# Contents

## COPYRIGHT

<table>
<thead>
<tr>
<th>Conten</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTENTS</td>
<td>3</td>
</tr>
</tbody>
</table>

## PPC ADVERTISING IN A NUTSHELL

<table>
<thead>
<tr>
<th>Sub-Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calculating the cost</td>
<td>4</td>
</tr>
<tr>
<td>Be cautious of PPC bidding wars</td>
<td>4</td>
</tr>
<tr>
<td>Keyword targeting</td>
<td>5</td>
</tr>
<tr>
<td>Choosing a PPC search engine</td>
<td>5</td>
</tr>
<tr>
<td>Things to look for in a PPC company</td>
<td>5</td>
</tr>
</tbody>
</table>

## CLICK FRAUD

<table>
<thead>
<tr>
<th>Sub-Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What is click fraud?</td>
<td>7</td>
</tr>
<tr>
<td>Who engages in click fraud?</td>
<td>8</td>
</tr>
<tr>
<td>Why do people steal?</td>
<td>8</td>
</tr>
<tr>
<td>How widespread is the problem?</td>
<td>9</td>
</tr>
</tbody>
</table>

## HOW TO COMBAT CLICK FRAUD

<table>
<thead>
<tr>
<th>Sub-Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anti-click fraud strategies</td>
<td>10</td>
</tr>
<tr>
<td>Avoid PPC networks that allow incentive sites</td>
<td>10</td>
</tr>
<tr>
<td>Frequency caps on clicks</td>
<td>10</td>
</tr>
<tr>
<td>Limit daily spend</td>
<td>10</td>
</tr>
<tr>
<td>Country filtering</td>
<td>10</td>
</tr>
<tr>
<td>Server log analysis</td>
<td>10</td>
</tr>
<tr>
<td>Display Warning Message</td>
<td>11</td>
</tr>
<tr>
<td>Use Specialized Click Fraud Tools</td>
<td>11</td>
</tr>
</tbody>
</table>

## USING SCORING SYSTEM

<table>
<thead>
<tr>
<th>Sub-Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define them. Score them. Own them.</td>
<td>12</td>
</tr>
<tr>
<td>Test 1. Visit depth.</td>
<td>12</td>
</tr>
<tr>
<td>Test 2. Visitors per IP.</td>
<td>12</td>
</tr>
<tr>
<td>Test 2a. Paid clicks per IP.</td>
<td>13</td>
</tr>
<tr>
<td>Test 3. No cookie - no play?</td>
<td>13</td>
</tr>
<tr>
<td>Test 3. Pageview frequency.</td>
<td>13</td>
</tr>
<tr>
<td>Test 4. Anonymous proxy servers.</td>
<td>13</td>
</tr>
<tr>
<td>Test 5. Geographic origin.</td>
<td>13</td>
</tr>
<tr>
<td>Test 6 and beyond.</td>
<td>13</td>
</tr>
</tbody>
</table>

## CLICKLAB: THE FIRST WEB ANALYTICS PLATFORM WITH ADVANCED CLICK FRAUD DETECTION

<table>
<thead>
<tr>
<th>Sub-Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTACT US</td>
<td>16</td>
</tr>
</tbody>
</table>

## REFERENCES AND RESOURCES

<table>
<thead>
<tr>
<th>Sub-Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>REFERENCES AND RESOURCES</td>
<td>17</td>
</tr>
</tbody>
</table>

## GLOSSARY

<table>
<thead>
<tr>
<th>Sub-Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLOSSARY</td>
<td>19</td>
</tr>
</tbody>
</table>
Copyright

All rights reserved. No part of the contents of this document may be reproduced or transmitted in any form or by any means without the written permission of Clicklab and Michael Bloch. Information in this document is subject to change without notice and does not represent a commitment on the part of Clicklab.

All trademarks acknowledged.

Michael Bloch of Taming the Beast.net (www.tamingthebeast.net) has been working the web as a consultant since 1996. Michael has a special focus on ecommerce, affiliate marketing and web site promotion. Taming the Beast.net includes an archive of his research, articles and tutorials, plus a wide range of tools, reviews and industry news items.

Dmitri Eroshenko, CEO of Clicklab (www.clicklab.com), has been a pioneer in the field of online advertising and web analytics since he created the original ad serving software Ad Juggler in 1996, followed by the first vertical PPC directory ISPcheck.com in 1998. Prior to founding Clicklab in 2001, Dmitri was editor and publisher of Web Hosting Magazine and conference chairman of Web Hosting Expo.

Web Address
www.clicklab.com

Mailing address
Clicklab, LLC
8345 NW 66th St #5504
Miami, FL 33166-2626

Contact Sales
Toll free: 888-841-3342
Email: sales@clicklab.com
Click fraud is a problem that can seriously undermine your PPC advertising efforts. This white paper expands on what we know about click fraud and outlines the steps you can take to protect your investment:

- What do you really need to know about PPC advertising
- Who's behind the different types of click fraud
- Using scoring algorithm to detect and document click fraud
- Measuring your traffic quality with Click Inflation Index (CII)

**PPC Advertising in a Nutshell**

Pay Per Click is a paid inclusion model used by some search engine companies that usually requires you to bid on words (keywords) or phrases (keyphrases) that your target market might use when performing searches.

The highest bidder gets the top ranking in the search results, with the next highest bid below and so on. Each time a listing is clicked on, the bid amount is subtracted from the advertisers' deposit.

Some companies charge a flat rate per click, so there's no actual bidding. In this model, ranking is determined by the perceived quality of the page as calculated by a ranking algorithm. When this model is used, it then becomes particularly important to ensure that landing pages are optimized for search engines. In fact, regardless of the PPC model, considering the investment you are making, you should ensure your site is as close to perfect as possible in every aspect in order to achieve maximum conversions.

Pay Per Click is an excellent marketing strategy as it can send very targeted clients to your site; but it can also be a budget black hole. Before you launch a PPC campaign, you'll first need to perform some calculations for projected ROI (Return On Investment).

**Calculating the Cost**

You should first calculate your current visitors/sales ratio. If one web site visitor out of a hundred currently purchases your product, then bidding 10 cents per click will cost you an estimated $10.00 per sale. If your profit margin is $15 per sale, then it may be viable. If it's $9, then it's just not worth it. This is just a rough guide, but a good rule of thumb to work by.
Be Cautious of PPC Bidding Wars

Some PPC advertisers, through either aggressive marketing strategies, ignorance or "auction fever", engage in a bidding wars for the no.1 spot - keep well clear of these scenarios. In very competitive markets, it's not unusual to see a difference of many dollars between the no.1 and no.2 rank bids. Given that not everyone who clicks on a listing will purchase, it can become an extraordinarily expensive marketing exercise to be no.1. Positions 2 - 5 may still perform well in terms of sending converting traffic to you.

Keyword Targeting

You may also find it more economical to bid on more targeted keywords and phrases that aren't quite as popular. For example, a search on "freebsd web hosting" on a leading PPC search engine showed that the top bidder only pays 10 cents for each click; a difference of over $8.30 on the term "web hosting".

Using this strategy will cut down your advertising costs and the more refined targeting may generate improved conversion rates. Searchers who are clear on what they wish to buy tend to be specific in their search criteria. The novice searcher and "tire-kickers" tend to be more generalized in the search terms they use. If you bid on generic terms; you'll be paying the bill while they are learning to refine their queries. Using a tool such as Clicklab will help you in refining your keyword lists by identifying the words and phrases that actually result in conversions.

Choosing a PPC Search Engine

Hundreds of Pay Per Click search engines have sprung up in recent years; but very few of them will actually deliver traffic, regardless of what their promotion states. A few companies, such as Overture and Google, account for the vast majority of PPC traffic.

PPC search engines extend network coverage by offering other site owners search boxes/feeds under a revenue share (affiliate) arrangement. The site owner is paid for each search carried out via their site, or for each click a search generates. The better pay per click engines have networks consisting of thousands of good quality sites where your listings can appear.
Things to Look for in a PPC Company

1. Tools. Does the company offer keyword suggestion features and extensive reporting?

2. Coverage. Who uses their data feeds?

3. Cost. Are there setup fees or minimum balances? What is the minimum bid?

4. Support. Try out their email support - ask a few questions before signing up. If they are slow in responding during the pre-sales process, you can practically guarantee that after sales support will be shocking.

5. Click fraud - this costs advertisers millions of dollars each year. Ask what type of anti-click fraud strategies the company has implemented. Will the company investigate fraud aggressively and compensate you where click fraud is proven? It's also wise to invest in an external monitoring system such as Clicklab. Clicklab's advanced analytics engine will flag instances of click fraud that occur in your campaigns.

There's no doubt that PPC advertising can be very profitable, but click fraud is probably the most ignored, yet potentially most expensive and damaging aspect of PPC that advertisers need to be very familiar with.
Click Fraud

What is click fraud?

Online advertising fraud has been around from the early days of the Internet. To justify the expensive rates and create additional inventory, shady publishers devised the means of artificial inflation of impressions and click-throughs to advertisers' websites.

Today, click fraud refers to the premeditated practice of clicking on pay-per-click ads without the intent to buy advertisers' products or services or take other actions.

Essentially, click fraud is the practice where a person or persons systematically click on links, or use software to do so, to either garner a profit for themselves through click commissions or to purposefully deplete the PPC funds of a competitor.

Who Engages in Click Fraud?

Click fraud can be as minor as an affiliate who clicks on an ad once a day to bump up his revenues, or a competitor who occasionally clicks on an ad out of spite. Major click fraud is very well organized, fleecing millions of dollars from advertisers each year. Some fraudsters create complex robots (software) to generate thousands of clicks, while spoofing IP addresses in order to avoid detection.

There are also ready-made software products, freely available on the market, for generating false clicks. For example, SwitchProxy, a third party extension for Mozilla Firefox browser, allows anyone to click on the same paid links repeatedly from a different IP address (that of a proxy server) without ever switching an Internet connection. Still too much work? There are commercial tools you can download, such as FakeZilla (fakezilla.com) and I-FAKER (i-faker.com), based in Bulgaria and Ireland.

Other fraudsters employ teams of people in developing countries to click on ads. This may sound a little extreme but with some click bids as high as $10 - $20 each, and if you only have to pay someone $5 a day to click on links, this strategy can be very profitable for the fraudster.

In March of this year a 32-year-old California man was arrested and charged with extortion and wire fraud in connection with the software he developed called Google Clique. Google Clique was designed to automatically click on paid ads, while remaining virtually undetectable by the search engine.
Michael Anthony Bradley allegedly contacted Google and demanded a payoff, threatening to release it to the "top 100 spammers" otherwise. Bradley claimed that Google Clique could defraud Google of 5 million dollars in half a year's time.

Bradley (or someone pretending to be him) posing under the nickname CountScubula, posted on alt.internet.search-engines newsgroup: "Google even called me to their office, I flew up, met with them, and let's just say, they are scared and don't want this software to get out, bottom line, I don't care anymore."

Google wrote in its S-1 registration statement filed with the Security and Exchange Commission on April 29, 2004: "We are exposed to the risk of fraudulent clicks on our ads. We have regularly paid refunds related to fraudulent clicks and expect to do so in the future. If we are unable to stop this fraudulent activity, these refunds may increase. If we find new evidence of past fraudulent clicks we may have to issue refunds retroactively of amounts previously paid to our Google Network members."

On May 3, 2004, the India Times published a widely read article, "India's secret army of online ad clickers." An excerpt from that article:

"A growing number of housewives, college graduates, and even working professionals across metropolitan cities are rushing to click paid Internet ads to make $100 to $200 per month,"

**Why Do People Steal?**

"People shoplift to get something for nothing," says Terrence Shulman, an attorney, therapist, corporate consultant, book author, and founder of Cleptomaniacs And Shoplifters Anonymous (CASA), a self-help support group.

Shulman estimates that the addictive-compulsive shoplifters represent 85 percent of total shoplifting population of 23 million (that's one in every 11 Americans!). "This group emotionally has a lot of repressed anger and often exhibits signs of other compulsive addictions, such as overeating, shopping, drug use, or gambling," says Shulman. "When caught and confronted, they will often break down and cry." The remaining 15 percent is shared between the professionals who steal for profit; impoverished stealing out of economic need; thrill seekers getting their fix; drug addicts; and kleptomaniacs, those who steal for no reason at all.

Bradley "does not appear to be typical of most of the persons I have worked with," says Shulman. "His plotting and planning and brazen 'extortive'
pressures on Google are different from the shy, passive-aggressive kinds of thefts I and most of my clients have engaged in."

Shulman hypothesizes that Bradley could have "rationalized that he was not hurting anybody – that Google is a rich company, not a particular person, and that they could afford it. There can also be a sense of inferiority in people who feel the need to outsmart others or ‘beat the system’." 

**How Widespread Is the Problem?**

Instances of advertisers who have had thousands of dollars drained from their accounts in just a few hours are not isolated. Over time, even on a small scale, click fraud can add up to significant amounts of money, dramatically affecting advertisers small and large advertisers.

Click fraud can also inflate cost of each click for all advertisers as some PPC companies adjust the minimum price of each click based on the popularity of the category or keyword.

Some of Clicklab clients estimate that up to 50% of PPC traffic in certain competitive categories is illegitimate. While that figure may be somewhat of an exaggeration as a general average, it does occur in that range in some sectors, perhaps at even higher percentages.

As PPC technology has evolved, so too have the inbuilt anti-fraud mechanisms that search companies implement. The major companies recognize click fraud as a problem that seriously threatens their businesses. The situation is somewhat similar to the battle against viruses - as a "cure" for a virus is released, a new virus appears.

Given the nature of the battlefield, it's of crucial importance that PPC advertisers have solid anti-fraud strategies in place and not to rely solely on the search company to provide protection.
How to Combat Click Fraud

Anti-click Fraud Strategies

Fraud can be simple to minimize initially, only requiring you to choose a pay per click company wisely and then monitoring results on a daily basis. The increasing incidences of more organized fraudsters will require you to use special tools to monitor activity for you. The following strategies will assist you in minimizing the amount you lose to click fraud.

Avoid PPC Networks That Allow Incentive Sites

Before opening an account, always ask the company if they allow incentivized sites into their network as feed partners or affiliates. An incentives site usually offers something to its' visitors in exchange for clicking on links or performing some other action. Given this model, the clicks that you’ll receive from these sites will more than likely not convert as the focus of the click isn't based on interest in your product. Incentive driven sites aren't fraudulent, but it's important to gain this clarification.

Frequency Caps on Clicks

Ask the PPC company if they utilize frequency caps and what the cap is. A frequency cap is a method that will prevent duplicate clicks originating from the same IP from being deducted from your balance.

Limit Daily Spend

Start your campaign with a reasonably low daily spend limit, then increase it slowly while monitoring results regularly. As an example, let's say you set a limit of $50 a day and during the first week you average $40 worth of clicks for a 24 hour period. Then the following week, that $40 is chewed through in the first 6 hours, without an appreciable increase in sales or leads - this could be due to click fraud. By using this strategy, your losses would have been minimized.

Country Filtering

What is your target market - do you really need coverage, for example, in Romania? Also keep in mind that the majority of all types of online fraud originates in Eastern Europe, Africa and some Asian countries.

Server Log Analysis

Study your server logs daily and check for multiple clicks originating from the same IP or range of IP’s.
Display Warning Message

For dealing with the rotten apples among your competition, have your programmers write a script that will display a nice warning message after several repeated clicks to your Web site from a paid listing on a PPC search engine.

Greetings!

Thank you for your interest in our product and services.

We noticed that you visited our site more than once recently by following a paid link from one or more of the pay-per-click search engines.

Please bookmark our site for future reference so you can save a step and visit us directly.

Enjoy your visit!

IP address: 123.45.67.89

This technique can dramatically reduce your click fraud rate.

Use Specialized Click Fraud Tools

Manual fraud monitoring can be very laborious - your valuable time is probably better spent in doing what you do best - marketing, following up on leads, refining products or developing new content. Modern third party analytical tools, unlike their predecessors, have become increasingly affordable, accurate and easy to use. One such product is Clicklab web analytics.
Statistical Scoring System for Combating PPC Click Fraud

Larger PPC networks have a working mechanism for detecting fraudulent clicks. Otherwise, we suspect that they wouldn't be able to stay in business. Today's PPCs are likely to be able to weed out non-malicious bots and amateur perpetrators. But do these systems have the capacity to stop the professionals? We're not so certain. If the history of spam-fighting is any indicator, the click inflation problem is here to stay.

Define them. Score them. Own them.

In order to remain undetected, professional inflators need to closely simulate real visitor behavior and visit parameters. They know the number of pageviews their clicks generate is among the first things to be evaluated.

The good news is if you use statistical methods, you will be able to beat the perpetrators at their own game. Whether it's for your internal use or for negotiating a refund from a PPC provider, what's needed is a system for statistically defining and documenting fraudulent click activity.

Enter the Click Inflation Index system. This system performs a variety of tests to detect fraudulent user session signatures, assigning penalty points to each offense. If the cumulative score - we call it Click Inflation Index (CII) - exceeds the threshold, the user's session is tagged as fraudulent.

This chapter explains the basic principles and tests you can use when developing your own Click Inflation Index algorithm. You will need a competent technical team armed with an adequate web analytics solution. The process is fun and the results are well worth the effort.

Words of caution before you begin to implement a wide-scale click fraud fighting campaign: Make sure your keyword bidding strategy is up to date. Top expensive keywords remain a high-profile target for con-artists. Unless your marketing strategy calls for you to engage in a bidding war -- and provides the budget for it -- it's a good idea to diversify and bid on the largest possible number of well-researched, lower-cost keywords.

The click-fraud detecting tests you can use include:

Test 1. Visit depth. How many pageviews did this particular user session generate? If it's just one, it's a good reason to lift a red flag a notch or two - but not more. Keep in mind that there could be a variety of reasons behind the single-page visits. Perhaps your ad copy isn't clear and misleads the visitors, or maybe the network connection was too slow and user decided not to wait for the other pages to load.
Test 2. Visitors per IP. Because of the proxy servers and networks of users sharing one Internet connection, there will always be unique visitors with the same IP address. It's normal. You just need to calculate the "normal" for your website's unique mix of traffic sources. IP addresses whose visitor counts exceed the control group by a certain percentage are added to the blacklist and trigger a penalty.

Test 2a. Paid clicks per IP. Works the same way as Test 2, except counts only user sessions that resulted from clicking on one of your paid links. Typically, you will track these by the unique destination URLs used in pay-per-click listings, such as yourwebsite.com/?source=google.

Test 3. No cookie - no play? Many marketers will tell you that because most bots and scripts are not capable of supporting the cookie mechanism, a user session without a cookie is a good cause for alarm. Others will say that it can't be an accurate indicator because some privacy devotees do not accept cookies and thus look indistinguishable from bots. So, penalize or not? We think you should.

Test 3. Pageview frequency. Most bots travel through your site and request pages from the server much faster than humans. If a particular user session has generated a few pageviews in a matter of seconds, it's a good enough reason to penalize it. On the other hand, you have to be careful not to go overboard when defining your threshold. Humans can surf through your site pretty fast too!

Test 4. Anonymous proxy servers. Click thieves know that IP address is the primary means for identifying the user session. Therefore they need to launch their attacks from many different IP addresses. The more, the merrier. Fortunately, IP address spoofing is not a trivial task. For this reason, click inflators often channel their activity through anonymous proxy servers. Your solution is to develop and maintain an up-to-date list of anonymous proxy servers and penalize user sessions originating from them. Most legitimate visitors have no reasons to use anonymous proxies.

Test 5. Geographic origin. Now on to the politically incorrect part. You get to blacklist any country in the world you'd like! Just think of the countries from which you never have and likely never will receive a viable lead. Remember, you're not about to ban visitors from these countries to access your website. You're just going about your regular business of assigning points.

Test 6 and beyond. Finesse and customize. You can devise your own triggers and assign points to them. For example, if 98% of your business activity occurs during normal business hours, you may want to penalize visitor
sessions originated at all other times. Or you may track visits from a set of suspicious IP addresses for a period of time, and plot their activity vs. time of the day. Does it follow your site's average activity patterns? It better!

Now you need to sit down with your technical, design, sales, and marketing teams. The agenda for the meeting is to: 1) decide on which tests to use, 2) come up with the scoring system for the selected tests, and 3) pick the right threshold.

To test and adjust your selections, run through the possible actions of a dozen or so hypothetical real user personas, and calculate their scores. They shouldn't trip the alarm.

Now do the same exercise using personas of click-inflating robots and humans. Visits made for the sole purpose of depleting of your PPC account should trip the wire every time.

Remember, to make sure your scoring system works precisely as intended, always compare your results against a control group of unbiased traffic sources, such as Google's and other major engines' organic search results.

Click fraud is a contact sport with no rules. Click Inflation Index is a defense system you can use to protect yourself and fight back.
The First Web Analytics Platform with Advanced Click Fraud Detection

Throughout the preceding white paper, we referred to the importance of having a reliable means to track and measure the metrics that are relevant to your e-business. Pay-per-click keywords, banner and link placements, email promotions, affiliate programs, and search engine optimization (SEO) are a great ways to drive traffic to your website. In order for these efforts to be effective, it is necessary to use web metrics to analyze your website traffic and the return on your marketing investment (ROI).

Clicklab web analytics allows you to:

- Eliminate non-performing advertising,
- Develop the perfect advertising mix for your site(s),
- Detect and document click fraud,
- Find the most profitable keywords,
- Improve web site usability and conversion.
No Additional Hardware, Software, or Programming

Clicklab takes care of hosting the application so you don’t need to invest in any software, programming, or additional staff. Clicklab starts gathering valuable data on your visitor activity and your ROI immediately after you insert simple JavaScript codes into your website HTML.

The Most Affordable Investment You Can Make in Your Business

We can get you up and tracking in as little as two hours and for as little as $50 a month. What you’ll end up saving in unproductive advertising alone will more than pay for our services. Plus, you can look forward to a substantial increase in sales, revenues, satisfied customers, and saved time.

"I like your product and find it extremely useful in determining real time traffic flow, advertising ROI and especially optimization objectives." Paul Lionti, Connection Channel

"We highly recommend Clicklab to any online business that needs a one stop e-commerce solution." Coryon Redd, Cellphone Battery Warehouse

"I use Clicklab to quickly eliminate the non-working portions of my clients’ campaign portfolios." Hank Dearden, 3D Technologies

Contact Us

Feel free to contact Clicklab for more information about our services or the contents of this white paper.

Web Address
www.clicklab.com

Mailing address
Clicklab, LLC
8345 NW 66th St #5504
Miami, FL 33166-2626

Contact Sales
Toll free: 888-841-3342
Email: sales@clicklab.com
References and Resources

Pay-Per-Click Analyst
"Click Fraud: State of the Industry"
By Dmitri Eroshenko

…“Clickpockets” represent a significant challenge for both PPC search engines and their advertising clients. Most of the larger PPC search engines employ dedicated security teams armed with sophisticated statistical algorithms to monitor paid click flows on its native keyword searches and content affiliate sites. In contrast, most marketers don’t do anything to detect even amateur clickers…

http://www.payperclickanalyst.com/article-dmitri-eroshenko-005.htm

Datamation
"New Attacks and Defenses In Click-Fraud War"
By Brian Livingston

…Just as antivirus and antispam vendors must constantly upgrade their products to detect new kinds of attacks, an escalating battle of software is raging against the scourge of online advertising — click fraud…


WebProNews
"PPC Guerilla Tactics"
By Brittany Thompson

…If your promotion strategy includes pay-per-click, listen up. You need to be aware of a few guerilla tactics that are gaining popularity - and as a result may end up hurting legitimate businesses…


C|Net
"Exposing Click Fraud"
By Stephanie Olsen

…Internet marketers facing higher advertising fees on search networks are becoming increasingly concerned about a form of online fraud that was thought to have been contained years ago…


WebProNews
"Click Fraud The Google Killer"
by Garrett French

…Google listed click fraud as one of the potential "worries" that would-be investors should consider. In fact, they admitted to regularly paying refunds because of click fraud and stated that they may have to make retroactive payments…

SearchEngineWatch
"Lost Per Click: Search Advertising & Click Fraud"
By Jessie Stricchiola

…Click fraud -- the practice of clicking on a text advertisement served by a search engine for the sole purpose of forcing the advertiser to pay for the click -- is emerging as an important concern for search engine marketers…

http://searchenginewatch.com/searchday/article.php/3387581

ClickZ
"Programmer Arrested in Alleged AdSense Extortion Plot"
By Pamela Parker

…A 32-year-old California man has been charged with extortion for allegedly demanding Google pay him for software designed to defraud its AdSense program…


The Times of India
"India's secret army of online ad 'clickers'"
By N. Vidyasagar

…With her baby on her lap, Maya Sharma (name changed) gets down to work every evening from her eighth-floor flat at Vasant Vihar. Maya's job is to click on online advertisements. She doesn't care about the ads, but diligently keeps count — it's $0.18 to $0.25 per click…

http://timesofindia.indiatimes.com/articleshow/msid-654822,curpg-1.cms
## Glossary

**Glossary**
Marketing and Metrics Terms Used in This White Paper

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Acquisition Cost</strong></td>
<td>The marketing/advertising costs divided by the number of click-throughs or other desired actions equals the cost of acquiring each visitor/purchaser.</td>
</tr>
<tr>
<td><strong>Affiliate Programs</strong></td>
<td>Programs that recruit and pay web site owners a flat fee or percentage to sell a product/service on their sites or redirect traffic to the vendor.</td>
</tr>
<tr>
<td><strong>Click Stream</strong></td>
<td>The tracked path of pages a visitor takes through a web site.</td>
</tr>
<tr>
<td><strong>Cookies</strong></td>
<td>Small files of information that a server automatically places on your computer when you browse web sites. Cookies are stored on your hard drive where servers can access them when you return to sites you’ve been to before.</td>
</tr>
<tr>
<td><strong>CPM</strong></td>
<td>Cost Per Thousand impressions. Advertiser pays for the number of times ad is viewed, regardless of whether it is clicked on.</td>
</tr>
<tr>
<td><strong>Conversion Rate</strong></td>
<td>The percentage of users who take a desired action, such as making a purchase or registering.</td>
</tr>
<tr>
<td><strong>HTTP</strong></td>
<td>Hypertext Transfer Protocol. The system the Internet uses to transfer files and information on the web. Whenever a web user opens a browser and types in an address or clicks a link, HTTP is being used.</td>
</tr>
<tr>
<td><strong>Key Performance Indicators</strong></td>
<td>(see Metrics) Measurements of web site visitor activity over a given time period, including data such as page views, orders, conversion rate, etc.</td>
</tr>
<tr>
<td><strong>Keyword Phrase</strong></td>
<td>The phrase typed into a search engine in order to begin an online search. Carefully selected KWP’s should appear in a web site’s content and HTML tags.</td>
</tr>
<tr>
<td><strong>Metrics</strong></td>
<td>(See Key Performance Indicators) Measurements of web site visitor activity over a given time period, including data such as page views, orders, conversion rate, etc.</td>
</tr>
<tr>
<td><strong>Page Views</strong></td>
<td>Also known as page impressions, the number of times a</td>
</tr>
</tbody>
</table>
single HTML page is requested from a server.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Paid Search</strong></td>
<td>Paid ads that appear on search engine or directory results pages, such as Yahoo’s paid business listings.</td>
</tr>
<tr>
<td><strong>PPC</strong></td>
<td>Pay Per Click. The advertiser pays a predetermined amount for each prospect who clicks through to their web page. Mostly used by search engines such as Google AdWords.</td>
</tr>
<tr>
<td><strong>PPL/PPS</strong></td>
<td>Pay Per Lead and Pay Per Sale. The advertiser pays a set fee for each prospect who either makes contact (PPL) or makes a purchase (PPS).</td>
</tr>
<tr>
<td><strong>PPV</strong></td>
<td>Pay Per View. The most common ad selling arrangement used by larger web sites. Often sold on a CPM basis.</td>
</tr>
<tr>
<td><strong>Proxy Server</strong></td>
<td>A server that holds the most commonly accessed and recently used content from the web in order to provide quicker downloads for users and to increase server security. It operates between a web client and a web server.</td>
</tr>
<tr>
<td><strong>ROI</strong></td>
<td>Return On Investment is a measurement of revenue earned from an ad or marketing campaign compared to money spent on it.</td>
</tr>
<tr>
<td><strong>SEO</strong></td>
<td>Search Engine Optimization. A set of optimization techniques that help ensure search engines recognize and rank your site as highly as possible, so more searchers find it.</td>
</tr>
<tr>
<td><strong>Spiders</strong></td>
<td>Also known as crawlers or bots, these are programs that search the Internet looking for new resources and adding what they find to a database.</td>
</tr>
<tr>
<td><strong>Unique Visitors</strong></td>
<td>The individuals who visited a web site during a specified time period, not counting repeat visits.</td>
</tr>
</tbody>
</table>