

Internet-Fallen enttarnt

DIE

SCHWARZE LISTE DES INTERNETS

Im Internet werden Sie verführt, belogen und betrogen – wenn Sie nicht aufpassen. Lernen Sie die Maschen hinter scheinbar kostenlosen Websites, lukrativen Jobangeboten oder Kleinanzeigen kennen, um nicht darauf hereinzufallen.

Von **Hendrik Becker**

NEPPER, SCHLEPPER, BAUERNFÄNGER – sie lauern nicht nur im echten Leben, sondern auch im Web. Sie haben alle ein gemeinsames Interesse: Geld zu verdienen – an Ihnen. Die Methoden dazu sind höchst unterschiedlich. Die einen versuchen es ihren Opfern direkt aus der Tasche zu ziehen, andere verkaufen ihre Adressdaten weiter. Wieder andere verdienen daran, dass sie arglosen Anwendern Ad-/Spyware unterjubeln. Oder sie installieren Würmer, die eine Hintertür öffnen, über die sich der PC des Opfers fernsteuern lässt. Die Zugangsdaten zu diesen PCs verkaufen sie dann

meistbietend weiter, zum Beispiel an Firmen, die sie zum Spam-Versand missbrauchen. Im Folgenden zeigen wir die dreisten Methoden und geben Tipps zum Schutz. In der Liste auf Seite 130 haben wir exemplarisch einige schwarze Schafe aufgeführt.

Abzock-Sites

Abzock-Websites werben damit, Inhalte zu jeweils einem prominenten Thema zu bieten, etwa Tauschbörsen, Hausaufgaben, Kochrezepten, Ahnenforschung, Lehrstellen oder Kinder-Malvorlagen. Die Gestaltung der Websites erweckt bei vielen Anwendern

den Eindruck, als seien diese Inhalte nach vorheriger Registrierung mit Name und Adresse gratis. Doch wer seine Daten eintippt, erhält einige Wochen später eine Rechnung. Denn er habe, so der Inhalt des Begleitschreibens, ein Abo abgeschlossen – zahlbar für ein oder zwei Jahre im Voraus. Wer nicht zahlt, wird mit Mahnungen, Anwaltsschreiben und Briefen von Inkasso-Unternehmen überhäuft, was die Kosten – zumindest auf dem Papier – immer weiter nach oben treibt.

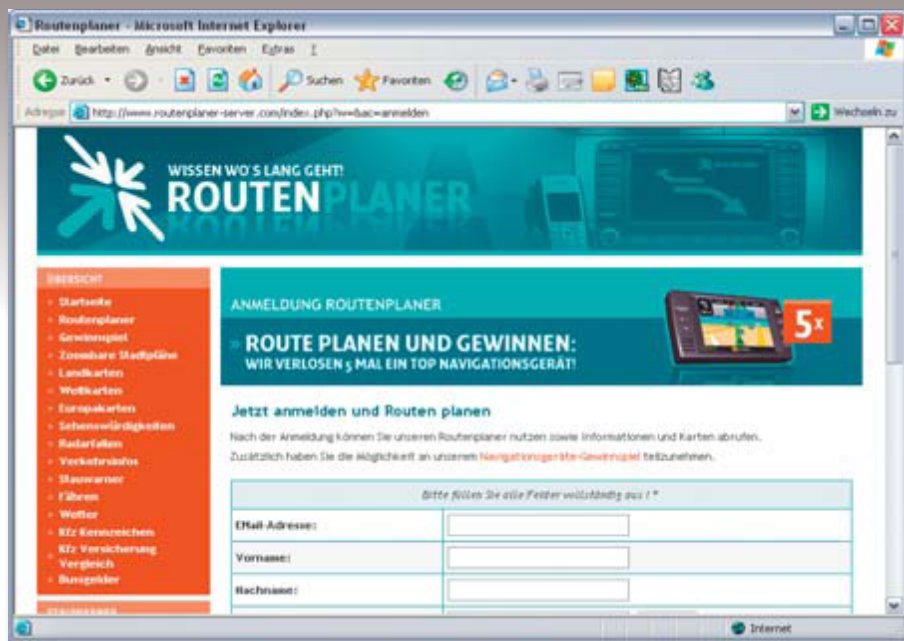
Betrug ist den Betreibern der meisten Abzock-Sites aus juristischer Sicht nicht



vorzuwerfen. Entsprechende Ermittlungen der Staatsanwaltschaft Frankfurt am Main gegen einen in diesem Bereich sehr aktiven Anbieter wurden eingestellt. Denn, so die Begründung, der Anwender erhält nach der Anmeldung ja tatsächlich Zugang zu Informationen. Dass diese Inhalte meist wenig wert sind und anderswo im Web frei verfügbar, ändert an der Sachlage nichts. Auch die Preisangaben sind vorhanden – zumindest, wenn man genau hinschaut. Die Praxis, die Preisinfo ganz tief unten auf der Seite zu verstecken, haben die meisten Anbieter auf Druck von Verbraucherzentralen inzwischen aufgegeben. Trotzdem tappt noch immer eine beträchtliche Zahl an Anwendern in die Abo-Falle. Das ist ein Indiz dafür, dass die Preisinformation noch immer nicht deutlich genug zu erkennen ist.

Wenn Sie Opfer einer Abzock-Website geworden sind und eine Rechnung erhalten, heißt es in erster Linie – Ruhe bewahren. Denn auch wenn es sich um keinen Betrug seitens des Anbieters handelt, so heißt das noch lange nicht, dass tatsächlich ein wirksamer Vertrag zustande gekommen ist.

Viele Anwälte sehen in der undurchsichtigen Preisangabe eine überraschende Klausel, mit der man als Web-Nutzer nicht rechnen muss. Daher hat man gute Karten, die Rechnung zivilrechtlich anzufechten. Aber das muss in der Regel nicht einmal sein. Uns ist kein Fall bekannt, in dem einer der Betreiber den ultimativen Weg eines gerichtlichen Mahnbescheids gewählt hat. Offenbar ist ihnen bewusst, auf welchem dünnem Eis sie sich bewegen. Außerdem scheuen sie die Öffentlichkeit. So lange Sie keinen gerichtlichen Mahnbescheid bekommen,



Beim Routenplaner neben der Adresse noch den Namen eintragen? Klar, man möchte ja am Gewinnspiel teilnehmen. Erst die Fußzeile verrät: Für den Dienst werden 59,95 Euro fällig

können Sie sich zurücklehnen und sämtliche Rechnungen und Mahnungen ignorieren. Auch die darin ausgesprochenen Drohungen sollten Sie sich nicht zu Herzen nehmen.

„Sie haben gute Karten, die Rechnung zivilrechtlich anzufechten“

Möchten Sie sich trotzdem rechtlich absichern, schicken Sie ein Einschreiben an das Unternehmen, in dem Sie den Vertrag an-

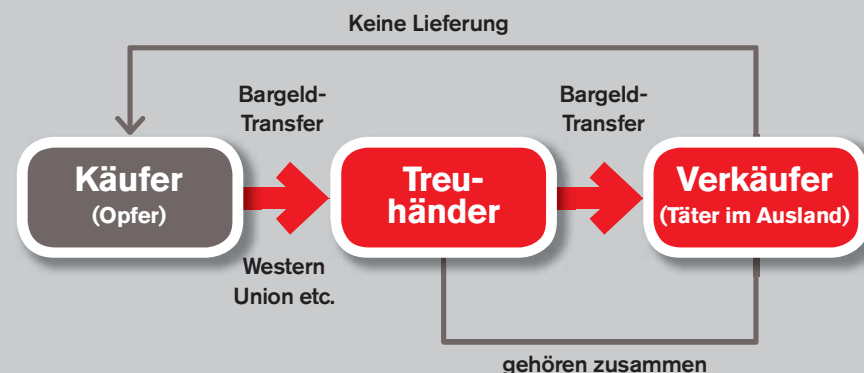
fechten. **Einen entsprechenden Musterbrief** bietet die Verbraucherzentrale Nordrhein-Westfalen zum Download an. Sie erhalten ihn über www.pcwelt.de/5be (auch auf CD/DVD, 13 KB). Ändern Sie nicht die vorgegebenen Formulierungen, und machen Sie auch keine zusätzlichen Angaben.

Wichtig: Wenn Sie die zweifelhafte Rechnung bereits bezahlt haben, werden Sie Ihr Geld kaum zurückfordern können. Der Anbieter würde sich darauf berufen, dass Sie durch die Zahlung die Vertragsbedingungen akzeptiert haben.

Um **gar nicht erst in eine Abo-Falle zu tappen**, gilt es beim Surfen im Web, wachsam zu sein, ein gesundes Misstrauen an den Tag zu legen – und dies auch anderen Benutzern Ihres Internet-Zugangs einzuimpfen. Vorsicht ist vor allem immer dann geboten, wenn die Eingabe von persönlichen Daten verlangt wird. Bei einer angeblichen Informationsseite zum Thema Filesharing erscheint das noch einleuchtend. Bei einer Website, die ein Gewinnspiel offeriert, schon weniger. Wenn diese nicht eindeutig von einem seriösen Unternehmen betrieben wird, das Ihnen bekannt ist, durchsuchen Sie die Seite akribisch nach Kleingedrucktem. Auch in den Allgemeinen Geschäftsbedingungen (AGB), die Sie in aller Regel per Klick auf ein Kontrollkästchen abnicken müssen, können überraschende Klauseln verborgen sein.

AUTO-ABZOCKE So werden Sie übers Ohr gehauen (Seite 131)

Der Weg des Geldes: Der Autokäufer übermittelt das Geld per Bartransfer an den angeblichen Treuhänder, bekommt im Gegenzug aber kein Auto geliefert



➤ Gewinnspiel mit Nachspiel

Gewinnspiele im Web sind beliebt. Bei Anwendern, weil sie ohne viel Mühe und ohne Portokosten die Chance auf wertvolle Produkte haben. Bei Unternehmen, weil sie damit publikumswirksam ihre Produkte in Szene setzen können. Und bei Betrügern & Spammern, **die die Popularität von Gewinnspielen schamlos ausnutzen**, um auf ihre Weise davon zu profitieren. Eine Masche haben wir bereits im vorhergehenden Punkt geschildert: Gewinnspiele, die sich beim genaueren Hinsehen als Abonnement für einen Zugang zu oft minderwertigen Informationen entpuppen.

Ein anderer Trick zielt nicht direkt auf das Portemonnaie des Anwenders, sondern auf seine Adresse. In den Teilnahmebedingungen oder den Datenschutzbestimmungen, die kaum ein Anwender liest, steht dann, dass die eingegebenen Daten für Werbemaßnahmen an Partnerunternehmen weitergegeben werden. Manch ein Anbieter listet im Kleingedruckten sogar unverhohlen ein knappes Dutzend Firmen auf, die Sie in Zukunft nach Belieben **per Post und Mail zusammentreiben** dürfen. Ob die angesprochenen Gewinne, die die Anbieter im Gegenzug versprechen, tatsächlich jemals verlost werden, steht in den Sternen.

Sollten Sie an einem zweifelhaften Gewinnspiel teilgenommen haben, genügt es in der Regel, dem Anbieter eine Mail mit folgendem Satz zu schicken: „Hiermit widerspreche ich der Nutzung meiner Daten durch Sie und durch Ihre Partnerunternehmen für Marketingzwecke.“ In ihren gesetzlich vorgeschriebenen Datenschutzbestimmungen verpflichten sich die Anbieter, diesem Widerspruch unverzüglich nachzukommen.

(Zu) gute Jobangebote

3000 Euro oder mehr als „Nebenverdienst“ für zwei bis acht Stunden Arbeit pro Woche? Klingt gut – zu gut, um seriös zu sein. Trotzdem gibt es genügend Anwender, die auf solche Angebote eingehen, welche per Mail ins Postfach flattern. Gesucht werden **„Finanzagenten“** oder auch „Regional Manager für Zahlungsbearbeitung“. Die Voraussetzungen sind gering: Internet und Mailkenntnisse reichen aus. Genau, pünktlich und zuverlässig sollte man sein – aber wer würde das nicht von sich behaupten. Ach ja: Einen Homebanking-Zugang bei einer deutschen Bank sollte man haben. **Spätestens hier sollte man stutzig werden.** Denn welche seriöse Firma lässt Finanztransaktionen über die Privatkonten ihrer Mitarbeiter laufen?

Bei diesem Jobangebot geht es schlicht und ergreifend um **Geldwäsche**. Die Hintermänner kapern fremde Bankkonten und überweisen das Guthaben an den arglosen Finanzagenten. Oder sie geben dessen Kontonummer bei krummen Geschäften wie fingierten Autoverkäufen an (Seite 131). Sobald das Geld auf dem Konto des Finanzagenten angekommen ist, muss dieser es als Bargeldtransfer bei Diensten wie Western Union anweisen. An dieser Stelle verlieren sich dann die Spuren des Geldes. Die Hintermänner können es irgendwo im Ausland faktisch anonym abheben.

Kommt der Agent seiner Aufgabe nicht unverzüglich nach, wird er von den Hintermännern **stark unter Druck gesetzt**. Denn Zeit ist für sie Geld – im wahrsten Sinne des Wortes. Sobald die geprellten Kunden bemerken, was ihnen widerfahren ist, werden sie oder die hinzugezogene Polizei sich an den unmittelbaren Empfänger des Geldes wenden, also an den Finanzagenten. Hat dieser die Beute bereits an die Betrüger weitergeleitet, muss laut aktueller Rechtsprechung er dafür gerade stehen.

SCHWARZE LISTE DES INTERNETS (Beispiele)

Abo-Fallen

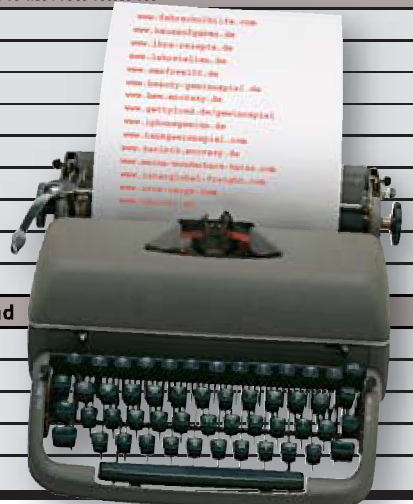
www.basteln-heute.com	2 Jahre Zugriff auf Bastelanleitungen etc. für 168 Euro
www.condome.tv	Auf ein Gratis-Kondom folgen 12 Monate lang jeweils weitere 12 Stück für jährlich 96 Euro.
www.fahrschulhilfe.com	99 Euro für eine simulierte Theorieprüfung
www.filmefabrik.com	239,40 Euro pro Jahr für einen zweiwöchentlichen Newsletter mit Filminfos und eine monatliche DVD
www.genealogie.de	Einjähriger Zugriff auf Ahnenforschungs-Datenbank für einmalig 60 Euro
www.hausaufgaben.de	Zweijähriger Zugriff auf vorgefertigte Hausaufgaben für 168 Euro
www.ihre-rezepte.de	84,80 Euro für einjährigen Zugriff auf Rezept-Datenbank
www.lebenscheck.com	99 Euro für eine Berechnung der Lebenserwartung
www.lehrstellen.de	Zweijähriger Zugriff, unter anderem auf „Berufsbilder mit Beschreibung“, für 168 Euro
www.meine-wunderbare-katze.com	Infos über Katzen für 84 Euro im Jahr
www.p2p-heute.com	2 Jahre Zugriff auf Anleitungen, Programme und Tools zum Thema Filesharing für 168 Euro
www.paywin.de	96 Euro pro Jahr für Warenproben und Gutscheine
www.routenplaner-server.com	Drei-Monats-Zugang zu einem Routenplaner für 59,95 Euro
www.smsfree100.de	Zwei Jahre lang jeden Monat 100 SMS versenden für 198 Euro

Gewinnspiele mit Datenweitergabe an Partnerunternehmen

www.beauty-gewinnspiel.de
www.bmw.mccrazy.de
www.citytripgewinnen.de
www.gettyload.de/gewinnspiel
www.iphonegewinn.de
www.iwin.de
www.karibik.mccrazy.de
www.tankgewinnspiel.com
www.z4-gewinner.de

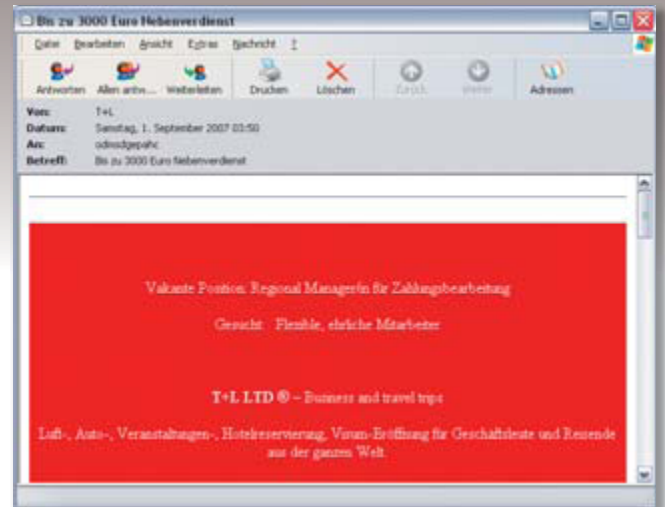
Treuhanddienste, die negativ aufgefallen sind

www.globaltrans-speditions.net.tc
www.interglobal-freight.com
www.iszexpres.com
www.tdc-cil.eu
www.vrox-cargo.com





Wie im Rausch: Von der Gewinnchance geblendet, lesen sich viele Anwender die Teilnahmebedingungen nicht durch



3000 Euro Nebenverdienst als Manager für Zahlungsbearbeitung: Dass es sich dabei um Geldwäsche handelt, verschweigt der Absender

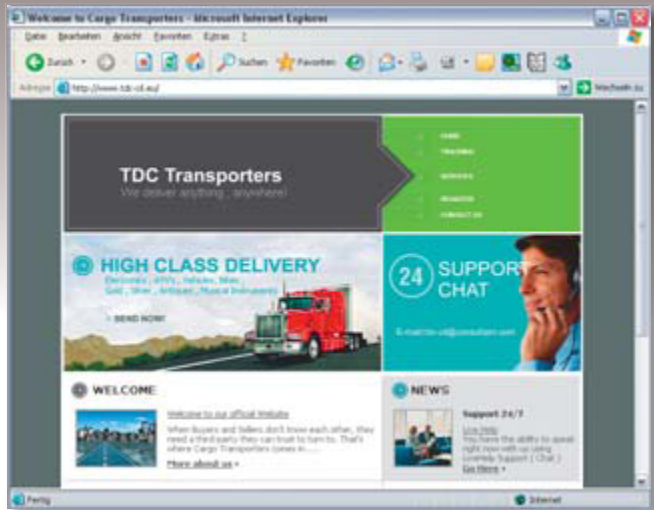
Zudem riskiert er eine Anzeige wegen Mit-täterschaft.

Vermeintliche Auto-Schnäppchen

Ein zwei Jahre alter Golf mit 25.000 Kilo-metern auf dem Tacho für gerade mal 7500 Euro? Das klingt nach einem echten Schnäppchen. Doch hinter solchen Annon-

cen bei Anzeigenbörsen wie Autoscout24.de oder Mobile.de stecken nur selten uner-fahrene Autobesitzer, die nicht wissen, was ihr Wagen wirklich wert ist. In der Regel geben professionelle Betrüger solche Anzei-gen auf, um Autos zu verkaufen, die es gar nicht gibt. Genau genommen gibt es sie schon, denn natürlich präsentieren die

Händler ihre Wagen mit Fotos. **Aber sie gehören ihnen in der Regel nicht** und werden die arglosen Käufer auch nie errei-chen. Doch wie schaffen es die Betrüger, den Interessenten ohne Gegenleistung Geld aus der Tasche zu ziehen und anschließend auf Nimmerwiedersehen zu verschwinden? Wie im richtigen Leben ist auch im Internet ➤



Blender: Hinter solchen Treuhänder-Diensten stecken oft die Verkäufer selbst. Die professionelle Website soll den Käufer in Sicherheit wiegen



McAfee Site Advisor: Das Tool für Firefox und den Internet Explorer warnt Sie vor betrügerischen Websites – allerdings nicht zuverlässig

➤ dazu eine gehörige Portion Psychologie nötig, außerdem **Überzeugungskraft gepaart mit Dreistigkeit**.

Am Anfang steht die Anzeige. Sie ist gut, aber nicht übertrieben professionell gestaltet. Die Fotos zeigen das beschriebene Auto im makellosen Zustand. Am wichtigsten ist jedoch der Preis: Er liegt deutlich unterhalb des Marktwerts – aber nicht zu extrem. Denn sonst würden Interessenten misstrauisch werden. Die erste Kontaktaufnahme des Käufers nutzt der Verkäufer, um ihn in Sicherheit zu wiegen. Er zählt noch mal alle Vorteile und den guten Zustand des Wagens auf. Sollte der Interessent wegen des günstigen Preises nachfragen, so erhält er eine Antwort wie „Ich benötige das Geld dringend und verkaufe den Wagen daher lieber etwas günstiger. Sie haben übrigens Glück. Ich habe die Anzeige gerade erst eingestellt, und Sie sind der erste Anrufer.“ Mit diesem Argument zufrieden und gleichzeitig auch unter Zeitdruck gestellt, willigt so mancher Anrufer schließlich in das Geschäft ein – und das, ohne das Auto je gesehen zu haben.

Nahezu beiläufig erzählt der Verkäufer im weiteren Gespräch, dass sich der Wagen gerade im Ausland bei einem Freund befindet. Aber das sei überhaupt kein Problem. Er kenne da einen **zuverlässigen Treuhänderservice**, der sich um die Abwicklung kümmert. Nach Überweisung des Kaufbetrags auf das Treuhänderkonto würde der Wagen abgeholt und zugestellt werden. Erst, nachdem der Empfänger die Lieferung quittiert hätte, würde der Treuhänder dem Verkäufer das Geld aushändigen, an-

sonsten erhält der Käufer es zurück. „Sie haben also gar kein Risiko.“ Derart überzeugt, tauschen beide Gesprächspartner ihre Adressen aus.

Wenige Tage später erhält der Käufer per Mail eine Zahlungsaufforderung des Treuhänders. Kunden, die sich durch einen Blick auf die Homepage des Dienstleisters von seiner Seriosität überzeugen wollen, finden eine professionell gestaltete Website vor. Wer nun das Geld überweist, ist **auf die**

„Geldtransfers per Western Union lassen sich quasi anonym abwickeln“

Masche der Betrüger hereingefallen.

Das Auto wird er nie bekommen, und seine Beschwerden beim Treuhänder werden ins Leere laufen. Denn genauso wie der Wagen ist auch der Dienstleister eine Luftnummer, hinter der der Betrüger selbst oder ein Komplize steckt.

Das Geld ist weg: Hat der angebliche Treuhänder den Kunden angewiesen, das Geld bar per Western Union zu transferieren, ist er sein Geld an Sicherheit grenzender Wahrscheinlichkeit los. Denn solcherlei Geldtransfers lassen sich quasi anonym abwickeln. Etwas besser stehen die Chancen bei der Überweisung ins Inland. Dann wird das Geld bei einem arglosen Menschen gelandet sein, den die Betrüger unter Vorspiegelung falscher Tatsachen als Finanzagenten angeheuert haben. Theoretisch können sie

von ihm das Geld zurückzufordern, auch wenn er es schon abzüglich seiner Provision per Western Union an die Betrüger weitergeleitet hat (Seite 130). Den Schaden hat dann er zu tragen, und er muss mit einer Anzeige rechnen. Bei jemandem, der auf ein solch dubioses Jobangebot eingegangen ist, gibt es aber oft nicht viel zu holen. Eine Liste von Treuhanddiensten, die negativ aufgefallen sind, finden Sie unter **www.escrow-fraud.com** (Auszüge auf Seite 130).

Der Trick funktioniert auch andersrum:

Sie inserieren ein Auto und erhalten einen Anruf oder eine Mail von einem Interessenten, der den Wagen unbedingt haben möchte. Er könne aber nicht selbst vorbeikommen, sondern schicke einen Abholservice. Bei der Übergabe erhalten Sie kein Bargeld, sondern einen Scheck – der jedoch ungedeckt ist, wie sich später herausstellt. Oder der Käufer überweist Ihnen das Geld – allerdings nicht von seinem Konto, sondern von einem gekaperten eines Unbeteiligten. Der wird sein Geld von Ihnen zurückfordern, sobald er den Diebstahl bemerkt.

Gegenmaßnahmen

Einen zuverlässigen automatischen Schutz vor Betrug & Abzocke gibt es nicht. Zumindest ansatzweise kann Sie der kostenlose **McAfee Site Advisor** vor Internet-Fallen bewahren (auf CD/DVD und unter **www.siteadvisor.de** und **www.pcwelt.de**, 1,7 MB). Er integriert sich in den Internet Explorer und in Firefox und warnt vor einigen, aber längst nicht vor allen betrügerischen Websites.