

Click Fraud

Can you imagine Google insisting that you to pay a \$100,000 AdWords bill, when you only planned to spend \$500 on your Pay-per-Click (PPC) advertising campaign? Or in another scenario, what if your website was pulling nice click-through profits thanks to Yahoo! PPC ads, but the system suddenly shut you out, claiming you were likely the person doing all that clicking just to increase your income?

These are the two ugly faces of click fraud, which is considered the largest threat to the Internet advertising and marketing industry. Frequently seen in the Pay-per-Click advertising world, click fraud is a deceptive technique that's costing companies and entrepreneurs thousands due to malicious PPC ad clicks.

Lots of real money is being lost through click fraud crimes. A 2006 online advertiser study conducted by Outsell, Inc., a publishing research firm, estimated click fraud's impact on advertisers to be \$1.3 billion. That included roughly \$800 million wasted by companies paying for fraudulent clicks, plus the \$500 million in ad revenues Google and other advertising networks lost due to PPC fraud fears.

That same year, Google settled a \$90 million class action lawsuit, paying attorneys fees and credits to advertisers affected by click fraud.

According to a *Business Week* cover story of October 2006 titled Click Fraud, most academics and consultants who study the matter estimate that somewhere between 10% and 15% of all ad clicks are fake or malicious, and account for \$1 billion in faulty PPC billings. In January 2009, ClickForensics, a leading monitoring service, published findings that an all-time high of 17.1% of ad clicks were fraudulent during the 4th quarter of 2008.

But Google staunchly believes those figures are inflated and misleading. Google says that, for reasons related to many site visitors' likely use of the back-button, data captured by ClickForensics is inaccurate. Click fraud occurs, Google contends, but at a mere fraction of what ClickForensic's alarming reports keep claiming.

Whatever the real percentage is, the fact is that click fraud could happen to *you*. And it's not just advertisers who're troubled by click fraud issues. Blog and website owners who run affiliate marketing PPC ads on their sites also can become victims of click fraud.

This article examines how both advertisers and affiliate marketers can be hurt and why many in the online marketing community are so concerned. We'll also provide you click fraud detection and prevention measures and tips.

Massive and Malicious PPC Clicks

In most cases, click fraud involves malicious, massive clicking of your PPC ad by a competitor, simply to inflate your advertising bill. Subsequently, you'll panic when you see your sky-high advertising bill and stop running PPC ads. Which is exactly what your competition wants you to do. Once you can longer afford to advertise, the "disappearance" of your ads from Google or Yahoo! means more clicks – and potentially more money – for the perpetrator's products or services.

Where Google and Yahoo are concerned, click fraud has created a dire situation; they're both highly dependent on revenues generated by PPC advertising. It will harm their profitability if people stop using PPC programs such as AdWords, fearing click fraud. Despite the fact that Google is continually improving prevention methods, Pay-per-Click fraud is not going away anytime soon, if ever.

Still, these very advertising networks are the biggest beneficiaries of click fraud: They'll insist that you still foot the advertising bill that someone (or *something*, as in a malicious bot) created to set you up. Try to sue the search engine for taking the money off your credit card and you could be blacklisted by them.

A Click Fraud Horror Story

According to the same issue of *Business Week* mentioned above, one of the nightmares regarding the financial damage that click fraud creates involves Martin Fleischmann, the owner of MostChoice.com. MostChoice.com is an Atlanta-based company that offers consumers a variety of information and rate quotes on insurance and mortgages.

Fleischmann, who only deals with U.S.-based clientele, had noticed that a growing number of clicks were coming from Botswana, Mongolia, and Syria. These ads that were being clicked on did not appear on Google or Yahoo. Instead, there were clicks registered on mysterious websites such as insurance060.com or insurance1472.com. As a result, Fleischmann has calculated that click fraud has cost his company over \$100,000.

Sources of Click Fraud

Needless to say, click fraud has become a source of much controversy and expensive litigation. It's become such a problem that it's now considered an Internet crime, and felony arrests for it are not uncommon.

Outside of the U.S., countries such as Botswana, Mongolia, and Syria appear to be the most prolific where click fraud is concerned; apparently, providing this fraudulent service is a money-making business. But dubiously emerging as click fraud capitols are Canada, Germany, and China.

But don't be fooled: The guy two towns over or two doors down might be directly causing someone this grief. . . sitting at a computer, clicking your ads out of spite to make Google or Yahoo! suspicious and give your site the boot.

There are four classifications of click fraud perpetrators who're considered to be the biggest offenders:

Advertiser's Competitors – The intent is to harm an advertiser within the same market by maliciously clicking on their ads. In so doing, they eliminate (or at least weaken) the competition by trying to deplete their advertising budget.

Publisher's Competitors – This is where a blog or website publisher running affiliate PPC ads is framed. Someone's making it appear that you're clicking your own advertisements over and over to bilk the PPC system. This could result in the termination of your relationship with the advertising network. It also could put your site out of business, despite your innocence.

Publisher's Friends – Let's say you successfully publish a blog or website. Your friends want to help you by clicking your ads, having no intention of purchasing a thing. Their plan could backfire: You, the publisher, could be accused of click fraud.

Other forms of malicious intent – Sometimes click fraud is simple vandalism. Someone simply wishes to cause you harm for no benefit at all. Typically, motives in this area are either personal or political. Perhaps they don't like the views expressed on your blog. Maybe you're dating their ex-boyfriend. Whatever the reason, they simply aim to cause trouble for you and your site.

How to Avoid Being a Victim

You cannot 100% eliminate the risk of click fraud. However, you can diminish the likelihood of it devastating your advertising budget. According to ClickTracks and incuBeta, two leading click fraud detection companies, there are various techniques you can employ to reduce your risk of being a click fraud victim:

1. ***Set different bid prices for content-targeted sites*** – Reduce your financial risk by limiting the amount you are prepared to pay per click. Industry experts at ClickTracks and incuBeta say that content-targeted websites are more frequently the sources of click fraud than non-contextual (search engine) ads. Limit your exposure by limiting your placement of ads on “just any” website relevant to your keywords.
2. ***Keep an eye on your competitors*** – Monitor who is competing with your keywords in the search engines, as they could be a potential source of competitor click fraud. ClickForensics offers free click tracking reports that details the number of clicks on your ads that come from competitors and other common sources of fraud. Companies such as AdWatcher and ClickDefense offer free trials of their popular click fraud detection reports.
3. ***Always track your advertising campaigns*** – Remember: You can’t manage what you don’t monitor. Google makes available to advertisers using its AdWords program two tools: Campaign Performance and Account Performance. These allow you to see the number and percentage of clicks that Google has categorized as invalid. Both of the top ad publishing companies now work with ClickForensics on the problem, but Yahoo! was the first to proactively introduce its Click Protection System, which flags clicks on an advertiser’s billing that appear fraudulent, and doesn’t charge you for that activity.
4. ***Only advertise in specific countries*** – Countries with low labor rates employ people for the sole purpose of clicking on advertisements. Don’t run ads in those countries where you can be seen and possibly sabotaged.
5. ***Target high-value sites for your ads*** – Some low-quality sites are hotbeds of click fraud... A person or a bot may be clicking your ad – any ad – on these sites to boost the owner’s PPC revenues. Google and Yahoo! allow you to set up ad campaigns that only run ads on the sites you specify, thereby avoiding sites where unethical revenue generating may occur.
6. ***Purchase software programs that generate special referral reports*** – ClickTracks and incuBeta are two top services that offer search reports that’ll help you identify any content-targeted websites that are sending suspicious amounts of visitors to your site. ClickTracks also helps you prepare a fraud report should you ever need to prove your case to a search engine firm.

In summary, be aware of click fraud possibilities and take measures to prevent your ad campaign and/or site from falling prey to it. Following the steps and tips above will go a long way in ensuring that you don't become a victim of these Internet crimes.

But don't shy away PPC advertising. It's probably too important a component of your marketing mix to stop entirely. Sure, lots of press coverage exists around click fraud, but much that coverage is self-perpetuating. The negativity and alarmist reactions are what's attracting so much more media attention to the issue.

In all likelihood, click fraud will never happen to you.