

This Free E-Book is brought to you by Natural-Aging.com.

100% Effective Natural Hormone Treatment
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!

Pay-Per-Click Fraud Exposed

By Dean Phillips

Pay-Per-Click Fraud Exposed by Dean Phillips

Has anyone else noticed a disturbing pattern in your pay-per-click advertising campaign, of the same IP addresses clicking on your ad, spending one or two seconds on your website and then leaving?

That's called click fraud and it's a major problem among all of the pay-per-click search engines.

Click fraud is a scheme that takes advantage of online advertising programs like those offered by Google, Yahoo/Overture, Findwhat and others. A fraudulent website is

set up and participates in programs like Google's AdSense program. Unlike legitimate websites that attract human visitors to the site, fraudsters use software "hitbots" or employ boiler-rooms of low-wage employees from other countries to generate clicks on ads, and then collect commission from pay-per-click programs.

In June, a federal grand jury returned an indictment against Michael Anthony Bradley 32, of Oak Park California who was charged with fraud and extortion for a scheme involving Google's pay-per-click program. Believe it or not, Bradley actually tried to extort Google into paying \$100,000 for click fraud software he created called "Google Clique."

Click fraud hurts advertisers by driving up the cost of each click because many online advertising programs adjust the price of each click based on the popularity of a particular keyword and the number of competing advertisers. And depending on how popular your keyword is, it can take just a few minutes to register hundreds of clicks. Click fraud can quickly deplete your pay-per-click account and leave you

Pay-Per-Click Fraud Exposed

with little or nothing to show for your expenditure.

In a recent filing to the Securities and Exchange Commission, Google acknowledged, "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."

Now, in all fairness to the pay-per-click companies I've used in the past, I have to give credit where credit is due. Whenever I complained of click fraud, which was often, all of the pay-per-click companies, without exception, did the right thing and credited the stolen funds back into to my account. Ironically, I have not had a click fraud problem with Google.

You can reduce your risk of being victimized by click fraud, by regularly auditing your website's log files and immediately reporting suspicious traffic to the pay-per-click companies. If you are unfamiliar with analyzing your site's log files, there are some excellent software products available to assist you like ClickTracks, WebTrends, and AWStats. These products make it fairly easy to identify patterns in your website's traffic.

Recently, I noticed the same IP number clicking on my ad over and over again—often many times within just a few minutes. I did some basic detective work and discovered it was actually a competitor of mine devouring my pay-per-click dollars. I approached him with my findings and threatened him with law enforcement intervention, if he didn't cease and desist. He denied any involvement, of course. But I haven't had any problems with that individual since.

So, how did I find out who the culprit was? Easy.

When checking your log files, if you notice a lot of clicks from one IP address, you can trace its origin by visiting the American Registry of Internet Numbers. By feeding the IP address into their "Whois" search, they will tell you who has been assigned that IP address, and whether it's an actual IP or another business entity.

Should the IP address not be assigned to the Americas, you can verify RIPE Network Coordination Center for all Russian, European, and Middle Eastern registries, or the Asia Pacific Network Information Center. There are only three such sites, so you should be able to track the source.

However, if someone is using sophisticated software to generate clicks on your ad, it will probably be impossible for you to trace the IP address yourself. For

example, according to alleged Google extortionist, Michael Bradley, "Holland Engine software was originally written to allow spammers to conceal their originating IP address from mailservers and to keep it from appearing in e-mail headers.

Holland Engine is the core of LincolnSX, the most powerful mass-emailing software, running at rates of 5 million e-mails per day per machine. Holland Engine will actually tunnel through the internet and connect to the desired IP address from, not your IP but rather from another, the one at the end of the tunnel."

In conclusion, if you choose to use pay-per-click search engines to advertise, watch your log files closely and report improprieties immediately.

Also, don't put all of your eggs into one basket, by depending solely on pay-per-click advertising. Utilize a variety of ways to attract traffic to your website, such as ezines, newsletters, writing articles, offline

advertising, etc.

Tips For Combating Click Fraud

By Gabriel Adams

Click fraud is one of the biggest issues in the pay per click industry right now. It's easy to understand why, too - click fraud costs advertisers money, but gives no return. It cuts deep into profit margins, and in some cases, may be the difference between making money and losing money.

Click fraud is, at its simplest, clicks on ads that are not generated by a real person interested in making a purchase. Click fraud can come from many different sources:

Click bots, which are robots designed to click on ads, are one source. Click bots are often run by an affiliate of the PPC search engine.

Competitors may click on your ads to try to drive your cost up.

Click schemes are programs people join to click on ads for each other. Usually these people are affiliates of the PPC search engines.

Combating click fraud can be tough. One of the easiest ways to combat click fraud is to not advertise on search engines who deliver lower quality traffic. This factor is easily determined with conversion rates. If one search engine's traffic converts at 2 percent, and traffic from the second search engine converts at 1 percent, you know the traffic from the second search engine is half the quality. Click fraud is likely one of the factors involved.

Pay-Per-Click Fraud Exposed

In addition to such basic tracking mechanisms, you can use more advanced tracking mechanisms to try to catch click fraud. For example, you could use a script that you would gather data on visitors from PPC search engines (data might include IP address, number of times they clicked on the ad, and time they spent on the site) and use that data to pick out suspicious visitors. You can then submit the data to the search engine and request a refund on the traffic.

Click fraud is probably the biggest problem in the PPC industry, and you can work to save yourself some money by combating click fraud.

Bespoke click fraud detection and protection software from Evolution Internet Ltd:



This Free E-Book has been brought to you by Natural-Aging.com.

[100% Effective Natural Hormone Treatment](#)
Menopause, Andropause And Other Hormone Imbalances
Impair Healthy Healing In People Over The Age Of 30!