Die dunkle Seite des Internets

Im Internet werden Sie verführt, belogen und betrogen – wenn Sie nicht aufpassen. Durchschauen Sie die Maschen hinter scheinbar kostenlosen Diensten, lukrativen Jobangeboten und verlockenden Kleinanzeigen, und schützen Sie sich.

Von **Hendrik Becker** und **Tobias Weidemann**

Gewinnspiele mit Datenklau, Routenplaner mit kostenpflichtigem Abo, Schnäppchen, bei denen Sie draufzahlen: Trickser und Ganoven im Internet wollen leichtes Geld an Ihnen verdienen. Wir zeigen die dreisten Methoden und geben Tipps, wie Sie sich schützen.

Abzock-Sites: Wertlose Inhalte zu horrenden Abogebühren

Abzock-Websites werben damit, Inhalte zu jeweils einem prominenten Thema zu bieten. Die Palette reicht von Filmen und Musik-Downloads über Hausaufgaben und Referate bis zu Kochrezepten, Ahnenforschung, Lehrstellen oder Kinder-Malvorlagen. Die Gestaltung der Websites erweckt bei vielen Anwendern den Eindruck, diese Inhalte seien gratis. Doch um Zugang zu bekommen, muss man sich mit Name und Adresse registrieren. Wer seine Daten einträgt, 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 formaljuristischer Sicht nicht vorzuwerfen. Entsprechende Ermittlungen der Staatsanwaltschaft Frankfurt am Main gegen einen in diesem Bereich sehr aktiven Anbieter wurden eingestellt. In anderen Fällen wurde zu Gunsten des Kunden entschieden, der dann nicht zahlen musste.

Vorsicht bei gewerblichen Mailadressen: Einige Gerichte wiederum urteilen, ein Vertrag sei sehr wohl zustande gekommen. Auch wenn der Hinweis auf die Kosten etwas schwer aufzufinden sei, sei er dennoch vorhanden. In einem Fall, der kürzlich vor dem Amtsgericht Mülheim verhandelt wurde (AZ 1C39/09), hatte der Kunde seine gewerbliche Mailadresse und einen gewerblichen Briefkopf benutzt. Deshalb ging das Gericht nicht von einem Privatanwender aus und entschied gegen den Kunden.

Widerruf oft nicht möglich: Ein Kündigungsrecht steht dem Kunden in solchen Fällen oft nur zu, wenn der Betreiber der Site nicht schon auf Wunsch des Kunden mit der Bereitstellung der Leistung begonnen hat. Das ist aber fast immer der Fall, da der Betreiber der Site dem Kunden sofort Zugang zu den gewünschten Leistungen gewährt. Allerdings darf, das haben die Gerichte zu Gunsten der Verbraucher entschieden, das Widerrufsrecht nicht per se ausgeschlossen werden – dies benachteiligt den Kunden unverhältnismäßig.

Wertlose Inhalte: Dass die Inhalte auf solchen Abzock-Sites meist wenig wert und anderswo im Web frei verfügbar sind, ändert am eigentlichen Problem 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 von Anwendern in die Abo-Falle. Das ist ein Indiz dafür, dass die Preisinformation noch immer nicht deutlich genug zu erkennen ist.

Fazit: Auch in Zukunft wird es auf den Einzelfall ankommen – und darauf, wie vertraut ein Richter mit derartigen Geschäftspraktiken ist und wie er diese beurteilt. Sicher ist: Ärger steht einem Anwender erst ins Haus, wenn der Betreiber die vermeintlichen Schulden einklagt. Dazu sind viele Unternehmen trotz anders lautender Drohungen nicht bereit. Schließlich haben sie kein Interesse daran, dass ihre Methoden vor einem Gericht und in der Öffentlichkeit auf den Prüfstand kommen.

Opfer von Abo-Fallen: Nicht immer ist ein Anwalt nötig

Wenn Sie Opfer einer Abzock-Website geworden sind und eine Rechnung (möglicherweise auch Mahnungen und Zahlungsaufforderungen) erhalten haben, heißt es in erster Linie: Ruhe bewahren. Denn es ist noch lange nicht klar, ob tatsächlich ein wirksamer Vertrag zustande gekommen ist.

Mahnungen zunächst ignorieren: Viele Anwälte sehen in der undurchsichtigen Preisangabe eine überraschende Klausel, mit der man als Web-Nutzer nicht rechnen muss. Wer die Rechnung zivilrechtlich anfechten will, hat daher gute Karten. So lange Sie keinen gerichtlichen Mahnbescheid bekommen, können Sie sämtliche Drohungen und Mahnungen ignorieren.

Vertrag anfechten: Möchten Sie sich rechtlich absichern, schicken Sie ein Einschreiben an das Unternehmen, in dem Sie den Vertrag anfechten. Einen entsprechenden Musterbrief bietet die Verbraucherzentrale Nordrhein-Westfalen zum Download an (*www.vz-nrw.de/link462161A.html*). Ändern Sie die vorgegebenen Formulierungen nicht, und machen Sie auch keine zusätzlichen Angaben.

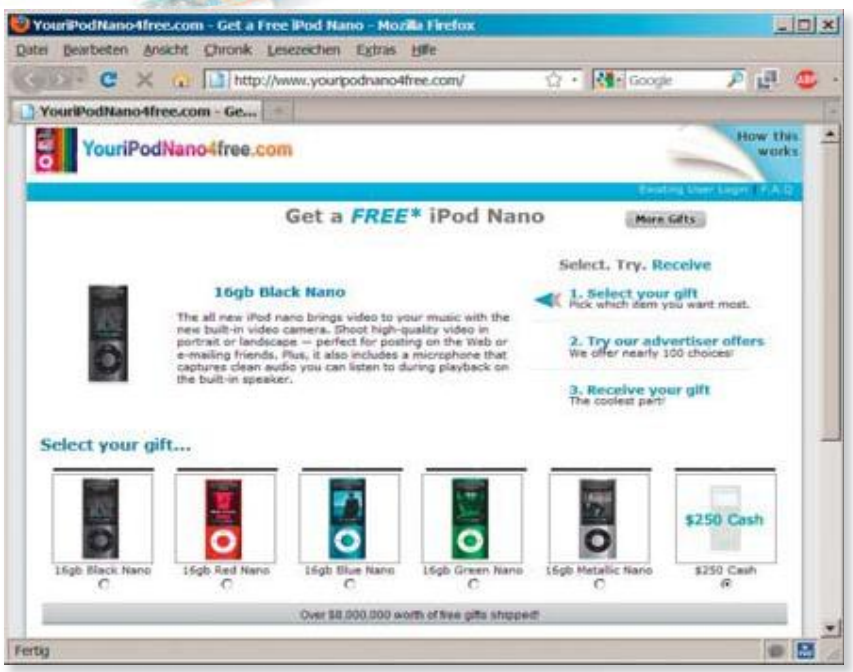
Wichtig: Wenn Sie die zweifelhafte Rechnung bereits bezahlt haben, werden Sie Ihr Geld kaum zurückfordern können, da die Rechnung damit anerkannt wird.

Gesundes Misstrauen schützt: Um gar nicht erst in eine Abo-Falle zu tappen, sollten Sie beim Surfen immer ein gesundes Misstrauen an den Tag legen. Impfen Sie das auch den Mitbenutzern Ihres Internet-Zugangs ein. Vorsicht ist vor allem geboten, wenn Sie Ihre persönlichen Daten eingeben sollen. Bei einer angeblichen Infoseite zum Thema Filesharing erscheint das ebenso wenig einleuchtend wie bei einer Website, die ein Gewinnspiel offeriert oder mit Kochrezepten oder Rätseln lockt. Wenn eine solche Site nicht eindeutig von einem seriösen Unternehmen betrieben wird, das Sie kennen, durchsuchen Sie die Seiten 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. Prüfen Sie außerdem, ob sich über das Unternehmen und die Site Beschwerden in Foren finden.

Gewinnspiel mit Nachspiel: Ihre persönlichen Daten werden verkauft

Gewinnspiele im Web sind beliebt: Anwender haben ohne viel Mühe und Portokosten die Chance auf wertvolle Produkte, und Unternehmen können ihre Produkte publik machen. Doch Betrüger und Spammer nutzen die Popularität solcher Werbemaßnahmen schamlos aus. So manches Gewinnspiel entpuppt sich bei genauerem Hinsehen als Abonnement für einen Zugang zu minderwertigen Informationen. Damit variieren die Anbieter eine Masche, die wir im vorhergehenden Punkt vorgestellt haben.

Hilfreiche Musterbriefe: Die Verbraucherzentrale Nordrhein-Westfalen bietet umfangreiche Informationen zum Thema Internet-Abzocke sowie Musterbriefe, mit denen Sie sich wehren können



Gibt's den iPod wirklich kostenlos? Bei solchen Angeboten zahlen Sie auf Umwegen, etwa indem Sie Ihre Adresse und Ihre persönlichen Daten preisgeben müssen

Wertvolle persönliche Daten: Zahlen mit dem guten Namen

Ein anderer Trick zielt auf persönliche Daten des Anwenders, die ebenfalls bares Geld wert sein können. 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 offen ein knappes Dutzend Firmen auf, die Sie in Zukunft nach Belieben per Post und Mail mit Werbung und Produktinformationen versorgen dürfen.

Ob die Gewinne, die die Anbieter im Gegenzug versprechen, tatsächlich jemals verlost werden, steht in den Sternen. Und selbst wenn tatsächlich Anwender etwas bekommen – in vielen Fällen hat sich das Geschäft für die Anbieter gelohnt. Ein iPod oder ein Notebook sind deutlich günstiger zu haben als hunderte oder tausende Adressen.

Werbemails unterbinden: 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." Dies sollten Sie mit der Absenderadresse tun, mit der Sie bei dem Dienst gemeldet sind, damit der Betreiber Sie zuordnen kann. Die gesetzlich vorgeschriebenen Datenschutzbestimmungen verpflichten die Anbieter, diesem Widerspruch unverzüglich nachzukommen. Falls Sie bereits Werbemails erhalten, finden Sie in der Regel einen Link am Ende der Mail, über den Sie sich aus dem Verteiler löschen lassen können.

iPhone oder iPod gratis: Doch oft gehen die Leute leer aus

In eine ähnliche Richtung geht eine Masche, die an Schneeballsysteme per Brief erinnert, wie sie in den 80er- und 90er-Jahren bekannt waren. Sie melden sich an bei einem Dienst wie *www.yourfreeiphone.com* oder *www.YourPS34Free.com*, der Ihnen für eine bestimmte Zahl von Anmeldungen Ihrer Freunde und Bekannten kostenlos einen iPod, ein iPhone oder ein Notebook verspricht. Sie müssen sich auf der Site noch für eine andere kostenlose Dienstleistung entscheiden, entweder ein Probe-Abo, eine Beratung in Geldfragen oder eine Anmeldung bei einer weiteren Site. Dafür kassiert der Betreiber der Get-free-Site einen kleineren Geldbetrag, über den er Ihre Sachprämie finanziert.

Schneeballprinzip: Danach sollen Sie die Namen und Mailadressen der Leute angeben, die Sie ebenfalls zum Mitmachen animieren wollen. Alle erhalten einen persönlichen Link, über den das System weiß, auf welchem Weg ein Kunde dazugekommen ist. Wenn sich genügend Ihrer Freunde und Bekannten registrieren, kann der Dienst deren persönliche Daten ebenfalls weiterverkaufen.

Zwei Haken hat das Ganze: Sie können erstens nicht nachvollziehen, ob der Dienst fair spielt und Sie Ihre Prämie wirklich bekommen werden. Zweitens kommt etwa beim iPhone natürlich ein Vertrag mit Kosten auf Sie zu.

(Zu) gute Jobangebote: Dubioser Nebenverdienst

3000 Euro oder mehr als „Nebenverdienst" für zwei bis acht Stunden Arbeit pro Woche? Klingt gut – zu gut, um seriös zu sein. Trotzdem gehen genügend Anwender auf solche Angebote ein, die per Mail ins Haus flattern. Gesucht werden „Finanzagenten" oder auch „Regional Manager für Zahlungsbearbeitung". Vorausgesetzt werden ein Mailkonto sowie Genauigkeit, Pünktlichkeit und Zuverlässigkeit – aber wer würde das nicht von sich behaupten? Einen Homebanking-Zugang bei einer deutschen Bank braucht man ebenfalls. Spätestens hier sollte man stutzig werden. Denn welche seriöse Firma lässt Finanztransaktionen über die Privatkonten ihrer Mitarbeiter statt über ein eigenes Konto laufen?

Mittelsmann für Betrugsdelikte: 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 an, etwa fingierten Autoverkäufen. Sobald das Geld auf dem Konto des Finanzagenten eingegangen ist, muss der es als Bargeldtransfer bei Diensten wie Western Union anweisen. An dieser Stelle verlieren sich dann die Spuren des Geldes. Denn anders als bei anderen Zahlungswegen lassen sich Western-Union-Zahlungen in vielen Fällen irgendwo im Ausland faktisch anonym in Empfang nehmen.

Finanzagent muss haften: Kommt der Agent seiner Aufgabe nicht unverzüglich nach, setzen ihn die Hintermänner stark unter Druck. Sobald die Opfer bemerken, was ihnen widerfahren ist, werden sie oder ›

Ein Angebot, das Sie ausschlagen sollten: In Kleinanzeigen und Spam-Mails suchen dubiose Firmen nach Finanzagenten. Wer sich darauf einlässt, bekommt meist Ärger mit geprellten Anwendern

die hinzugezogene Polizei sich an den unmittelbaren Empfänger des Geldes wenden, an den Finanzagenten. Hat er die Beute bereits an die Betrüger weitergeleitet, muss er laut aktueller Rechtsprechung dafür geradestehen und riskiert eine Anzeige wegen Mittäterschaft. Unabhängig von der Schuldfrage werden sich die ermittelnden Behörden zunächst an den Mittelsmann halten, da dieser die einzige Verbindung zu den Tätern darstellt.

Auto-Schnäppchen: Trickserei mit Treuhandkonto

Ein zwei Jahre alter Golf mit 25.000 Kilometern für gerade mal 7500 Euro? Das klingt nach einem echten Schnäppchen. Doch hinter solchen Annoncen bei Anzeigenbörsen wie Autoscout24.de oder Mobile.de stecken nur selten Autobesitzer, die sich nicht im Klaren darüber sind, was ihr Fahrzeug wirklich wert ist. In der Regel geben professionelle Betrüger solche Anzeigen auf, um Autos zu verkaufen, die es gar nicht gibt. Natürlich präsentieren die Verkäufer auf etlichen Fotos die Wagen. Aber sie gehören ihnen in der Regel nicht und werden die arglosen Käufer auch nie erreichen. Doch wie schaffen es die Betrüger, den Interessenten ohne Gegenleistung Geld aus der Tasche zu ziehen und anschließend auf Nimmerwiedersehen zu verschwinden?

Am Anfang steht die Annonce: Die Anzeige ist gut, aber nicht übertrieben professionell gestaltet. Die Fotos zeigen das beschriebene Auto in einem makellosen Zustand. Am wichtigsten ist jedoch der Preis: Er liegt unter dem Marktwert – zwar deutlich, aber nicht zu extrem. Andernfalls werden die Interessenten misstrauisch. Beim ersten Kontakt zählt der Verkäufer noch einmal alle Vorteile des Wagens auf. Fragt der Interessent wegen des günstigen Preises nach, 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." So mancher Anrufer gibt sich mit dieser Begründung zufrieden. Er sieht sich zudem unter Zugzwang und willigt in das Geschäft ein – ohne das Auto je gesehen zu haben.

Vermeintliche Sicherheit: Im weiteren Gespräch erzählt der Verkäufer beiläufig, 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 überführt werden. Erst nachdem der Empfänger die Lieferung quittiert habe, würde der Treuhänder dem Verkäufer das Geld aushändigen, ansonsten erhalte der Käufer es zurück. „Sie haben also gar kein Risiko." Wenn der Käufer nun überzeugt ist, tauschen die beiden Adressen aus.

Wenige Tage später erhält der Käufer per Mail eine Zahlungsaufforderung des Treuhänders. Wer sich von der Seriosität des Dienstleisters überzeugen will, findet eine professionell gestaltete Website vor. Sobald ein Kunde das Geld dorthin überweist, ist er endgültig auf die Masche der Betrüger hereingefallen. Das Auto wird er nie bekommen, und seine Beschwerden beim Treuhänder werden ins Leere laufen, wenn die Site dann überhaupt noch erreichbar ist. Denn genauso wie der Wagen ist auch der Treuhänder eine Luftnummer, hinter der der Betrüger selbst oder aber ein Komplize steckt.

Das Geld ist weg: Hat der angebliche Treuhänder den Käufer angewiesen, den Betrag bar per Western Union zu transferieren, ist er sein Geld mit an Sicherheit grenzender Wahrscheinlichkeit los. Denn solche Geldtransfers lassen sich quasi anonym abwickeln. Eine Liste von vorgeblichen Treuhanddiensten, die in der Vergangenheit negativ aufgefallen sind, finden Sie unter *www.escrow-fraud.com*.

Etwas besser stehen die Chancen bei einer Überweisung ins Inland. Dann wird das Geld bei einem arglosen Menschen gelandet sein, den die Betrüger unter Vorspiegelung falscher Tatsachen als Finanzagenten angeheuert haben (siehe oben). Theoretisch kann der Käufer von ihm das Geld zurückzufordern, auch wenn der es schon – abzüglich seiner Provision – per Western Union an die Betrüger weitergeleitet hat. Den Schaden hat der Finanzagent zu tragen, der obendrein mit einer Anzeige rechnen muss. Bei jemandem, der auf ein solch dubioses Jobangebot eingegangen ist, gibt es allerdings oft nicht viel zu holen.

Auto-Schnäppchen: Auch Verkäufer sind gefährdet

Der Trick funktioniert auch andersherum: 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. Erst später stellt sich heraus, dass dieser ungedeckt ist. Oder der Käufer überweist Ihnen das Geld – allerdings nicht von seinem Konto, sondern von einem gekaperten eines Unbeteiligten. Dieser wird seinerseits das Geld von Ihnen zurückfordern, sobald er den Diebstahl bemerkt.