



Measuring and countering click-fraud

a white paper from

Speed-Trap

Click-fraud is a growing problem for the Internet at large, and advertisers in particular. This paper discusses how Speed-Trap's e-business intelligence software can be used to counter this problem and ensure credibility/auditability of click-thru statistics.



Introduction

Click-fraud is a term that describes the process of an individual clicking on search or affiliate adverts on the web with fraudulent intent.

"A fraudulent clicker can exploit the way web ads work to rack up fees for a business rival, boost the placement of his own ads or make money for himself. Some people even employ software that automatically clicks on ads multiple times."

Source: "In click-fraud web outfits have a costly problem"

By Kevin J. Delaney,

The Wall Street Journal Online, April 6 2005, Page A1

**"Businesses that pay billions to Google and Overture to steer potential customers to their Web sites are increasingly questioning how much fraud lurks in the blossoming pay-per-click model of advertising...
...a tangle of conflicting interests makes it hard to straighten out or even quantify the click fraud problem. ...**

Add buyers worry that "click fraud" could become rampant, if unchecked – a development that could undermine confidence in the fastest growing segment of Internet advertising."

Source: "Web Marketers Fearful of Fraud in Pay-Per-Click" By Nat Ives

The New York Times March 3, 2005

This document describes how Speed-Trap's unique and patented e-business intelligence solution can be used to measure and alert instances of click-fraud, and thereby eliminate fraudulent clicks from the accounting processes that determine the cost and placement rules for adverts on the web.

Measuring click-fraud

By implementing Speed-Trap on the site that hosts adverts (the "host" site), and/or the site that owns the target content of the advert (the "target" site), advertisers and their customers can understand the exact clicking behaviour of all visitors to the site.

This is possible because Speed-Trap provides a complete session based "audit trail" of each visitor's activity on the site(s), including all pages loaded, all hyperlinks and elements clicked on, and millisecond timestamps of each of these "events".

By measuring activity on the host site, Speed-Trap can determine when people click the same advert multiple times within one session. Similarly, by measuring activity on the target site, Speed-Trap can determine how many times a visitor "arrived" on the site from an advert within one session. If necessary we can even link the browsing sessions between the host and target site.

Monitoring the host site will highlight those sessions that have an abnormally high number of clicks on a particular advert, or have an abnormally high click rate on one or more adverts.

Monitoring the target site will provide a correlation between the number of clicks per session on the host site, and the actual arrival of sessions on the target site. Sessions never actually arrive, or arrive and disappear very quickly are likely to be fraudulent – particularly if this occurs more than once or twice in a particular session.

Click-fraud session attributes

The "normal" behaviour may vary by site and even by advert, but Speed-Trap can be used to determine the normal range of various session attributes.

These include:

- **click-number** - number of clicks on particular adverts on the host site
- **click-rate** - time between successive clicks on particular adverts on the host site
- **arrival-number** - number of times sessions actually arriving on the target site
- **arrival-rate** - time between successive arrivals on the target site
- **arrival-retention** - time that an arrival actually spent on the target site
- **arrival-activity** - amount of real browsing activity after arrival on the target site

Using click-fraud measurement

There are two primary uses for using the click-fraud measurement described above. Firstly, by actually measuring the amount of fraudulent activity, fair rates and accurate payment for advertising can be achieved, and further, adverts can be sustained and placed based on their "real" usage rather than "real" and "fraudulent" activity combined. This capability alone will allow an advertising agency or online business to provide their clients with a set of rules and guidelines against which they will be charged. The obvious benefit is regaining the trust of the client and eradicating the confusion and ill will so prevalent in the industry today.

Secondly, it would be possible to isolate individual sessions that are exhibiting apparent fraudulent behaviour in near real time. By close-coupling the Host server with the Speed-Trap collection server, fraudulent sessions could be recognized and modified by the host server/Speed-Trap server. The exact nature of the modification depends on the level of activity required, but would typically include features such as:

Session Termination – The offending session could be terminated by the server, although this would only stop the offender loading another page in that session context.

Link suspension – The Speed-Trap Client Side Adapter (CSA) in the page could be instructed to disable one or more adverts for a period of time (or indefinitely for that page). This would prevent multiple clicks being generated.

Popup Messages – The Speed-Trap CSA could be instructed to display a JavaScript alert that advises the user that their current behaviour is deemed to be inappropriate, and requires the user to acknowledge the alert. The advert could then also be suspended for a period of time.

Conclusion

Speed-Trap's technology can provide out-of-the-box solutions to the problems of click-fraud, and these can be enhanced to provide active systems to prevent, deter or trap fraudulent activity.



Speed-Trap

Speed-Trap Limited

Venture West, New Greenham Park
Newbury, RG19 6HN, UK

tel: +44 (0) 1635 230630

e-mail: info@speed-trap.com

www: www.speed-trap.com