Wie erkenne ich unseriöse Seiten und Angebote?

Sie sollten sich immer fragen: Ist diese Angabe notwendig? Wenn ich mir etwas im Internet anschauen oder herunterladen möchte, wofür braucht die Webseite eine Registrierung von mir? Warum muss ich bei der einen Seite meinen Namen, Adresse usw. angeben, wenn ich eine Software herunterladen möchte, aber eine andere Webseite stellt diese frei zur Verfügung?

Warum sind solche Seiten meist unseriös?

Es ist gesetzlich festgelegt, dass man nur Daten und Angaben erfassen darf, die für die Anwendung notwendig sind. (Grundsatz der Datenschutzgrundverordnung, DSCVO Art. 5/1c). Wenn ich eine Software herunterladen oder einen Liedtext anschauen möchte, warum ist es da notwendig meinen Namen, Adresse usw. zu erfassen? Welche Interessen haben Seiten, die diese Angaben verlangen? Wer sich diese Fragen stellt und sich daraufhin die Seiten genauer anschaut, findet oft unauffällige Hinweise. Versteckt wird häufig darauf aufmerksam gemacht, dass man sich mit einer Registrierung für ein gegebenenfalls kostenpflichtiges Abo anmeldet.

Was ist der Antispam e.V.?

Der Antispam e.V. ist ein Verein, der sich dem Schutz vor Spam und dem Verbraucherschutz verschrieben hat. Der Verein hat keine kommerziellen Interessen und seine Mitglieder engagieren sich zu 100% ehrenamtlich. Die Tätigkeit des Antispam e.V. wurde als gemeinnützig anerkannt, dadurch kann der Verein für Spenden eine steuerlich absetzbare Spendenquittung ausstellen. Gewachsen ist der Verein aus dem Forum Antispam-ev.de. Ein Forum, wo anfangs Erfahrungen zum Thema “Spam" ausgetauscht werden konnte. Inzwischen geht es dort aber auch um viele weitere Themen, die den Verbraucherschutz betreffen. Schauen Sie doch gerne einmal vorbei!

Freie Software

Stellen Sie sich vor, jemand erzählt Ihnen von einem supertollen Programm, das es auch noch kostenlos gibt! Das kann man ja gar nicht glauben. Es ist so, dass sich viele Internetnutzer zusammengeschlossen haben, um sich von den großen Konzernen unabhängig zu machen. “OpenOffice” oder “Firefox” sind zum Beispiel bekannte Programme, die auf dieser Basis entwickelt wurden. Diese kostenlosen Programme werden allerdings von vielen Anbietern angeboten, sodass man schnell den Überblick verlieren kann. Einige Abzocker nutzen dies aus und jubeln dem Downloader ein kostenpflichtiges Abo unter. In der Anfangsphase wurde der Kostenhinweis in den AGB versteckt, inzwischen findet man diesen meist unauffällig auf der Registrierungsseite.

Erkennen von Betrugsangeboten

1. Das wichtigste Merkmal ist das Abfragen von Daten, wie Name, Adresse, E-Mail, Bankverbindung und vieles mehr.

2. Das Setzen eines Haken, mit dem man sich den AGB einverstanden erklärt.

3. Anzeigen bei Suchmaschinen. Bei Suchmaschinen (wie z.B. Google) können Kunden, gegen Bezahlung, einen Platz oberhalb der Trefferanzeige oder an einem besonderen Platz neben der Auflistung bekommen. Angebote aus dem Bereich “freie Software” werden aber oft nicht durch bezahlte Werbung dem potentiellen Nutzer angeboten.

Spendenkonto:
Volksbank Mittelhaardt eG
IBAN: DE05 5469 1200 0117 3387 03
BIC GENODE61DUW

Geschäftsstelle:
An der Marlach 21
67146 Deidesheim
Tel: 09191-83924630
ticket@antispam-ev.de

Warnung vor unseriösen Seiten

Glücklicherweise reagieren Menschen im Internet oft sehr schnell auf solche Seiten und warnen in verschiedenen Foren oder Blogs vor diesen. Eine Suchmaschinen-Abfrage der Seite ist immer sinnvoll und bietet etwas mehr Sicherheit. Zusätzlich Sicherheit bieten Browser-Addons, wie “WOT". Sie beurteilen die Seriösität von Webseiten aufgrund von Nutzererfahrungen.

Welche Möglichkeiten habe ich als Nutzer?

Laden Sie freie Software nur von Seiten herunter, denen Sie vertrauen können. Geben Sie nicht mehr Daten weiter, als für den Vorgang notwendig sind. Fragen Sie sich immer, ob die Angabe, die gefordert wird, überhaupt notwendig ist. Und das nicht nur beim Download “freier Software". Es wird wahrscheinlich mehrere Seiten geben, die die gewünschte Software anbieten. Schauen Sie sich diese in Ruhe an. Die Downloadbereiche großer Computerzeitschriften sind in der Regel gute Adressen. Beispielsweise heise.de (der Verlag der Zeitschrift/TV-Sendung “c't").

Hereingefallen, was nun?

Plötzlich bekommen Sie eine, meist aggressive, Rechnung für die Nutzung einer Webseite. Lassen Sie sich durch die Drohgebärde nicht einschüchtern! Schauen Sie sich die Seite genau an . Überprüfen Sie, ob diese in der Zwischenzeit verändert wurde (kurz vor den “Rechnungen” wird diese oft mit einem Preishinweis versehen). Notieren Sie sich solche Änderungen schriftlich. Überprüfen Sie auch, ob die Seite anders aussieht, wenn Sie sie über den Weg aufrufen, den Sie beim ersten Mal genommen haben. Manchmal ist dies eine ganz anders gestaltete Webseite, auf der bewusst der Preis verheimlicht wird. Sichern Sie diese Seiten mit einem Screenshot (= Bildschirmfoto). Wenn Sie nicht wissen, wie das geht, fragen Sie jemanden oder machen Sie gegebenenfalls ein Foto mit Ihrem Handy.

Gemeinsam gegen Internetfallen vorgehen!

Suchen Sie im Internet andere betroffene Personen, um gemeinsam gegen die Abzocker vorzugehen. Je mehr Personen bezeugen können, dass das Angebot irreführend ist, umso schwerer ist es für die Anbieter, das Gegenteil zu behaupten. Für die Suche eignen sich Verbraucherschutzforen, wie z.B. das von Antispam e.V. oder “Computerbetrug.de". Natürlich gibt es einige mehr, aber auch hier muss man vorsichtig sein. Solche Foren kann man schnell und billig eröffnen. Daher benutzen manche diese als Mittel, um die Lage der Hilfesuchenden auszunutzen und sie mit Fehlinformationen zu Zahlungen zu bewegen. Jedoch ist uns kaum ein Fall bekannt, bei dem die Abzocker über die Drohgebärden (Mahnungen, Inkassoschreiben usw.) hinausgegangen sind. Seit diese Art der Abzocke in Deutschland betrieben wird, hat es nur ganz wenig echter Prozesse gegen Opfer solcher Abzocke gegeben. Außerdem wurden alle Prozesse von den Abzockern verloren. In der Regel können also diese Drohungen mit “Prozess, Schufa-Eintrag, Pfändung" etc. als hohle Luftnummern betrachtet werden.

Allgemeine Informationen

Überall, wo viele Menschen zusammen kommen, gibt es Taschendiebe, Trickbetrüger und Hütchenspieler. Auch im Internet, ein Ort in dem man von Zuhause viel erledigen kann, wie einkaufen, Informationen suchen, mit Freunden kommunizieren und noch vieles mehr. Hier sind die Taschendiebe, Trickbetrüger und Hütchenspieler Anbieter von Waren, die es in Wirklichkeit nicht gibt (z.B. Angebote bei eBay). Sie machen einem vor, dass man zum Beispiel der millionste Besucher einer Seite sei und nur einen Klick vom unendlichen Reichtum entfernt ist.