COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/so-umsurfen-sie-alle-gefahren,1936326

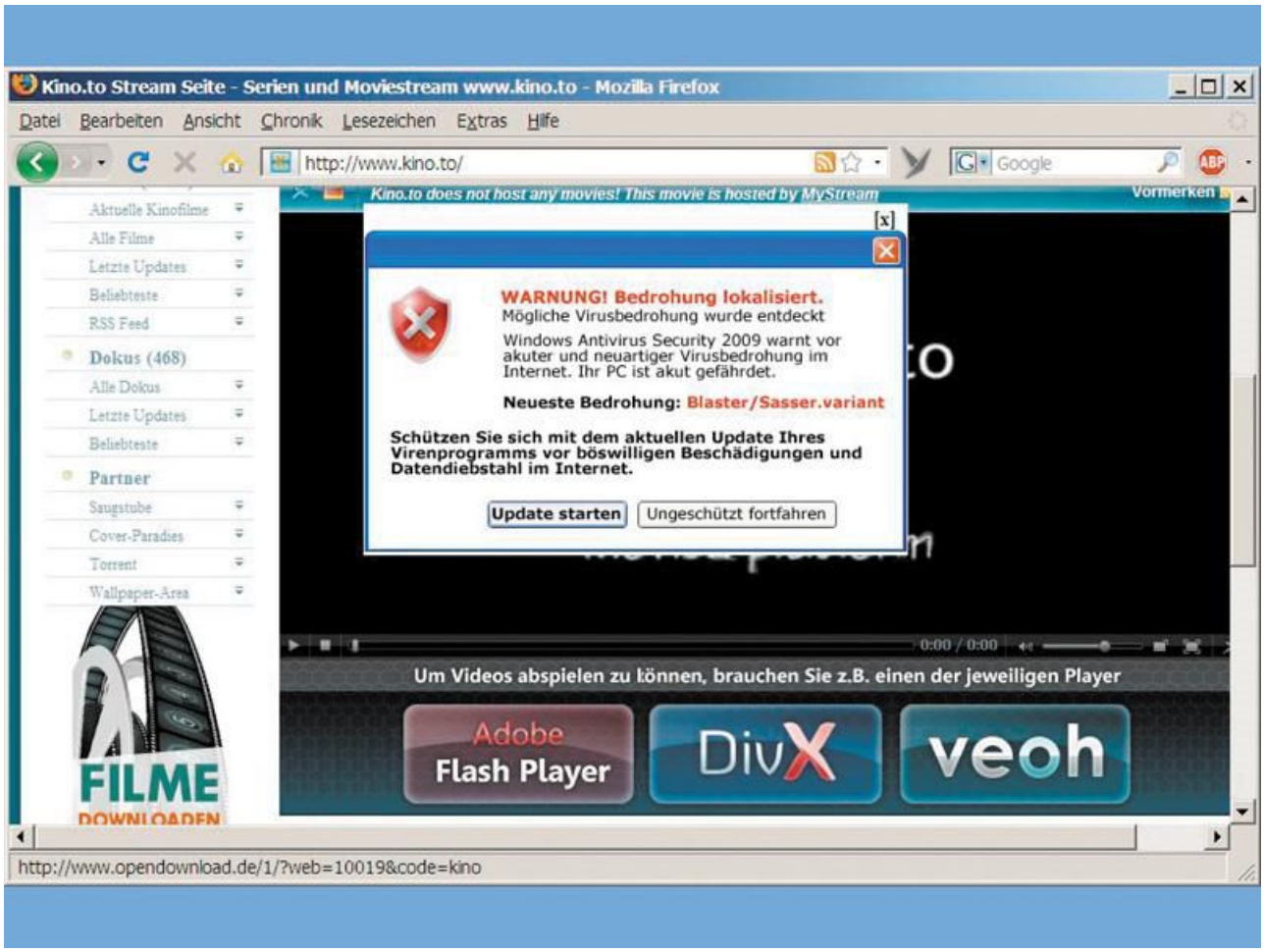
Die 7 größten Internet-Fallen

So umsurfen Sie alle Gefahren

Datum: 17.06.2010
Autor(en): Tobias Weidemann

Schadsoftware, Viren, Trojaner: Im Internet kann man sich jede Menge Probleme einfangen. Hier lesen Sie über die sieben schlimmsten Fallstricke im Web und wie Sie diese sicher umsurfen.

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 durchs 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.



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

1. Fehler: 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**[1] aussehen. Die Einblendungen wollen Ihnen weismachen, dass sie Systemhinweise Ihres **PCs**[2] 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).

2. Fehler: Sie nutzen Downloadlinks von zwielichtigen Sites

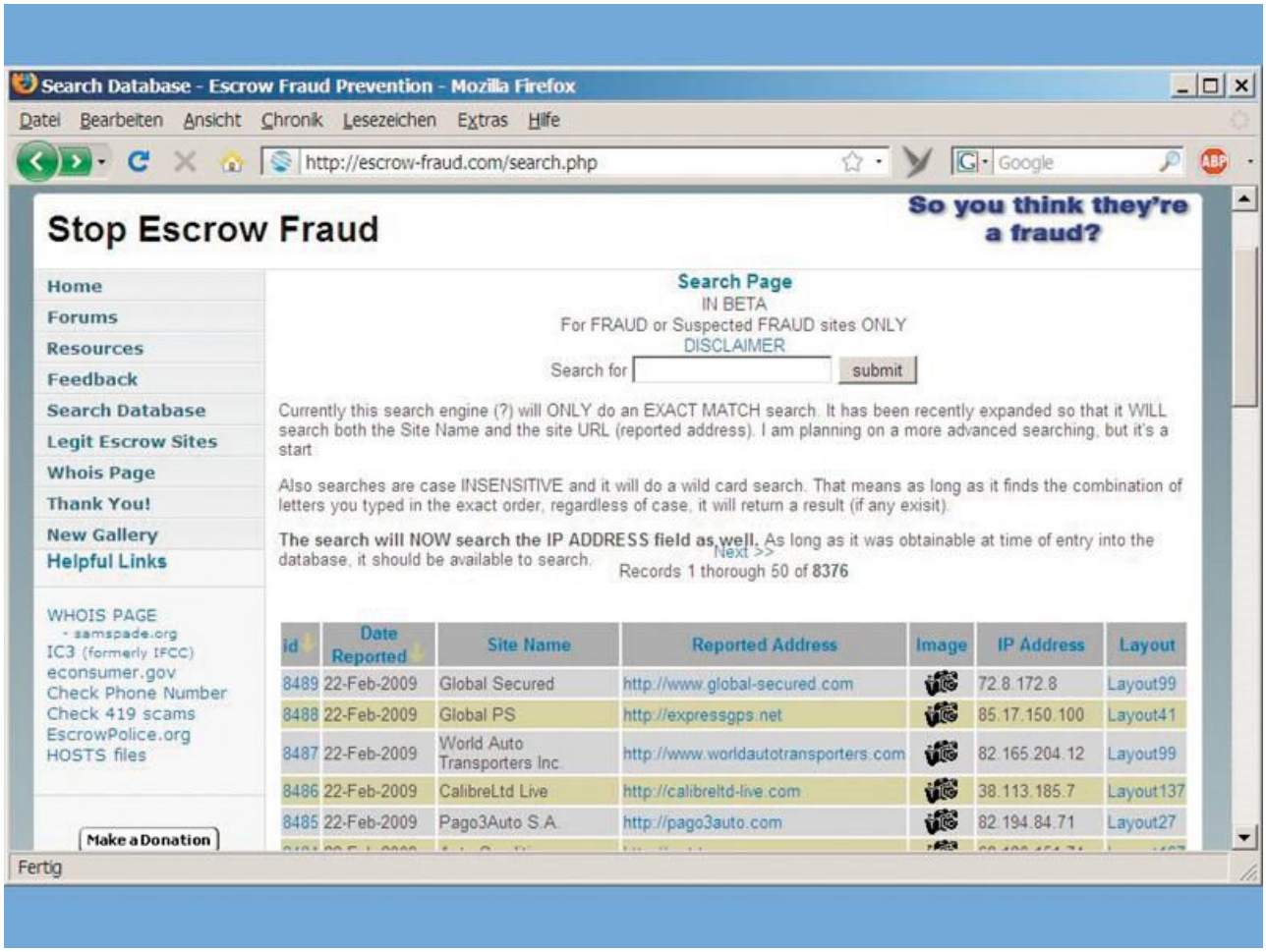
Es scheint einfach zu sein: Datei anklicken und herunterladen – per Filesharing-System oder per Direkt-Download. Doch es kommt vor, dass statt der kostenlosen Freischaltmöglichkeit für Bezahl-Software ein Trojaner auf der Festplatte landet. Wir haben das mit einem Key-Generator für eine teure Grafik-Software 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**[3], 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. Fehler: Sie geben persönliche Daten auf dubiosen Sites preis



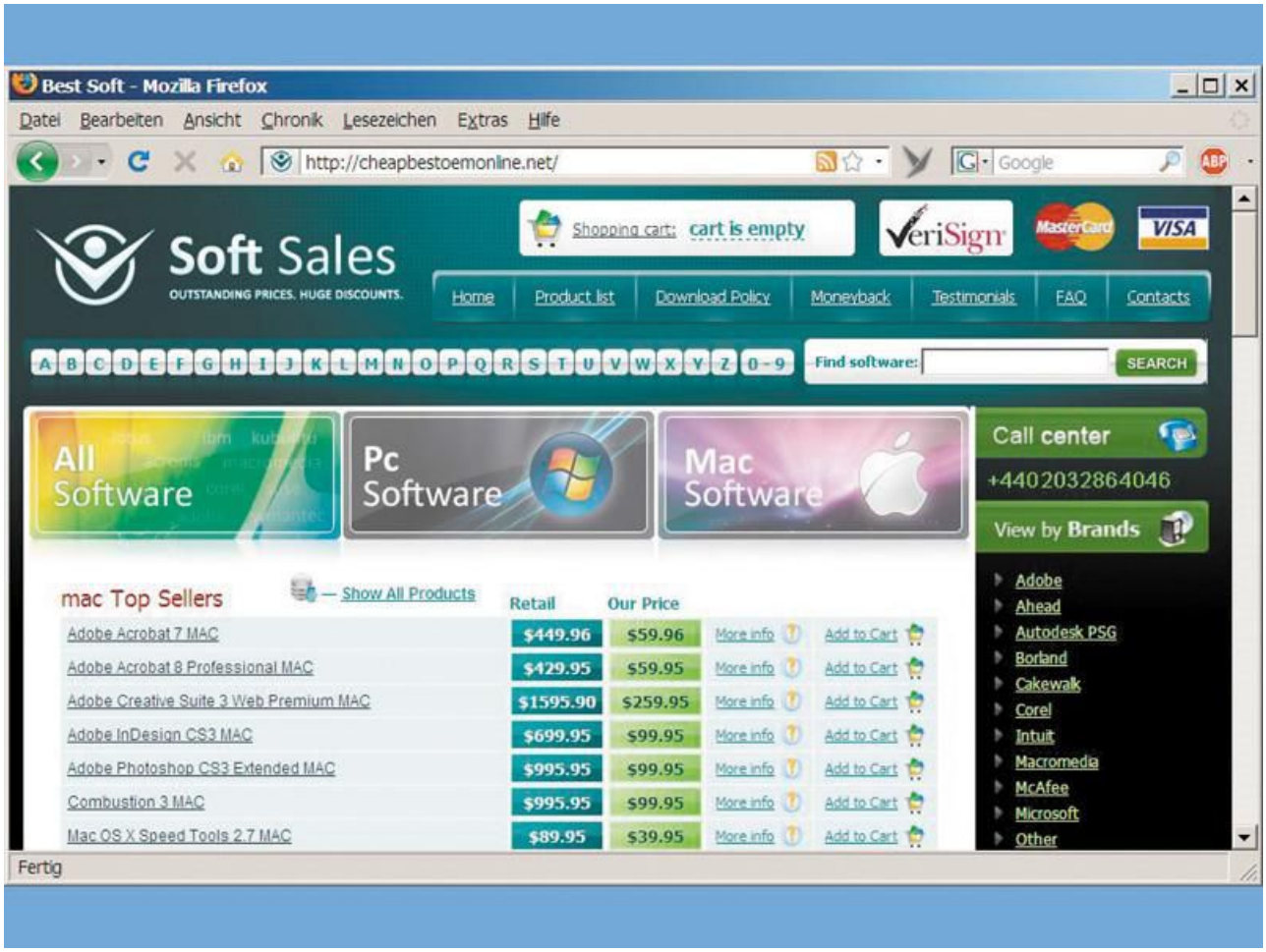
Auf seriösen Sites ist nichts dagegen einzuwenden, **persönliche Daten**[4] anzugeben – diese dienen im besten Fall nur der Kundenbindung und ermöglichen dem Anbieter eines Dienstes, Ihnen Zusatzinformationen zukommen zu lassen. Prüfen Sie, in welcher Form Ihre Daten verwendet werden. Selbst wenn in 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.

4. Fehler: Sie vertrauen den falschen Sites

Es



lohnt sich nicht, für Programme von dubiosen Download-Sites Geld auszugeben.

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

„Was tun bei einer Hausdurchsuchung?“ ist der Titel eines populären **E-Books**[5], 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**[6] 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. Fehler: 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**[7] ersteigerte Ware über Western Union oder **Moneygram**[8]. 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 bei **escrow-fraud**[9].

Tipp: Die Abwicklung über einen seriösen Treuhandservice kann gerade bei hochwertigen Waren sinnvoll sein. Bei Ebay-Geschäften sollten Sie unbedingt den **Ebay-Treuhandservice**[10] nutzen.

6. Fehler: Sie gehen auf allzu verlockende Angebote ein

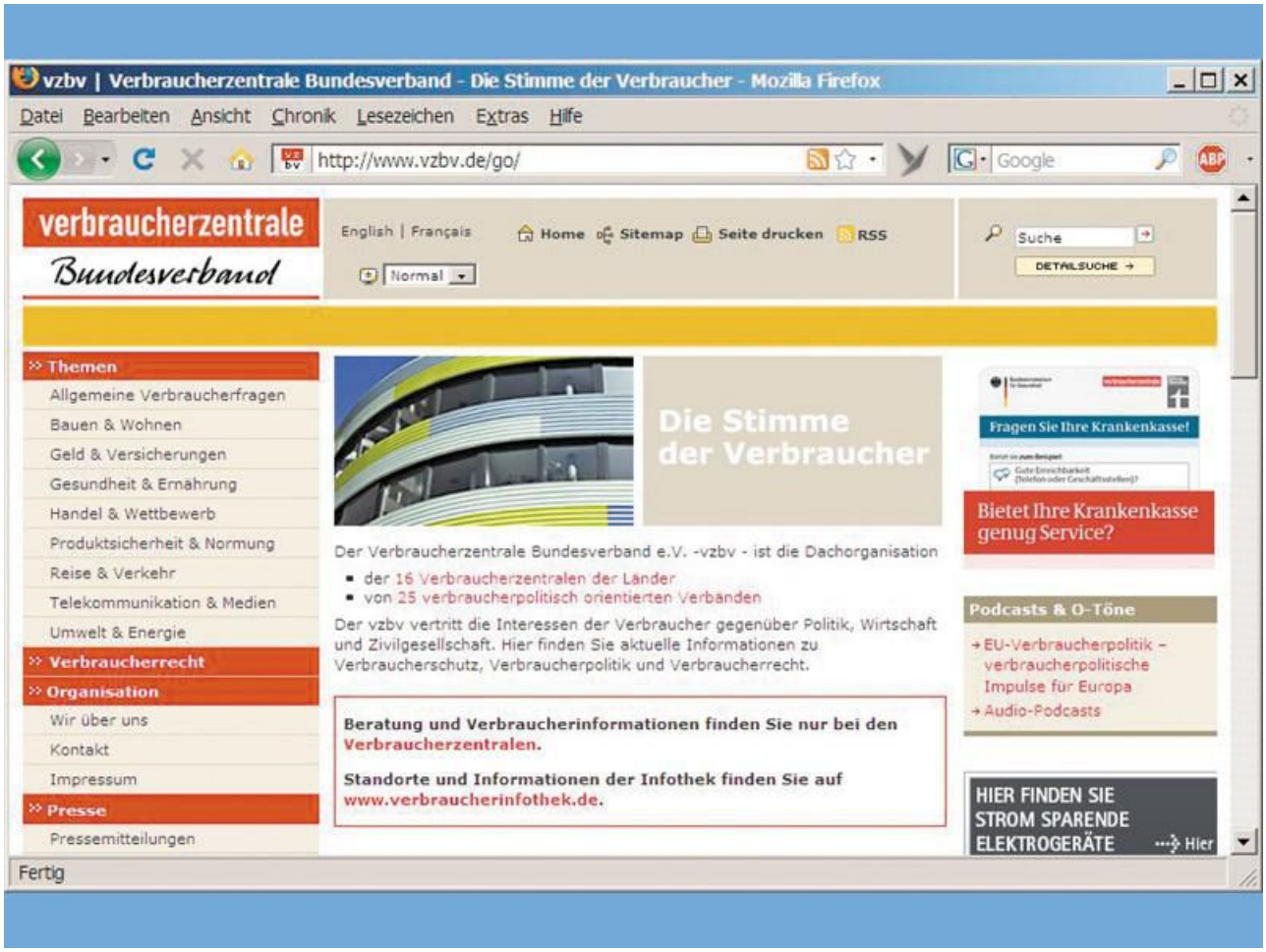
Im Internet kann jeder alles schreiben und versprechen. Für Sie als **Kunde**[11] ist es später oft schwierig bis unmöglich, das Versprochene einzufordern. Seien Sie daher nicht zu schnäppchenorientiert, und verlassen Sie sich auf Ihren gesunden Menschenverstand. Vor allem, wenn Sie finanziell in Vorleistung 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. Fehler: Sie kaufen Dinge aus illegalen oder unautorisierten Quellen



Auch die Verbraucherzentralen warnen vor Abzockern

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**[12], 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.

Links im Artikel:

[1] **https://www.computerwoche.de/schwerpunkt/b/Browser.html**
[2] **https://www.computerwoche.de/schwerpunkt/p/PC.html**
[3] **https://www.computerwoche.de/schwerpunkt/t/Tools.html**
[4] **https://www.computerwoche.de/schwerpunkt/d/Datenschutz.html**
[5] **https://www.computerwoche.de/schwerpunkt/e/E-Book.html**
[6] **https://www.computerwoche.de/schwerpunkt/w/Website.html**
[7] **https://www.computerwoche.de/schwerpunkt/e/ebay.html**
[8] **http://www.moneygram.de/**
[9] **http://www.escrow-fraud.com/**
[10] **http://pages.ebay.de/treuhandservice**
[11] **https://www.computerwoche.de/schwerpunkt/k/Kunde.html**
[12] **https://www.computerwoche.de/schwerpunkt/k/Kunde.html**
