. Während der Internet Explorer bereits eine Funktion zum Importieren enthält, müssen Sie den Firefox noch mit der Erweiterung BlockSite nachrüsten. Das Programm finden Sie auch auf der beiliegenden Heft-CD/-DVD.

Gefährliche Internetseiten im Internet Explorer sperren

Der Internet Explorer von Microsoft hat einen eingebauten Filter für Internetadressen, den „Inhaltsratgeber". Setzen Sie darin eine Adresse auf die schwarze Liste, können alle Computernutzer die Adresse nur noch mit einem Kennwort öffnen. Wie Sie die Funktion einrichten und die Sperrliste importieren, lesen Sie hier:

1 Starten Sie den Internet Explorer mit Mausklicks auf Start, auf Alle Programme und auf Internet Explorer. Klicken Sie auf Extras und in der daraufhin aufklappenden Liste auf Internetoptionen. Im nächsten Fenster folgen Klicks auf Inhalte und auf .



2 Im erscheinenden Fenster klicken Sie auf Allgemein, setzen hier

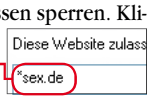
per Mausklick einen Haken und klicken danach auf Übernehmen. Damit stellen Sie sicher, dass nur die gefährlichen Internetseiten aus der COMPUTERBILD-Sperrliste blockiert werden und nicht andere, harmlose Angebote.

3 Laden Sie jetzt die Sperrliste. Legen Sie dazu die COMPUTERBILD-Heft-CD/-DVD dieser Ausgabe ins Laufwerk, und schließen Sie das erscheinende Fenster per Klick auf BEENDEN. Nach einem Klick auf Erweitert klicken Sie auf die Schaltfläche Importieren.

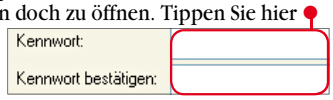
Zur Auswahl der Sperrliste klicken Sie im nächsten Fenster auf und doppelt auf den Eintrag des Laufwerks, hier SAFECRACKERS (J:).

Es folgen Doppelklicks auf Titelthema und Sperrliste-IE. Klicken Sie auf .

Sie können noch weitere Adressen sperren. Klicken Sie auf Zugelassene Sites, und tippen Sie zum Beispiel ein. Das vorangestellte Sternchen sorgt dafür, dass sowohl sex.de als auch www.sex.de blockiert werden. Klicken Sie auf Niemals und auf Übernehmen.

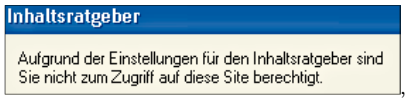


4 Nach einem Klick auf OK müssen Sie ein Kennwort festlegen. Das brauchen Sie, um die Sperrfunktion zu ändern oder um blockierte Seiten doch zu öffnen. Tippen Sie hier



zweimal das gewünschte Kennwort ein, und fügen Sie danach im Feld darunter einen Hinweistext als Gedächtnisstütze ein, zum Beispiel gleiches Kennwort wie E-Mail. Nach drei Klicks auf OK ist die Funktion aktiviert. Beenden Sie den Internet Explorer per Klick auf .

5 Versuchen Sie zur Probe, eine gesperrte Internetseite zu laden, im Beispiel mp3va.com. Daraufhin erscheint das Fenster



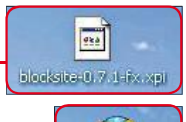
und das Laden der Seite wird verhindert. Klicken Sie auf Abbrechen, um zur vorherigen Seite zurückzukehren. Falls Sie eine blockierte Seite dennoch laden möchten, tippen Sie im gleichen Fenster Ihr Kennwort ein und und klicken anschließend auf OK. *[hes]*

Gefährliche Internetseiten in Firefox sperren

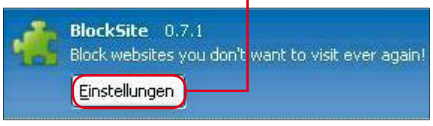
Falls Sie mit Firefox im Internet surfen, brauchen Sie das Zusatzprogramm BlockSite von der aktuellen COMPUTERBILD-Heft-CD/-DVD. Lesen Sie hier, wie Sie es installieren und die Sperrliste von COMPUTERBILD übernehmen. Gibt es auf Ihrem Computer mehrere Benutzerkonten? Dann müssen Sie die Anleitung auf allen Konten durchführen.

1 Legen Sie die beiliegende Heft-CD/-DVD in das Laufwerk, und kopieren Sie die Erweiterung BlockSite 0.7.1 auf die Arbeitsoberfläche*. Sie finden den Eintrag in der Rubrik Titelthema. Danach schließen Sie die CD-/DVD-Oberfläche per Klick auf BEENDEN.

2 Installieren Sie nun die Erweiterung. Dazu klicken Sie auf , ziehen dann das Symbol mit gedrückter Maustaste auf das Symbol und lassen die Taste los. Daraufhin startet Firefox mit dem Fenster Software-Installation. Warten Sie, bis darin die Schaltfläche Jetzt installieren zu sehen ist, und klicken Sie darauf. Die Erweiterung wird installiert. Sobald das abgeschlossen ist, starten Sie Firefox mit einem Mausklick auf Firefox neu starten neu.

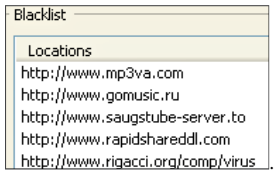


3 Nach dem Neustart klicken Sie im Fenster Add-ons auf .



Importieren Sie dann die Sperrliste von der Heft-CD/-DVD. Dazu klicken Sie auf Import, auf

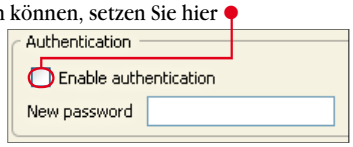
und doppelt auf den Eintrag für das Laufwerk mit der CD/DVD, hier SAFECRACKERS (J:). Klicken Sie jeweils doppelt auf Titelthema und Sperrliste-Firefox. Im Fenster BlockSite Import klicken Sie einmal auf Append. Das Ergebnis sieht so aus:



Übrigens: Sie können die Liste bei Bedarf noch um weitere Adressen erweitern. Dazu klicken Sie auf Add. Im nächsten Fenster drücken Sie einmal auf , auf und tippen die Adresse ohne „www" ein, in diesem Beispiel .

Nach einem Klick auf OK wird die Adresse zur schwarzen Liste hinzugefügt.

4 Wenn Sie nicht wollen, dass andere Nutzer Ihres PCs Änderungen an dieser Liste vornehmen können, setzen Sie hier



einen Haken und tippen neben New password ein Kennwort ein. Speichern Sie dann die Änderungen per Klick auf OK, und schließen Sie das Fenster Add-ons per Mausklick auf .

5 Probieren Sie es aus: Tippen Sie eine gesperrte Adresse ein, etwa mp3va.com, und drücken Sie . Die Internetseite wird nicht geladen. Stattdessen erscheint der Hinweis .

Die Datei blocksite-0.7.1-fx.xpi können Sie von der Arbeitsoberfläche löschen. *[js]*