



Identifying and Stopping Click Fraud

March 2007

Introduction: The undetected threat

According to the Internet Advertising Bureau^[1] pay-per-click (PPC) advertising generated over \$5 billion in annual revenue for 2006. Of this, an estimated 25% or over \$1.5 billion will come from content syndication networks.

While online advertisers have always accepted of some level of fraud within PPC advertising, there is mounting concern^[5,7,8] that click fraud is now having a major impact on the internet advertising market.

While search companies publicly maintain that click fraud is a small percentage of overall clicks, our research suggests that for certain advertisers this number may be as high as 50%. Our own research has uncovered a large and growing network of web sites developed for the sole purpose of generating revenue from AdSense and other content syndication networks. These web sites are growing rapidly in number and sophistication, and are possibly costing advertisers hundreds of millions of dollars in fraudulent or low-value clicks while going largely undetected.

In this paper we describe the various types of click fraud, show details of click fraud attacks, examine trends that are influencing the increase in fraud, and provide suggestions for detecting and preventing click fraud.

Definition: Click Fraud and other Low Value Clicks

What is click fraud?

We define the term “click fraud” as the practice of clicking on paid advertising links to either (1) harm a competitor, or (2) make money by “forging” clicks on web sites that show ads through content syndication. The term “fraud” is used because in either case, the advertiser is paying for a click without receiving any true value.

To better understand various types of click fraud, it is important to understanding the basic revenue model of paid search advertising. Since many organizations outsource pay-per-click management, advertisers may not be fully aware of the details of each model. And as the saying goes – the devil is in the details.

Paid Search Revenue Models

There are two primary types of “Pay-Per-Click” (PPC) advertising. The first is “direct” search, where users access the main web site of a search engine (such as Google, MSN or Yahoo) and type in keywords. The second is Content Syndication (otherwise known as “content networks”) where web site owners receive commissions on the click charges by posting ads on their web sites. Google’s AdSense™ program is an example of a content network that involves thousands of web sites. Each revenue model has its own type of click fraud.

Traditional Pay-Per-Click

In traditional paid search, advertisers bid on a variety of search terms to trigger various advertisements. The amount of the bid (combined with other factors such as the overall success of the ads in generating clicks) generally determines the ad’s position on the search page. Each time a search user clicks on one of the ads, the search company (Google, Yahoo, MSN or others) makes anywhere from a few cents to several dollars on each click.

Advertisers who use paid search advertising can run reports showing the effectiveness of their ads, including the number of clicks and their total dollars spent on clicks for each billing period. Online advertising budgets range from pennies per day to thousands of dollars per day.

Content Syndication

The other primary advertising model in pay-per-click is known as content syndication. In this model, businesses can place PPC ads on their own web site, and then share in the click revenue from users who click on these ads. Content syndication is responsible for the near ubiquitous “Ads by Google” that are found on thousands of web sites.

For example, a web portal devoted to tennis may be generating thousands of visits a day. To make additional revenue, the web site could become part of a syndicated

network such as Google's AdSense™ network. Once part of the network, they use a simple script to display ads on their site. If any web site visitors click on these ads, they get a fraction of the click-fee that the advertisers pay to Google.

Click Fraud Attacks

In this section we describe the two most common click fraud attacks against advertisers – the *Budget Attack* and the *Click Farm Attack*.

The Budget Attack

To help control spending, advertisers are allowed to specify a daily "budget" or maximum spend for their various ad campaigns. After the maximum is reached, their ad will be taken down from the search pages. This feature, invaluable to advertisers, enables the first type of attack, which we call the "budget attack." In the budget attack, a competitor or other third party will click repetitively on your ad until your budget is depleted and your ad is no longer visible.

The budget attack is well known, but there is not reliable data on how often it occurs. It is certainly large enough that businesses have been created specifically to address this problem.

While the budget attack is probably common, two factors make it less likely that a given advertiser will be targeted. First, it requires a motivated competitor who is willing to take the risk of being detected. Second, it doesn't bring direct revenue to the attacker. While the attacker may get the satisfaction of doing financial harm to a competitor, they must still rely on their own ads and web site to generate revenue.

Click Farming Attack

The second type of attack, which occurs within content syndication networks, is sometimes called "click farming." Compared with a budget attack, click farming is a far more common and alluring attack for fraudsters. It is alluring because of the huge revenue potential, and it is common because of the ease in which click farm web sites can be created. While a budget attack requires the effort of a malicious competitor, any online advertiser can become a victim of click farming.

While the ad syndication model of PPC greatly expands the potential reach of an online ad, the model is practically a prescription for click fraud. In the simplest case, a member of a content syndication network (such as Google's AdSense™ network) can click on their own web site, or recruit others to click on it, hundreds or even thousands of times. With each click, a portion of the money goes to the search company and a portion goes to the web site. At the end of the month, the search company sends the site owner a check for a percentage of the click revenue. The advertiser experiencing the clicks pays the search engine (Google in this example) the full amount for the clicks, but received no legitimate traffic for their money. Since advertisers bid anywhere from a few cents to over \$10 per click, the monthly revenue potential is enormous.

Example: Anatomy of a Click Farming attack

To demonstrate a typical click farming attack, we will use log data from an advertising campaign running on Google's AdSense™ network. For each paid search listing, we are able to record various details of each click including the data and time, referring URL, keywords, and end-user IP address.

Figure 1 shows the detailed click-referral log for a one-hour period on November 21st, 2006. Reviewing the detailed logs, we observe a large number of clicks coming from a suspicious-looking web site called "searchemu.com". The log shows that within one hour, this ad received over 20 clicks from the same web site on the AdSense™ network, all from different IP addresses.

11/21/06 10:59:09 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	86.71.211.2
11/21/06 11:00:18 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	86.201.81.33
11/21/06 11:00:39 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	83.189.240.181
11/21/06 11:04:32 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	81.242.190.166
11/21/06 11:04:42 AM	se	google	hipaaGroup		No referrer	81.243.176.60
11/21/06 11:09:14 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	189.140.185.222
11/21/06 11:09:55 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	200.56.183.150
11/21/06 11:16:45 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	212.152.23.13
11/21/06 11:20:43 AM	se	google	hipaaGroup		http://pagead.l.google.com/pagead/ads?cl	213.47.1.235
11/21/06 11:22:37 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	81.241.33.168
11/21/06 11:24:07 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	189.157.75.102
11/21/06 11:26:34 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	201.6.137.102
11/21/06 11:28:34 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	200.79.1.161
11/21/06 11:30:56 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	211.123.246.80
11/21/06 11:31:45 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	200.186.128.2
11/21/06 11:34:43 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	172.173.48.174
11/21/06 11:35:27 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	201.24.56.68
11/21/06 11:39:29 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	88.149.140.27
11/21/06 11:45:26 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	84.73.112.20
11/21/06 11:47:38 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	200.66.208.252
11/21/06 11:49:07 AM	se	google	hipaaGroup	www.searchemu.org	http://pagead2.googleadsyndication.com/pagead/js/adsbygoogle.js	81.208.106.64

Figure 1: Click log detail for one hour on November 21, 2006.

A quick review of the searchemu.com web site shows that it is merely a "shell" site that looks like a legitimate search portal. (See Figure 2) However, there is no real content on the site, except for content syndication ads by Google. (In a not too clever disguise, even clicks on the "about us" page provide a list of ads!) This is a classic click-farm. It is basically a web site designed to look like a portal or search engine, but is really an engine designed to serve ads for click fraud. (Note: Since the initial version of this paper, searchemu.com is no longer showing ads from Google.)

Similar clicks from similar sites were found throughout the logs, occurring at all hours of the day and from sites all over the world. Searchemu.com has many cousins at searchemu.org and many other URLs. Our research has uncovered hundreds of similar sites. The organization and sophistication of these sites is also increasing. Some examples include 10bestsites.com, 2oos.org, and ultrasites.cc. Most of these sites use multiple domain extensions, including .info, .com and .org, so they escape blocking based on domain name.

A sure indicator of click fraud is a large number of clicks coming from sites that have no relation to your business or keywords. In the example, our test ads had keywords related to a popular healthcare regulation called “HIPAA.” Popular business terms, such as “mortgage”, “loans”, or “insurance” have become favorites of click farming sites because of their high cost-per-click. The higher the cost-per-click for a given keyword, the more revenue is generated for the click farm.

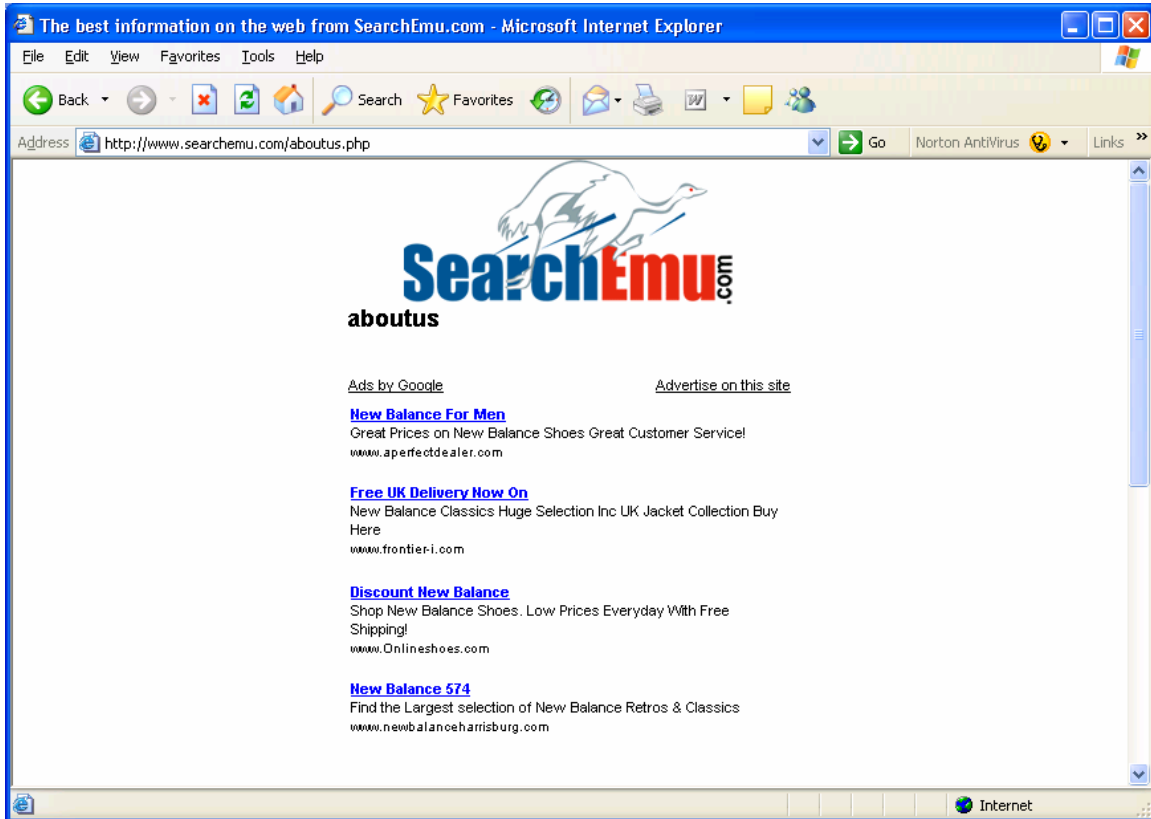


Figure 2: A classic click-farm at searchemu.com

Click True maintains a growing “blocklist” of web sites that follow similar patterns of click fraud or low value clicks. A “top 100” list of the most potentially damaging sites is available with a free trial of our audit technology available at www.clicktrue.net.

Other Sources of Low-Value Clicks

Low-Value Clicks versus Fraud

When looking at the problem of click fraud, it is important to distinguish what we call “low-value” clicks for clicks that appear to be blatant fraud. We define “low value” clicks as repetitive clicks from sites that seem to have no direct relation to advertising keywords, but generate a large volume of clicks that never convert to leads. Some examples of sites generating low-value clicks that advertisers should be weary of include domain parking and community-driven sites.

For example, our test ads also received a large volume of clicks from a site called www.mylot.info. When we blocked this site, it reappeared in our logs under various URLs including mylot.com and mylot.org. A visit to mylot.com reveals a community-driven web site, where each page of user content is sprinkled with ads on various topics from Google's AdSense™ network. (Figure 3).

While evidently a real web site with some content, this site pays users to browse and post information on their site. There is a large a growing network of these sites which all participate in the AdSense™ network. Other web sites such as Net's Reward (<http://netsreward.com>), are more explicit, and advertise that they pay people to browse and click on ads. Advertisers that focus on business-related terms should be careful of these sites. Within our tests, none of the clicks from these sites resulted in a meaningful conversion.

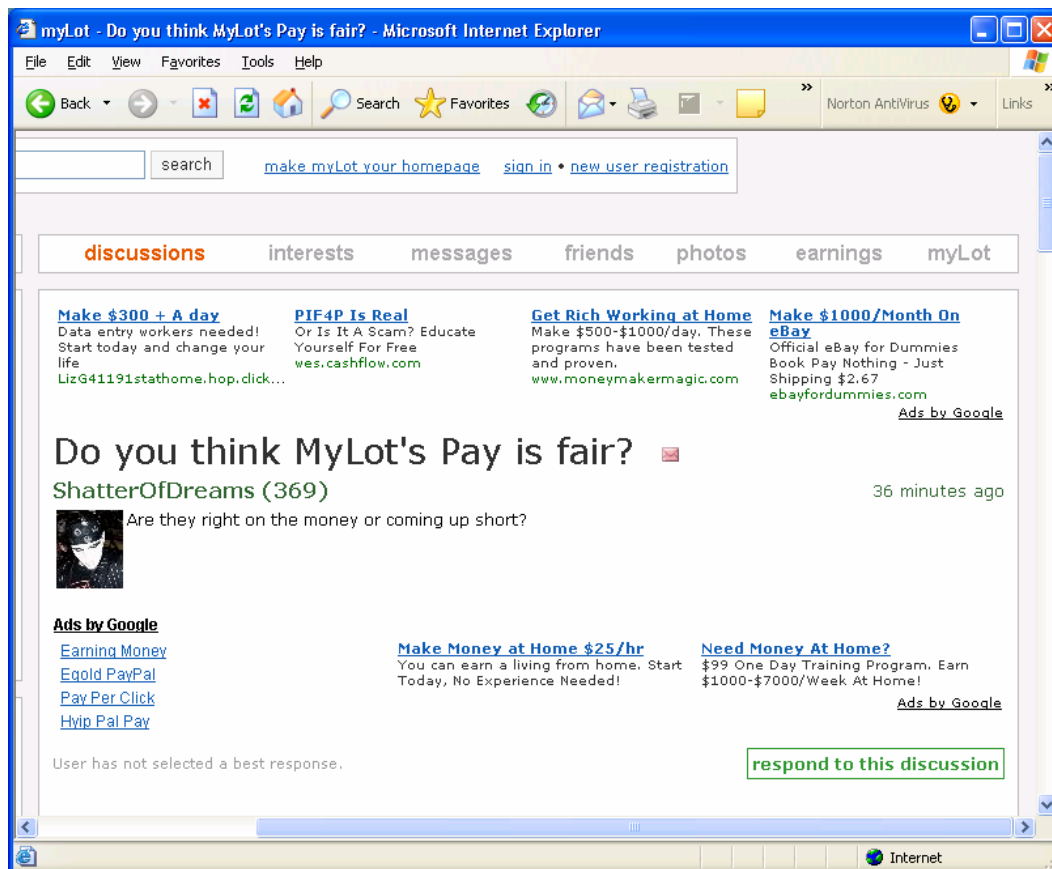


Figure 3: Example of Content Syndication ads on user sites. This page of content shows at least 10 different ads from Google's network.

Domain Parking

Advertisers need to be aware of another related problem within content syndication networks. Within the last year, Google has struck deals with domain registrars that allow the registrars to place ads on the “parked” home pages of registered domain names.

It turns out that this is now common practice among domain registrars and has become very profitable. In a recent article in Business 2.0 ^[4], the CEO of a large domain registrar stated that his company makes *only* \$12,000 per day from these ads. Other internet pioneers are seeing green, and are developing networks of thousands of domain names with nothing but ads on the site. The idea is that people oftentimes type the exact words they are looking for into the browser URL window. The people who own the domains currently receive no revenue from these sites. A more recent article in Business 2.0 reports that certain individuals own banks of hundreds of thousands of domains generating millions of dollars per year in ad revenue

Our own research shows that we routinely received clicks from parked domains, as the next example shows.

Domain Parking Example

In another example from our own test campaigns, we received clicks from a domain parking service with a DNS name of “oingo.” The click log looked like this:

```
10/30/06 04:54:21 AM se google hipaaGroup http://apps5.oingo.com/apps/domainpark/d... 124.157.229.66
```

When we looked at the web page that was referring these clicks, it was an automatically generated web page that included Google ads, as well as links to other related domain name pages with still more ads (Figure 4).

An attempt to trace the “oingo.com” domain name led to a company called Applied Semantics, which was acquired by Google in 2003. This brings up an interesting question: Do search engines own sites that are generating PPC dollars from their own advertisers?

This is certainly a grey area. While one could argue that this will still provide targeted traffic to an advertiser, these sites start to look a lot like click-farms. And it would be extremely difficult to detect if the companies began paying individuals to drive traffic to these sites. In the end, advertisers should carefully review their data to see if clicks from these sites generate any real quality leads.

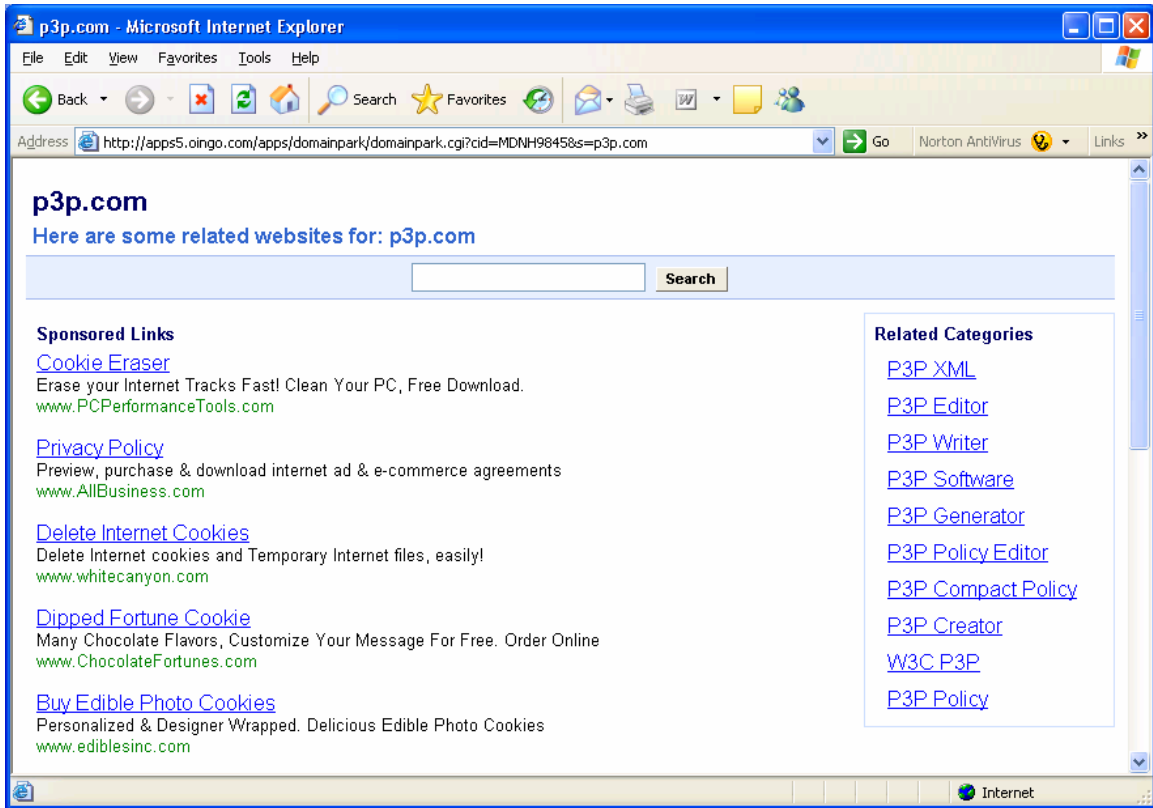


Figure 4: Domain parking with syndicated content ads

MySpace and other social networking sites

Our research also showed an increasing number of paid clicks coming from user-generated social networking sites such as MySpace and YouTube.com. While there may be legitimate advertising on these sites, most business-to-business marketers would probably not be interested in paid clicks from social networking sites. Our research showed that these clicks rarely provided value and were most-likely another easy way to click farm, since setting up pages on these sites is easy and provides another level of indirection.

Evading Detection

Google and other PPC networks attempt to detect click fraud by various methods, such as stopping multiple clicks from the same IP address. To avoid detection, attackers have become more sophisticated, using a variety of techniques, including proxy servers, DNS hijacks, and multiple ISPs to generate fraudulent clicks from different IP addresses.^[5,9] Many of these attackers have simply recruited networks of individuals to click on various ads within their network for a share in the profits.

Users are instructed to click on different ads and different times to elude detection.
[6]

Some attackers are even going beyond the simple click and generating fake “conversions” by filling out web forms with bogus data. Simple web programming scripts can be used to fill out web-based forms with fake data. If a form is filled out and submitted, this will often generate a “conversion” by triggering another script. Our own test site has received many of these as the number of fraudulent clicks has rapidly increased.

The problem of unsolicited email (SPAM) has followed a similar growth path. Security pundits announced the “end of SPAM by 2004.” Instead, sophisticated methods to avoid filters and armies of thousands of computers in “botnets” have driven SPAM to over 50% of all email traffic.

Since Google, Yahoo, MSN and other paid search companies do not provide details as to the source and timing of paid clicks within content syndication, click-farming fraud is very difficult for advertisers to detect. Detecting click fraud generally requires the use of a third-party auditing tool, or a detailed analysis of web site logs.

While each of the major search engines declares that they are vigorously battling click fraud, Google and others provide very few public details as to their exact methods for determining fraud. Whatever the details, our research indicates that today these fraud algorithms are having little impact, as the network of fraudulent sites is growing rapidly. Therefore, it is up to advertisers to detect fraud on their own sites.

Click fraud detection and prevention

Our research suggests that click fraud is growing so rapidly, than most advertisers using content syndication are experiencing click fraud. In this section we discuss some options for auditing, detecting and preventing click fraud. There are both direct and indirect methods of detecting click fraud and low value clicks.

Indirect Detection - Signs of Click Fraud

As we mentioned previously, Google and other large advertising sites do not provide enough detailed reporting to directly detect click fraud. However, advertisers can detect *patterns* within the standard reports that indicate possible click fraud. Most online advertisers begin to suspect click fraud when they see the following patterns in their paid search:

1. **Increase in click rates with few conversions** – One sure sign of click fraud is a drastic increase in the number of clicks without any increase in conversions. The “cost per conversion” numbers reported within Google and Yahoo rise dramatically. In our test campaigns, cost per conversion increased over 100%.

2. **Large growth in advertising impressions on Content networks** – Another sure sign of click fraud is a drastic increase in the number of impressions for ads within the content network. This happens when your ad is suddenly being triggered by keywords from a click farming site. In our case study, one of our ads with a very popular keyword had a 1000% increase in impressions within only 10 days.
3. **Early depletion of daily budgets** – As click fraud increased, advertisers will see their daily budgets become depleted quickly. This is especially true when advertisers enable the content network within their PPC campaigns. In these cases, clicks from both sources will hit the budget.

While these indicators can suggest problems with click fraud, the only way to accurately detect and measure the impact of click fraud is using detailed click auditing.

Direct Detection - Click Auditing

As our examples show, the first step in detecting click fraud is to obtain detailed auditing of your paid clicks. Typically this requires advertisers to include special tracking characters in the URL of their paid search ads. All of the major search engines, including Google and Yahoo, allow advertisers to specify target URLs with special characters to track clicks and conversions for online ads.

Figure 5 shows a typical detailed audit log from a pay-per-click ad campaign. The log entry shows the time of the click, which ad campaign it came from (organized by category), the keyword used in the search, the referring URL, and the IP address of the end-user to performed the click. The log nicely shows the difference between clicks that came directly from Google search, and which clicks came from ads on the content network. This is the type of detailed report required to identify click fraud on content syndication networks.

Landed	Category	Campaign	Segment	Keyword	Referrer	User IP
10/30/06 09:20:29 AM se	google	Policy2		www.searchemu.com	http://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	203.124.0.245
10/30/06 09:45:19 AM se	google	Policy2			http://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	219.79.18.85
10/30/06 09:56:06 AM se	google	Policy2			No referrer	213.146.148.180
10/30/06 09:58:55 AM se	google	Policy2			http://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	196.12.159.71
10/30/06 10:28:41 AM se	google	Policy2		www.searchtorpedo.com	http://pagead2.googlesyndication.com/pagead/js/adsbygoogle.js	85.130.29.79
10/30/06 01:21:49 PM se	google	Policy2			http://www.polies.com/home.php	196.205.201.13
10/30/06 01:38:02 PM se	google	Policy2		security policy writing	http://www.google.com/search?hl=en&lr=@q...	70.183.62.113
10/30/06 03:44:43 PM se	google	Policy2		Data retention policies	http://www.google.com/search?q=Data rete...	67.93.0.2
10/30/06 03:58:53 PM se	google	Policy2		document security policy templates	http://www.google.co.za/search?hl=en&sa=...	198.54.202.234
10/30/06 05:24:06 PM se	google	Policy2			No referrer	213.226.118.163
10/30/06 06:33:50 PM se	google	Policy2			No referrer	131.225.35.2

Figure 5: Example detailed click referral report

Reducing the Impact of Click Fraud

It is unreasonable to assume that any advertiser can completely eliminate click fraud. However, there are several methods for reducing the cost of click fraud within your on-line advertising campaigns.

Disabling Content Syndication

The simplest and most effective way to reduce your exposure to click-fraud is to disable your ads within the content syndication network. Each of the major search advertisers provides this feature. While this may be the easiest, it may not be optimal for all businesses. Some businesses receive a large amount of legitimate traffic from ads on the content network. Of course, disabling the content network will only prevent “click-farming,” and won’t address direct attacks on the search sites.

Pay-Per-Click Auditing

Some businesses are devoted to click-fraud detection and auditing. These services provide detailed evidence of possible click fraud patterns. The model is that advertisers present this data to Google or other search companies, and attempt to obtain a refund for the fraudulent clicks.

Our experience and the experience of others suggest that this method is unlikely to be effective. In our experience, the process of receiving refunds from Google is time consuming and rarely generates a refund. Even when presented with detailed audit logs from obviously fraudulent sites, Google maintained that these were “valid” clicks. In fact, a review of Google’s “User Agreement” clearly shows that Google is the final judge and jury on what constitutes a valid click. So advertisers are left with few options if they are rejected by the search engine.

Site Blocking

One final solution for businesses that choose to advertise on the content network is site blocking or “blacklisting.” Currently, Google enables advertisers to block ads from appearing on certain sites within the content network. This feature requires advertisers to manually enter the list of known domains into the blocked site list.

Click True research suggests that site blocking is a very effective way to reduce the impact of click fraud and other low value clicks. Within our test campaigns, we were able to reduce the number of fraudulent clicks from over 80% to less than 10% over a three week period. Using blocklists for each campaign, cost-per-lead was reduced by over 50% within the content syndication network.

As of this writing, each campaign within Google can have a blocklist of up to 500 sites. Neither Yahoo! Search nor MSN Search currently provides blocklist features.

Click True Solutions

Click True provides several products designed specifically for detecting and preventing click fraud. Unlike other services which provide only click audit data, Click True allows advertisers to quickly identify possible click fraud and build custom blocklists of the offending sites. Click True solutions based on our own experience with click fraud among various search engines.

Click View Auditing

Click True provides detailed click auditing services specifically designed to quickly identify and respond to click fraud. Using a simple javascript code placed on various landing pages, advertisers can track the source and quality of clicks within any content syndication network. Clicks are immediately flagged with a "rating" level of possible fraud based on patterns and referrals from our master list of sites known for low-value clicks (Figure 6). Advertisers can quickly review suspected sites and add them to custom blocklists which can be saved and exported to Google ad campaigns.

Internet advertisers can sign up for a free trial of our Click View auditing service by registering at www.clicktrue.net.

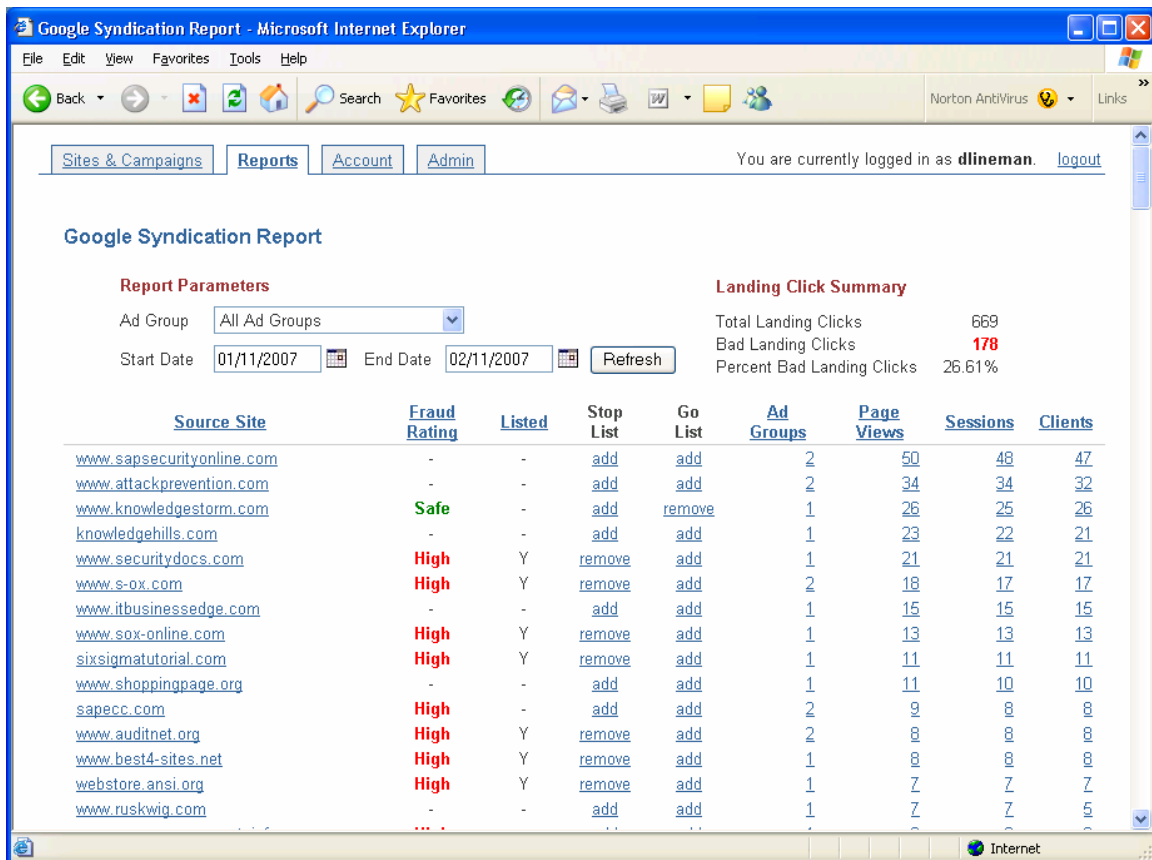


Figure 6: Click True Syndication Report

Click True Blocklist

To help reduce the impact of click fraud, Click True maintains a master list of web sites known to generate fraudulent or low-value clicks. Click True uses a proprietary web crawler to identify web sites based on known fraud patterns. The master blocklist currently contains over 5000 web sites and is growing rapidly. Advertisers can use this master blocklist to identify possible click fraud within their campaigns. Registered users of the Click True auditing service can build their own custom blocklists based on their own web site keywords. The blocklists can be imported easily into Google campaigns to immediately reduce the impact of click fraud.

Advertisers who register for the free trial of our Click View auditing service also receive access to our "Top 100" sites from the master blocklist. Using this free service, advertisers can immediately begin blocking some of the most dangerous click fraud sites. Advertisers can upgrade to our premium service and build an unlimited number of custom blocklists based on their own campaigns.

To help maintain the quality of our master blocklist, we encourage online advertisers to submit known fraudulent sites by visiting our submission page at <http://www.clicktrue.net/submitsite.html>.

Click True SafeSite Network

To enable trust within content syndication, Click True has created the SafeSite™ network of safe advertising sites. The SafeSite™ network is a list of web sites available for hosting ads within content syndication networks. All SafeSite web sites have been approved by Click True and other online advertisers and are known to generate legitimate traffic. Membership in the SafeSite network is free to add sites that apply.



Web sites that host legitimate ads can also apply for the AdSafe Seal. The AdSafe seal lets web users and others within the advertising community that this web site is verified as "safe" by online advertisers. Web sites with the SafeSite network can display the AdSafe logo on their web site. Users can then click on the logo to immediately verify membership. Web sites are encouraged to apply for free membership in the SafeSite network by visiting Click True at <http://www.clicktrue.com/safesite.html>.

Conclusion – Advertisers must take action

Search Engine Responses

The “official” line from Google, Yahoo and other search engines is that they have a handle on click fraud. In fact, both Yahoo and Google lost class-action lawsuits for click fraud in 2006. As a result of these suits, the companies were required to increase their attempts to detect and eliminate fraud. According to our own forensics, detecting these fraudulent web sites is relatively simple once detailed log information is obtained. However, our data also suggests that many of these same clicks are not currently detected or blocked. The number of sites and the potential revenue they generate is simply too large. When we add parked domains, the number of sites is easily in the hundreds of thousands.

Advertisers on their Own

Since paid-search companies indirectly benefit from click fraud, it remains to be seen how much will be done. In a recent article in Fortune, CEO Eric Schmidt acknowledged Google’s content network as a major differentiator between Google and its competition. According to Google’s own reports, as much as 39% of the revenue comes from content advertising. With the possibility of widespread fraud across its network, it remains to be seen if Google will begin to address the problem more aggressively.

In the meantime, advertisers are left to fend for themselves. Advertisers concerned with click fraud are encouraged to obtain detailed auditing of their click data or block content advertising entirely. Advertisers who use content syndication networks should consider blocking known networks of fraudulent sites.

About Click True

Click True, Inc. is a leading provider of online advertising solutions that help eliminate click fraud. Click True solutions allow organizations to dramatically increase the return on investment within online advertising by detecting and eliminating unwanted clicks. Click True’s leading technology allows companies to detect and stop click fraud before it happens. For more information, visit our web site at www.clicktrue.net, email info@clicktrue.net or call Toll-free at 1.800.829.9955.

© Copyright 2007. Click True, Inc.

All registered trademarks and copyrights are understood and recognized by Click True. Click True is not affiliated with Google, YAHOO!, or MSN. AdSense™ is a registered trademark of Google. No part of this publication may be reproduced, stored in a retrieval system, or transmitted by any form or by any means without the prior written permission of the publishers.

References

1. **Internet Advertising Bureau (IAB)** – Quarterly report on online advertising revenue. <http://www.iab.net/>
2. **Google AdSense Network** - Description of the AdSense content syndication network at Google.com. <http://www.google.com/adsense/>
3. **Click True Site Black List** – Current list of known click farms from our own research. www.clicktrue.net/clickfraud.html
4. **Who's Your Go Daddy?** – Article in November 2006 issue of Business 2.0.
5. **'Click Fraud' Threatens Foundation of Web Ads** – Washington Post
http://www.washingtonpost.com/wp-dyn/content/article/2006/10/21/AR2006102100936_pf.html
6. **Clicks that sting.** *Armies of citizens have been lured into fraud rings* – San Francisco Chronicle
<http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2006/10/02/CLICK.TMP>
7. **Click-Fraud threatens river of gold** – Sydney Morning Herald
<http://www.smh.com.au/news/biztech/click-fraud-threatens-online-river-of-gold/2006/11/06/1162661616360.html>
8. **How Click Fraud Could Swallow the Internet** – Wired Magazine, Jan. 2006
<http://www.wired.com/wired/archive/14.01/fraud.html>
9. **Detail of a Pay-Per-Click Hijack**
<http://www.lurhq.com/ppc-hijack.html>