Markus Kellermann

»Betrugsmethoden im Affiliate-Marketing

Affiliate-Marketing gehört immer noch zu den größten Wachstumstreibern im Performance-Marketing. Allein das Affiliate-Netzwerk Zanox hat 2010 über 367 Millionen Euro Umsatz generiert. Auch affilinet erwartet für 2011 ein Wachstum von über 20 Prozent. Dennoch gibt es wie in jeder Branche auch im Affiliate-Marketing schwarze Schafe, durch die laut dem Software-Anbieter Xamine jährlich ein Schaden von über 13 Millionen Euro entsteht. Markus Kellermann deckt für Website Boosting die Betrugsmöglichkeiten gnadenlos auf und gibt Tipps, wie man sich vor Betrug besser schützen kann.

Es gibt viele Arten von Betrug im Affiliate-Marketing, aber auch genauso viele Möglichkeiten, sich vor Betrügern zu schützen. Allerdings bedarf es hier der nötigen Erfahrung und auch des Wissens, wie die Betrüger genau vorgehen.

In diesem Artikel möchte ich einen Überblick bieten, mit welchen Maßnahmen immer wieder versucht wird, unrechtmäßig an Provisionen zu kommen, und mit welchen Methoden man dagegen vorgehen kann.

1. Cookie-Dropping

Das Cookie-Dropping ist so alt wie das Affiliate-Marketing selbst. Dabei wird versucht, Klicks zu simulieren, welche dann im Browser des Nutzers ein oder mehrere Cookies zu bestimmten Partnerprogrammen setzen, ohne dass ein Nutzer aktiv auf ein Werbemittel geklickt hat. Sollte der Nutzer nun einen Sale/Lead generieren, erhält der Publisher dafür eine Provision, obwohl gar keine Werbeleistung entstanden ist. Die technischen Methoden beim Cookie-Dropping reichen mittlerweile vom automatischen Ausliefern der Advertiser-Seite über iFrames, Flashtracking, Zwangsklicks oder automatische Weiterleitungen nach dem Log-out bis hin zum kriminellen Website-Hacking und der Ausnutzung von Browserschwachstellen. Auch URL Shortener wurden schon verwendet, um im Hintergrund Cookies zu droppen. Der Ideenvielfalt sind hier keine Grenzen gesetzt. Erschwert wird die Analyse von Cookie-Dropping zudem durch die Verschleierung des

> „Das Cookie-Dropping ist so alt wie das Affiliate-Marketing selbst.

Traffics durch IP-Blocker, Referrer*-Abfragen, Mouse Actions, Browsererkennung und Fingerprinting.

Schützen kann man sich vor Cookie-Dropping vor allem durch eine Cookie-Weiche, die man auf jeden Fall immer einsetzen sollte, v. a. auch, um das Setzen von Cookies über mehrere Netzwerke zu regeln. Dazu gehören auch die regelmäßige Account-Überwachung und das Überprüfen besonders umsatzstarker Affiliates, die eine schlechte Click-Trough-Rate bzw. schwache Conversion-Rates* haben und als abnorm gegenüber den Statistiken normaler Affiliates auffallen. Ein erfahrener Affiliate-Manager erkennt in der Regel solche Unterschiede und kann somit schnell gegen die Betrüger vorgehen.

Generiert beispielsweise ein Publisher 1.000 Views und 1.000 Klicks oder hat eine ungewöhnlich hohe Click-Trough-Rate, dann sollte man sich diesen Partner einmal genauer anschauen. Auch wenn bestimmte Partner sehr schnell im Ranking der Top-Publisher steigen, sollte man deren Werbearten genau kontrollieren.

Auch Affiliates aus dem Software- und Tool-

* siehe Glossar Seite 92-93

DER AUTOR

Markus Kellermann ist Head of Affiliate-Marketing bei explido. Zudem organisiert er die Affiliate NetworkxX, die Affiliate Conference und die Affiliate TactixX.

barbereich verwenden in der Regel kein View-Tracking. Falls daher bei diesen Partnern ein sehr schnelles Klick-Wachstum erkennbar ist, sollte man hier ebenfalls den Kontakt mit dem Partner suchen.

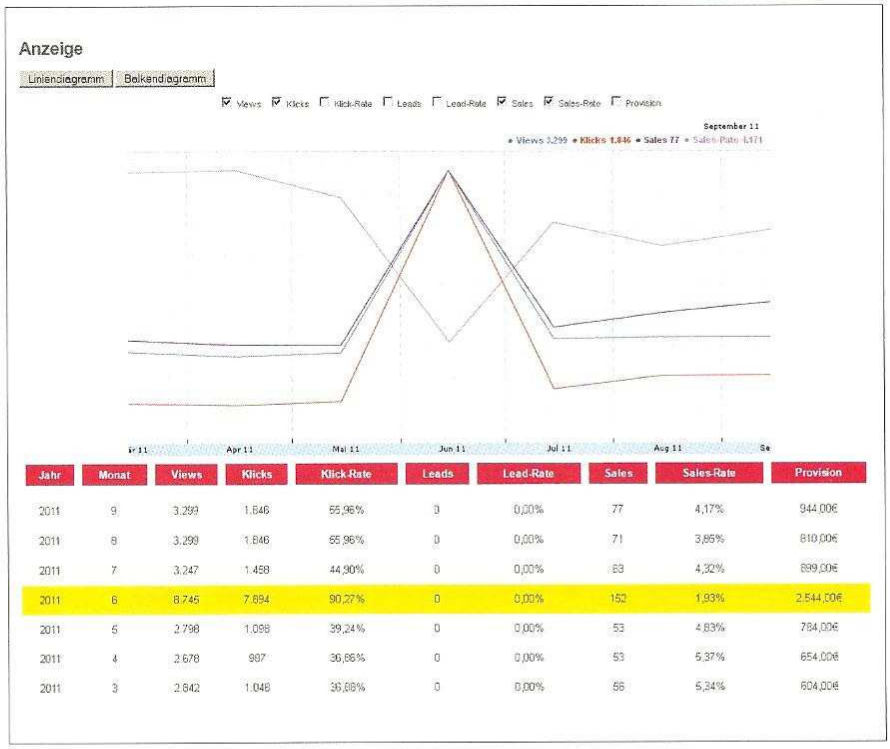
Zudem werden von professionellen Agenturen wie z. B. explido auch Tools eingesetzt, um über definierte Schwellenwerte genau solche Abnormitäten in den Statistiken zu erkennen und Betrugsfälle analysieren zu können.

Des Weiteren hat man auch die Möglichkeit, über die meisten Affiliate-Netzwerke einen IP- oder Referrer-Check durchzuführen, zum einen, um zu kontrollieren, auf welcher Seite genau die Werbemittel eingebunden sind, und zum anderen, um auch die Abstände der Klicks zu überprüfen. Werden diese innerhalb weniger Sekunden gesetzt, besteht der Verdacht von Rechtsverletzungen.

Es gibt auch spezialisierte Tools, um Cookie-Dropping zu erkennen. Dabei werden von verschiedenen regionalen Standorten aus Suchergebnisse, Keyword-Advertising, Media-Kampagnen und Domains analysiert und Cookie-Dropper identifiziert. Hierzu wird eine Datenbank mit über 30 Millionen Websites und 200.000 Keywords nach automatisch gesetzten Klicks durchsucht.

Wichtig ist in diesem Zusammenhang, dass man die Methoden des Cookie-Dropping nicht mit der Postview-Technologie verwechseln darf, die dazu genutzt wird, über eine Display-Bannerkampagne ein View-Cookie zu set-

> „Wichtig ist, dass der Advertiser immer eine Validierung der Sales/Leads durchführt.



Jahr	Monat	Views	Klicks	Klick-Rate	Leads	Lead-Rate	Sales	Sales-Rate	Provision
2011	9	3.299	1.846	55,96%	0	0,00%	77	4,17%	944,00€
2011	8	3.299	1.846	55,96%	0	0,00%	71	3,85%	810,00€
2011	7	3.247	1.458	44,90%	0	0,00%	63	4,32%	899,00€
2011	6	8.745	7.894	90,27%	0	0,00%	152	1,93%	2.544,00€
2011	5	2.798	1.098	39,24%	0	0,00%	53	4,83%	784,00€
2011	4	2.678	987	36,86%	0	0,00%	53	5,37%	654,00€
2011	3	2.842	1.048	36,88%	0	0,00%	56	5,34%	604,00€

Abb. 1. Toolbasierte Analyse von Betrugsfällen (Quelle: explido Partner-Datenbank)

zen. Hierzu gibt es mittlerweile ausgereifte Regeln, welche ein vom BVDW verabschiedeter Code-of-Conduct definiert und die die Werbeleistung garantieren sollen.

2. Brand-Hijacking

Eine immer noch beliebte Methode bei SEA-Publishern ist die Markenrechtsverletzung über Brand-Hijacking. Dabei wird die SEA-Anzeige des Advertisers eins zu eins kopiert und der Affiliate-Link integriert. Obwohl der Advertiser oder dessen Agentur in der Regel auch selbst eine Werbeanzeige geschaltet hat, wird diese durch die kopierte Anzeige des Partners überschrieben und somit werden Provisionen ergaunert, die der Advertiser sonst nicht bezahlen müsste.

Auf den ersten Blick werden die Ad-Hijacking-Anzeigen vom Advertiser selbst gar nicht erkannt und oftmals für das Original gehalten. Dass es sich allerdings um eine Fremdanzeige durch einen Affiliate handelt, kann erst durch die Kontrolle der Ziel-URL erkannt werden. Zudem werden die SEA-Buchungen oftmals auch außerhalb der regulären Bürozeiten vorgenommen und regional so ausgesteuert, dass an den Firmensitzen der Werbetreibenden oder deren Werbeagenturen durch manuelles Überprüfen Regelverstöße unerkannt bleiben.

Um solche Betrugsfälle zu erkennen, kann man spezielle Tools zur Brandprotection einsetzen. Diese nutzen Server in den reichweitenstärksten Regionen, um permanent die geschalteten Anzeigen für Marken lokal zu überwachen. Zudem werden Screenshots der Display-URL und der Tracking-URL erstellt, mit denen man die ausgelieferten Anzeigen archivieren und dokumentieren kann. Damit hat man dann die Möglichkeit, anhand der Publisher-ID den Partner herauszufiltern und juristisch zu belangen. Die bekanntesten Brandprotection-Tools am deutschen Markt sind Xamine, Sistrix und AdPolice. Auch ein schneller Anstieg der Orders, ein unverhältnismäßiger Platz in der Sales-Statistik oder eine sehr gute Conversion-Rate kann ein Signal dafür sein, dass ein Publisher auf die Marke einbucht.

Laut dem Software-Anbieter Xamine sind durch Brand-Hijacking 2011 über 13 Millionen Euro Schaden ent-

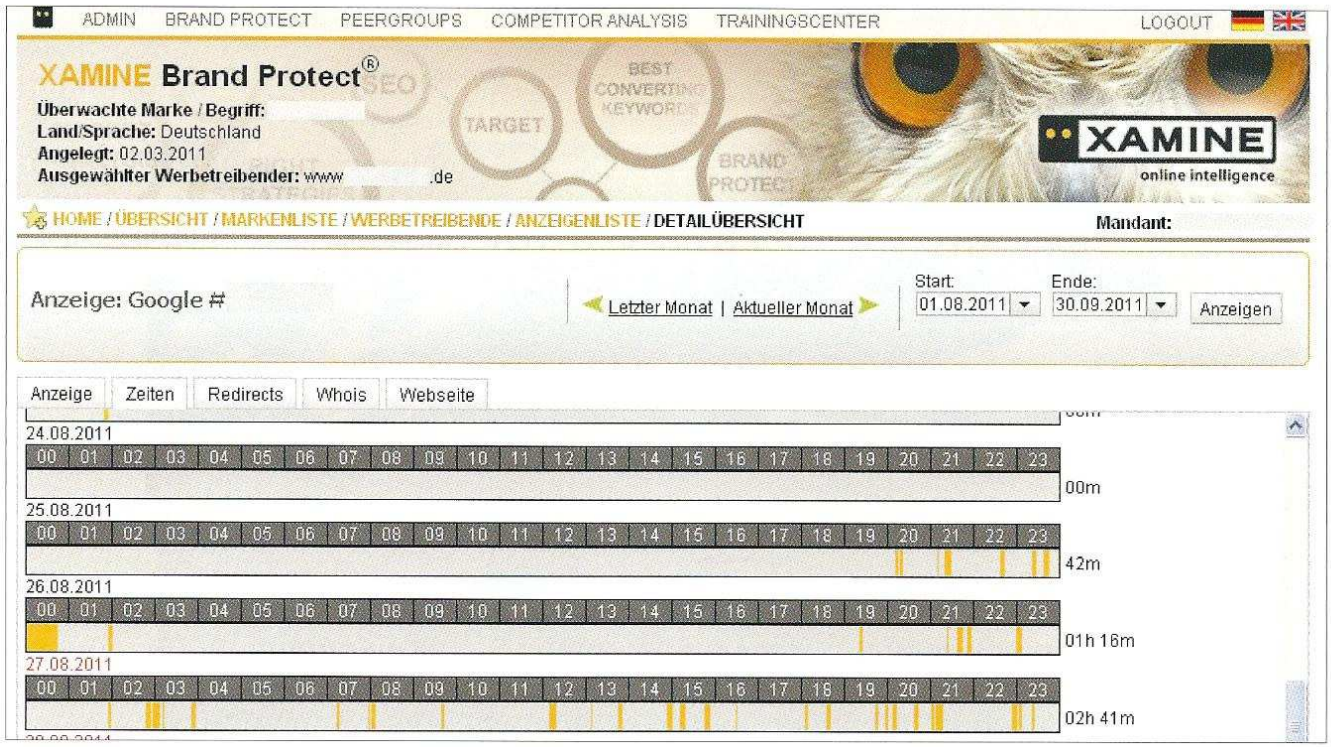


Abb. 2. Brandprotection durch Xamine (Quelle: Xamine)

> Ein gut ausgebildeter Affiliate-Manager sollte sich im Handel mit Domains auskennen.

standen. Wichtig ist daher, dass der Advertiser immer eine Validierung der Sales/Leads durchführt, um Provisionen, die über betrügerische Brand-Hijacking-Maßnahmen generiert wurden, frühzeitig zu stornieren. Dadurch lässt sich der Schaden auf jeden Fall reduzieren.

Nötig ist auch, dass man bereits in den Teilnahmebedingungen des Partnerprogramms SEA-Maßnahmen durch die Partner untersagt, damit es im Fall rechtlicher Streitigkeiten eine einheitliche Regelung gibt.

3. Vertipper-Domains

Immer wieder ein Streitthema sind sog. Tippfehler- oder Vertipper-Domains. Für mache Advertiser ist es eine zusätzliche Einnahmequelle, wenn der Affiliate Tippfehler-Domains verwendet, um darüber Kunden zum Advertiser zu leiten, der sonst vielleicht bei einem Wettbewerber eingekauft hätten. Doch gerade bei eindeutigen Verwechselungen kann dem Advertiser auch ein großer Provisionsschaden entstehen.

Gern genutzt dabei werden v. a. Tippfehler, um damit per URL die Direkteingabe abzufangen. So wird z. B. anstelle der URL www.websiteboosting.com der klassische Tippfehler www-websiteboosting.com eingesetzt. Auch Buchstabendreher wie "ei" bzw. "ie" sind sehr beliebt. Und auch bei Buchstaben gibt es viele kreative Möglichkeiten, neue Domains zu nutzen. Anstelle von "i" könnte man auch "I" nutzen oder auch das kleine "L" ("l") ist mit dem großen "i" ("I") leicht zu verwechseln. Auch die Zahl "0" wird gern für den Buchstaben "O" eingesetzt. Die Fake-Domains werden dann häufig, für den Internetnutzer unmerklich, direkt auf die richtige Advertiser-Seite weitergeleitet. Dabei werden dann ein oder mehrere Cookies gesetzt, was für den Advertiser zu einem Provisionsschaden führt, da der Kunde auch so eingekauft hätte.

Tippfehler-Affiliates melden solche Domains in der Regel auch nicht bei den Affiliate-Netzwerken an, sondern arbeiten mit Scheinunternehmen wie Domainvermarktung oder englischen Ltd-Firmen. Daher ist es technisch sehr schwierig, solche Betrugsfälle eindeutig zu erkennen.

Wie sollte man also vorgehen? Ein gut ausgebildeter Affiliate-Manager sollte sich eigentlich im Handel mit Domains auskennen, insbesondere mit dem Handel von Expired-Domains. Zudem sollte der Account-Betreuer gerade von den Top-Affiliates wissen, wie diese ihren Traffic generieren und auf welchen Seiten die freigegebenen Werbemittel korrekt eingebunden sind. Auch die kontinuierliche Überwachung der Statistiken gehört zur Aufdeckung von Betrugsfällen. Wenn zu den Klicks eines Partners keine Views generiert werden, dann kann das ein Indiz dafür sein, dass die Nutzer automatisiert weitergeleitet und Klicks nur simuliert werden.

Auch in den USA sind Typo-Domains*, wie sie dort genannt werden, ein großes Problem. Der Anbieter CitizenHawk.com hat sich deswegen da-

* siehe Glossar Seite 92-93

Abb. 3 - Typo-Domains über CitizenHawk.com finden (Quelle: www.citizenhawk.com)

rauf spezialisiert, über Online-Brand-Monitoring solche Domains zu finden. Der Anbieter arbeitet in den USA auch mit den großen Affiliate-Netzwerken wie Google Affiliate Network, LinkShare, ShareASale und Commission Junction zusammen, um den Betrügern das Handwerk zu legen.

4. Software und Toolbars

In Deutschland ist es aktuell noch ein eher unbekanntes Problem, in den USA entstehen allerdings über räuberische Software und Toolbars mehrere Millionen Euro Schaden im Affiliate-Marketing. Das Portal www.affiliatefairplay.com prangert daher öffentlich Toolbars und Adware an, die bereits auffällig wurden.

Folgende Methoden sind dabei die bekanntesten Betrugsarten über Adware und Software:

a) Browser Redirect Applications

Dabei übernehmen die installierten Apps die komplette Kontrolle über den Browser des Internetnutzers und führen serverseitig im Hintergrund eine Weiterleitung zum Online-Shop des Advertisers durch. Da diese Anwendungen keine Pop-ups oder Werbung beinhalten, kann der normale User die Weiterleitung nicht erkennen. Gerade bei 404-Fehler-Seiten oder Redirect-Seiten ist diese Art von Betrug sehr beliebt. Sehr dreist sind auch Apps, welche den Type-in-Traffic (also direkt in die Adresszeile eingetippte Webadressen) oder die offizielle SEA-Anzeige dazu nutzen, um ein Affiliate-Cookie zu setzen und direkt auf die Advertiser-Seite weiterzuleiten.

b) Contextual Advertising Applications

Hierbei werden häufig Pop-ups oder Browser-Redirects verwendet, um über Contextual Adware direkten Einfluss auf das Surfverhalten des Nutzers zu nehmen. So werden dem User beispielsweise über den Browser Rabatte oder Gutscheincodes angezeigt, um ihn damit zu veranlassen, bestimmte Websites aufzurufen. Zudem ist es möglich, dass bereits bestehende Affiliate-Cookies von seriösen Partnern über die Adware überschrieben werden und der Betrüger das letzte Cookie durch ein eigenes überschreibt. Dem Affiliate würde somit eine Provision gutgeschrieben, welche ihm gar nicht zusteht, da er keine Werbeleistung erbracht hat.

c) Rebate Applications

Bei Rebate Applications handelt es sich um Anwendungen, die z. B. Einfluss auf die Google-Suchergebnisse nehmen und im Zusammenhang mit der Advertiser-Website Rabattcodes anzeigen, um dadurch einen Klick zu generieren, der den Advertiser sowohl den Rabattwert als auch die Provision kostet und somit zu einem Schaden führen kann.

d) Toolbars

Es gibt jede Menge hilfreicher Toolbars im Internet, es gibt aber auch in diesem Bereich Affiliates, die meinen, sie müssten ahnungslose User ausnutzen, um dadurch Provisionen zu ergaunern. So gibt es z. B. Toolbars, die automatisch Bookmarks im Browser des Nutzers setzen, um damit Einfluss auf das Surfverhalten zu nehmen. Andere wiederum verändern die Ergebnisse von Suchmaschinen und platzieren dort künstliche Affiliate-Anzeigen. Ziel der Betrüger ist es auch hier, Klicks auf Partnerprogramme zu erzeugen, die der normale User selbst eigentlich gar nicht aufgerufen hätte.

Die Betrugserkennung über Software- und Toolbar-Publisher ist relativ umständlich. Um betrügerische Umsätze in

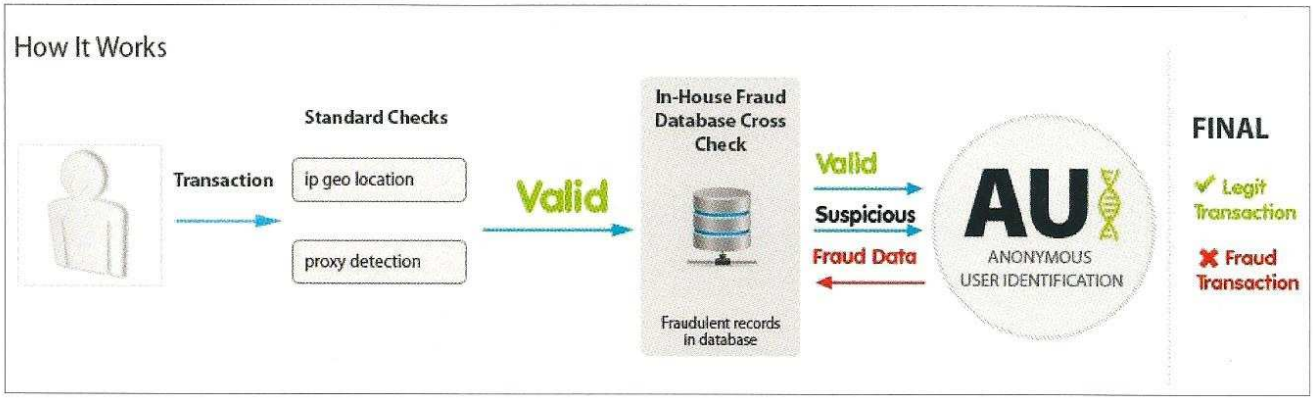


Abb. 4: Fraud-Protection durch fraudlogix *(Quelle: www.fraudlogix.com)*

diesem Bereich zu erkennen, bedarf es v. a. der Erfahrung des Affiliate-Managers und des proaktiven Austauschs mit den Affiliate-Netzwerken. Dazu kommt die detaillierte Auswertung von Statistiken, die natürlich auch automatisiert über Tools erfolgen kann. Auch hier gilt, dass sich Regelverstöße für die Affiliates meist erst ab einer bestimmten Umsatzgröße lohnen. Kennt man den Publisher und fällt ein neuer Publisher auf den obersten Plätzen im Top-Publisher-Ranking auf, dann sollte man den Aktivitäten des neuen Partners nachgehen. Zudem empfiehlt sich auch hier ein regelmäßiger Referrer-Check, der dem Affiliate-Manager erlaubt, die Traffic-Herkunft zu verfolgen. Werden die Referrer nicht sauber übergeben oder ist die Herkunft verschleiert, sollte das Gespräch mit dem Publisher gesucht werden.

Wichtig ist in diesem Zusammenhang natürlich der Hinweis, dass es auch seriöse Affiliates in diesem Bereich gibt, die mit werbefinanzierter Software sehr wohl einen Mehrwert bieten und zusätzliche Umsätze für das Affiliate-Marketing erzielen können.

5. Betrug mit gefakten Kundendaten

Ein beliebtes Mittel bei den Betrügern ist auch die Generierung von

Sales mit gefakten Kundendaten. Dabei wird entweder der Netzwerk-Trackingpixel automatisch aktiviert oder es werden reale Bestellungen, allerdings mit falschen Adressdaten, erstellt. Der Betrüger spekuliert darauf, dass im Partnerprogramm keine Validierung der Sales stattfindet, was heutzutage leider immer noch sehr häufig der Fall ist. Zudem sollten die Kundendaten immer auf Plausibilität überprüft und ein Datenabgleich durchgeführt werden.

In Deutschland gibt es bereits Software-Anbieter wie Datras oder Prodata, die eingegebene Namen und Adressen daraufhin überprüfen, ob diese in Wirklichkeit existieren oder ob die Kundendaten nur aus dem Telefonbuch entnommen wurden.

Speziell in den USA haben sich Software Anbieter rein auf den Abgleich von Kundendaten im Affiliate-Marketing spezialisiert. Anbieter wie www.fraudlogix.com nutzen ihre Lösung, um betrügerische Bestellungen zu erkennen und damit einen Index zu erstellen, der es Advertisern ermöglichen soll, sich auf Basis von 150 Variablen schon vorab vor Betrug zu schützen.

Tipps zur Betrugs-Analyse eines Partnerprogramms:

- Analysieren Sie regelmäßig die Statistiken nach Auffälligkeiten und Traffic-Ausreißern.
- Definieren Sie Schwellenwerte für die Click-Trough-Rate und die Conversion-Rate und beobachten Sie diese aufmerksam.
- Überprüfen Sie regelmäßig die IP-Adressen und Referrer der Partner.
- Liegen die Klickzeiträume der Partner oftmals nur Sekunden auseinander, kann das ein Indiz für Cookie-Dropping sein.
- Auch das mehrfache Auftreten gleicher IP-Adressen könnte ein Warnhinweis sein.
- Vergleichen Sie die Stornoquoten pro Publisher, um Auffälligkeiten zu finden.
- Validieren Sie immer Ihre Sales/Leads, damit durch betrügerische Umsätze kein Provisionsschaden entsteht.
- Kommunizieren Sie regelmäßig mit Ihren Partnern. Verweigert ein Partner das Gespräch, ist Vorsicht geboten.
- Nutzen Sie spezialisierte Tools, um Fraud zu erkennen.
- Definieren Sie klare Regeln in den Teilnahmebedingungen Ihres Partnerprogramms, um möglichen Betrügern von Beginn an das Handwerk zu legen.
- Wenden Sie sich an einen ausgebildeten Affiliate-Manager oder eine spezialisierte Affiliate-Agentur, wenn Ihnen das Know-how fehlt, eine Affiliate-Kampagne professionell zu betreuen.
- Betrachten Sie das Affiliate-Marketing als seriöses Geschäftsfeld und messen Sie ihm die nötige Aufmerksamkeit zu.

Zusammenfassung

Wichtig ist natürlich, dass nicht der Eindruck erweckt werden soll, Affiliate-Marketing bestünde nur aus Betrugsfällen, denn 99 Prozent der Affiliates arbeiten sauber und leiden selbst unter dem Imageschaden, der von den Betrügern verursacht wird. Doch dass es wie in jeder anderen Branche auch schwarze Schafe gibt, dürfte jedem mittlerweile bekannt sein. Daher sollte man sich im Zweifelsfall am besten immer an das Affiliate-Netzwerk wenden oder eine spezialisierte Affiliate-Agentur beauftragen, das Affiliate-Programm zu betreuen.

Affiliate-Marketing sollte generell als seriöses Geschäftsfeld gesehen werden. Hierzu bedarf es dann natürlich auch im Unternehmen selbst der Erkenntnis, den Affiliate-Kanal im Marketing-Mix entsprechend einzustufen und ihm auch die nötige Aufmerksamkeit zu schenken. Daher sollte Affiliate-Marketing auch professionell betreut werden. Wenn man selbst nicht die Ressourcen hat, einen erfahrenden Affiliate-Manager zur Verfügung zu stellen, dann sollte man sich an eine spezialisierte Affiliate-Agentur werden, welche die Erfahrung hat, ein Affiliate-Programm auch entsprechend zu betreuen und zu optimieren.

Man darf auch nicht vergessen, dass Betrug im Affiliate-Marketing kein Kavaliersdelikt ist, sondern auch rechtlich verfolgt werden sollte. Wenn Ihnen also ein Betrüger im Affiliate-Marketing auffällt, dann scheuen Sie sich nicht, einen Anwalt hinzuziehen und die Möglichkeiten einer Schadensersatzforderung zu prüfen. Auch wenn Sie die Sales validieren und die Umsätze stornieren konnten, ist Ihnen doch ein Aufwand entstanden. Und nur wenn es die Branche schafft, auch Exempel zu statuieren, hat man die Möglichkeit, die Gauner auch langfristig aus dem Affiliate-Marketing zu verbannen. Die "sauberen" Affiliates werde es Ihnen danken.

Daher ist es wichtig, dass Sie klare Teilnahmebedingungen für Ihr Partnerprogramm definieren und diese auch jedem Affiliate klar kommunizieren. Nur wenn Sie durch klare Regeln festgelegt haben, welche SEA-Tätigkeiten ein Affiliate umsetzen darf oder mit welchen Publisher-Modellen Sie arbeiten möchten, haben Sie auch vor Gericht gute Möglichkeiten, dem Betrüger das Handwerk zu legen.¶