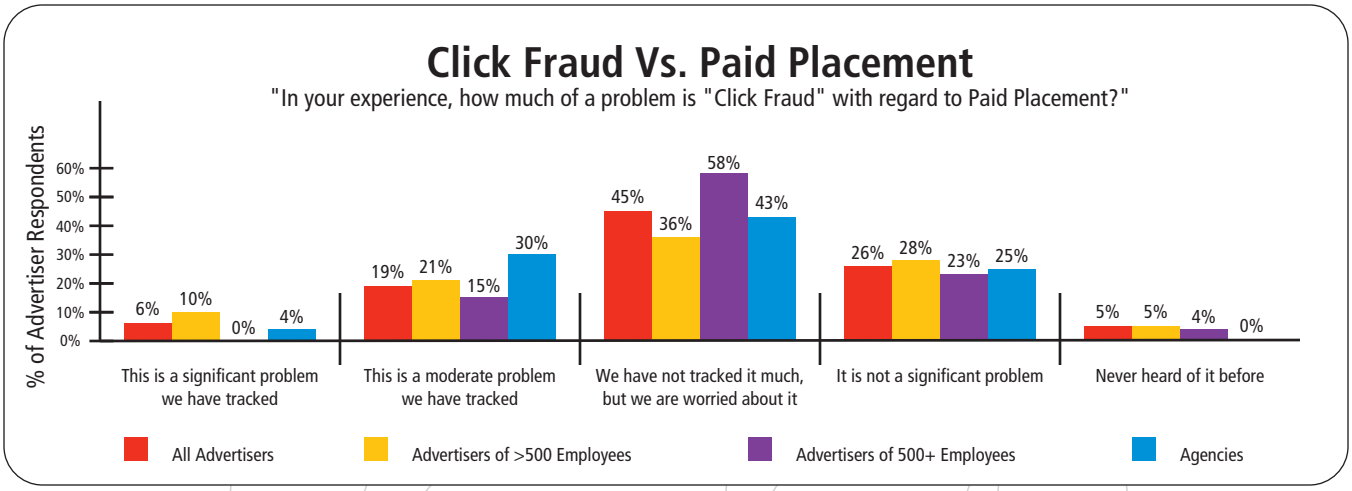
Using Web Analytics To Identify Possible Click Fraud

A White Paper From Net Applications

EXPOSING CLICK FRAUD

Net Applications 65 Enterprise Aliso Viejo, CA 92656 949-330-7910
netapplications.com

What Is Click Fraud?



Click fraud has recently emerged as a topic of discussion and debate regarding the potential of undermining the pay-per-click revenue model that has made Google and Yahoo the financial success that they are today.

At its essence, click fraud is the willful act of clicking on a search engine sponsored listing or banner ad with the intention of falsely increasing clicks while consuming the advertiser's pay-per-click budgets.

While there is little consensus that click fraud will undermine the pay-per-click market, most search engine marketers agree that click fraud does occur and diminishes the success rate of many online marketing programs. Below are the results of a recent survey conducted by the Search Engine Marketers Professional Organization (SEMPO).*

*The State of the Search Engine Market 2004, SEMPO 2004

Net Applications 65 Enterprise Aliso Viejo, CA 92656 949-330-7910
netapplications.com

Click Fraud - Why People Do It?

There are numerous reasons why someone will intentionally commit click fraud. In some cases, click fraud may be an isolated occurrence. In other cases, click fraud may be a malicious and well thought out systematic method of generating excessive and erroneous click activity.

The Covert Competitor

In some cases it may be a rival competitor who jealously has clicked on a top sponsored ad to visit your web site. In this case the click fraud may easily go undetected if the number of clicks is not exceedingly high. Even if identified, the time involved for seeking remuneration from the pay-per-click network may not justify the time involved in the research and pursuit of the credit.

However, some more sophisticated unethical marketers have developed a variety of programs and techniques in an attempt to out wit other advertisers by depleting their budgets, daily allocations or reducing return on investment in an attempt to take top position for sponsored links. In some cases, these marketers utilize cloaking technologies to generate clicks while going undetected. In addition they may develop "spider" technologies that automatically and systematically click on sponsored links.

In the cloaking example, a click fraud perpetrator may be accessing the Internet using a single IP address or block of IP addresses, while fraudulently clicking on your ads. They may cloak or disguise their IP address (similar in manner to a spammer using an erroneous reply to an address) so they appear to be accessing your pay-per-click ads from a variety of IP addresses in an attempt to avoid detection

Alternatively, the click fraud perpetrator may develop a computer program that automatically "crawls" a search engine or their affiliates in a spider like fashion looking for competitor pay-per-click ads and generating erroneous clicks on sponsored links.

The Advertising Affiliate

Some search engines with pay-per-click / sponsored listings have developed a network of affiliate sites that distribute listings based on search term results in what is known as contextual advertising. The ads or sponsored links are served up in the context of related Web site copy. For example, a search request for news on the Apple iPod™ may direct the user to a news Web site that displays a sponsored link along with an article about the new iPod Shuffle.

The advertising affiliate is compensated with a percentage of the revenue associated with "click" resulting from the display of the sponsored link. Some affiliates have actually generated erroneous clicks in an attempt to boost their own revenue. In addition to using spider technologies that generate click fraud, some of these affiliates have resorted to a form of "outsourced" click fraud. In this case, they enlist the help of foreign labor who click on advertiser listings with no intention of looking at your site. These clicks increase the amount the advertising affiliate gets from the pay-per-click network.

Recently, Wired News** reported that Auction Experts International, a Google AdSense partner located in Houston, allegedly reaped $50,000 in commissions by hammering away on ad links until Google sued in November 2004. Its principals never showed up in court, and Google won by default.

In summary, there are a variety of factors that induce click fraud. Some of these perpetrators have developed sophisticated technologies and business processes in order to fraudulently generate clicks without getting detected. Others are less sophisticated, but still poise a threat and burden for accurately measuring a campaigner's online success.

**Click Fraud: Problem and Paranoia by Adam L. Penenberg, 10 March 2005

Net Applications 65 Enterprise Aliso Viejo, CA 92656 949-330-7910
netapplications.com

Click Fraud - What To Look For?

By monitoring your site visitors from pay-per-click marketing and establishing baseline visitor behavior, unusual patterns usually become apparent. Almost everyone can be a victim and no one is immune. There are a variety of indicators that you can watch for to identify possible click fraud including:

Conversion Rates
If you are spending ANY money on pay-per-click marketing programs you should establish base line conversion rates for your campaigns. For example, how many clicks does it take to generate a desired site behavior (e.g., shopping cart transaction, e-mail opt-in, contact us form completion). By comparing your campaign results to your expected baseline, you can identify underperforming campaigns as suspicious click activity.

Clicks By Country
Some search engine marketers and advertising affiliates have outsourced the task of erroneously clicking on your sponsored links. If you have an increase in activity from domains like Romania (.ro) or India (.in) you may be a victim of click fraud.

Repeat Visitors From The Same IP Address
Repeated clicks from the same IP address may be a possible sign of click fraud. This technique is a first line of defense in the identification of click fraud. There may be legitimate reasons why campaign clicks may originate from the same IP address (e.g., aol users). However, by combining this information with a number of other variables, suspicious clicks can easily be differentiated from genuine customer visits.

Page Depth
When analyzing click behavior, it is important to note the average page depth of the suspicious visitor. If a repeated site visitor generates only one page view per visit this may be suspicious. Compare these results to a typical visitor session on your site. Be wary as some sophisticated bots which can generate multiple page views from an automated fraudulent session.

Time On Site
In addition to identifying repeat visitors and page depth, also consider the time spent on the site. An automated bot may generate many visits and lots of page views, but do so in a period of time too short for a human. By knowing how long a typical visitor spends on your site you will be able to identify suspicious click activity.

Acceptance Of Cookies
Many bots use browser-less spider technology to visit your site. In many cases these spiders do not accept cookies. Evaluate what percentage of your site visitors accept cookies (typically more than 95%). Repeat visits though a sponsored link from the same visitor who does not accept cookies may be a bot that is attempting to deplete your ad budgets.

Clicks At Unusual Hours
The World-Wide-Web never sleeps, however, be wary of an unusual increase of visitor activity at odd hours of the day or night. This may be suspicious visitors from different time zones not typical of your usual site visitor or automated spiders that are clicking your ads at all hours of the day or night.

Net Applications 65 Enterprise Aliso Viejo, CA 92656 949-330-7910
netapplications.com

Click Fraud - Who Gets Hurt?

Click fraud is not a victimless crime. Victims of click fraud include the search engine marketer, the advertiser, the consumer, and ultimately the search engine or pay-per-click network.

The Search Engine Marketer

Search engine marketers who are victims of click fraud see their rate of return on marketing programs diminished by these activities. It needlessly consumes budgets and decreases results. As a result, search engine marketing organizations may be delivering results at a sub-optimal level jeopardizing their client relationships. Click fraud can become a difficult topic of discussion if it has been ongoing for a prolonged period of time and left undetected.

The Advertiser

What business can afford to pay more for advertising dollars needlessly? Whether an organization is large or small, return on ad dollars is under paramount scrutiny. One of the benefits of online and eCommerce business models is the ability to "close the loop" on advertising dollars. By marketing through search engines and selling online, there is an unprecedented opportunity to track and report return on investment from search engine marketing dollars – down to the keyword! The growing prevalence of click fraud contributes to diminishing performance industry wide for online marketing campaigns directly impacting all advertiser's.

In addition, if click fraud continues unchecked, there may be the possibility of an industry shakeout where less credible companies will be forced out of the market resulting in fewer search engine/pay-per-click network operators allowing those remaining to be under less scrutiny for raising minimums and increasing online ad fees.

The Customer

Because organic search engine listings can be complicated and competitive, many companies rely on sponsored listings to ensure that they are highly ranked in search engines. Customers have come to rely on sponsored listings to find what they are looking for on the web. Should click fraud undermine the pay-per-click business model, advertisers will find its cost prohibitive to place sponsored listings. In turn, customers will find it more difficult to find what they are looking for on the web.

Furthermore, there is the possibility of higher cost of goods and services. If marketing budgets are increased due to click fraud and associated customer acquisition costs, marketers may elect to pass on the increased costs to the consumer in higher prices for goods and services

The Search Engine/Pay-Per-Click Network

Ultimately, if click fraud reduces results to a point where it is no longer economically feasible to sponsor listings, advertisers will stop spending and the search engines will suffer accordingly. While it seems that they benefit in the short run by erroneous clicks (they get paid anyway don't they), these engines compete to deliver top results. Letting click fraud run rampant on their networks is not in their best interests and they know it.

It should be noted that many of the more respected networks have acknowledged the click fraid problem and are actively reviewing suspicious activity on their networks. When it has been uncovered, the networks are beginning to automatically credit back advertisers for the suspicious click activity. However there are many unscrupulous or just plain lazy networks out there with no intention of taking on the burden of policing their own networks. In cases like these, their business practices of today will come back to haunt them as their future livelihood and longevity depends in part with their industry participation in detecting click fraud.

Net Applications 65 Enterprise Aliso Viejo, CA 92656 949-330-7910
netapplications.com

What To Do About Click Fraud?

There are a variety of best practices, services and technologies available to identify and protect yourself against click fraud.

Know Your Pay-Per-Click Vendor
Before signing up for a pay-per-click program, research where and how your sponsored listing will appear. If your listing appears on obscure web sites that seem irrelevant to your potential site visitors you may be exposing your self to click fraud. Many pay-per-click programs provide the option to include or exclude affiliate properties. Make sure you are comfortable with where your sponsored links will appear. Not only will it mitigate click fraud, but it helps you control your brand.

Develop a Baseline
Establish expected results for your site visitor behavior from pay-per-click programs. Many live web site statistics products are available that are affordable and easy to implement. These online services typically provide hundreds of web site statistics, pay-per-click conversion tracking, visitor behavior and more. It is important to have comprehensive reporting to establish your baseline. Repeat visitors by campaign are not enough to determine whether the clicks are from a customer, prospect or an erroneous visitor with the intent of click fraud.

ANALYZE your Navigation Paths to determine what paths your visitors usually take. Unusual and repeated paths from a repeat visitor may be a spider trying to trick you.

LOOK at the Page Depth and Average Time spent per page for your visitors. Repeated visits with minimal page views and short time spent per page may again be a spider clicking on your sponsored links.

REVIEW visitors by country to identify increased traffic from suspicious countries of origin. Unusual patterns in visitor traffic by country may be a sign of outsourced click fraud.

ANALYZE your referrals by search engine and search term. Make sure the referral source for your pay click visitors appears valid. Check these referral sources to make sure your ad is appearing. If you are getting clicks from a search engine, but don't see your ad, you may be a victim of an affiliate scam.

KNOW your typical pay-per-click conversion rates. Review your campaign activity summary reports to identify any underperforming pay-per-click campaigns. Make sure to compare these to similar campaigns over the same time period. All else equal, you should get similar results from similar search terms with similar ad copy.

Implement Click Fraud Detection Technologies
Tracking repeat visits by IP address from your pay-per-click campaigns is your first line of defense against click fraud. Comparing this data to information such as number of visits, page depth and minutes per session are ways of identifying suspicious activity from your pay-per-click marketing programs.

You may consider SETTING UP EMAIL ALERTS to notify you of multiple clicks from the same IP address. By proactively monitoring and reporting click fraud you can do your part to stem the flow of erroneous charges to search engine marketing budgets.

In addition, there are some ADVANCED TECHNOLOGIES from a variety of vendors that incorporate sophisticated statistical models that can analyze your site activity and "predict" potential click fraud behavior. Beyond the first line of defense these techniques can assist in identification of click fraud that may go undetected by the human eye.

If your budgets dictate, there are also PROFESSIONAL SERVICES available to audit the performance of your pay-per-click programs. These programs are comprehensive and provide a definitive method of identifying click fraud. If your company has spent hundreds of thousand of dollars or even millions on pay-per-click and feel they have been victimized, this option will allow them to look back, identify and quantify exposure to click fraud.

These items listed in this section are suggestions for steps to take. They do not constitute a complete list of methods and techniques for the detection of click fraud.

Net Applications 65 Enterprise Aliso Viejo, CA 92656 949-330-7910
netapplications.com

Exposing Click Fraud

Glossary

Pay-Per-Click – Online advertising technique that only charges when the ad is clicked

Sponsored Listing – Search engine result where placement is typically determined in order of the highest pay-per-click

Organic Listing – Natural search engine listing determined when a search engine finds your site through a crawler or search engine submission

IP Cloaking – A technique of disguising an IP address

Spider or Bot – a computer program that systematically performs a function on a web site, such as, repeatedly clicking on a sponsored link for a specified search term or URL

About HitsLink

HitsLink™ is Net Applications' flagship product providing advanced Web site statistics and analysis for Webmasters and eMarketers alike. For as little as $9.95/month, HitsLink tracks hundreds of statistics, analyzes sites for search engine optimization, pay-per click performance and acts as a first line of defense against click fraud. With no software to install, HitsLink can be up in minutes tracking visitor behavior, search terms, conversion tracking and more.

About Net Applications

Since 1999, Net Applications has been a leading source of tools and utilities for Webmasters and eMarketers for small to medium enterprise (SME). The company has a complete suite of simple and affordable subscription-based applications that are designed to help users have greater success with their Web site marketing efforts. Headquartered in Aliso Viejo - California, NetApplications distributes its services through over 6,000 partners and affiliates. These services may also be founded at **www.netapplications.com**, **www.hitslink.com**, **www.submitter.net**, **www.publishplus.com**, **www.1stwarning.com** and **www.toolshack.com**.

Net Applications 65 Enterprise Aliso Viejo, CA 92656 949-330-7910
netapplications.com