



The Web: Catching 'click fraud' online

By Gene J. Koprowski

June 15, 2005

An auto repair shop owner buys some online ads and thinks he snagged a bargain by negotiating a deal with the advertising agency to pay only when Web surfers click on the banners. It sounds like a good deal, until the owner receives the bill: His \$1 per click deal turns into a \$1 million invoice, and he has no idea how many of the clicks came from legitimate prospects.

Welcome to the world of Internet click fraud -- crimes emerging from an increasingly popular practice of pricing online ads.

Until recently, online advertisers had no way of knowing whether they were being victimized by click fraud, experts told UPI's The Web. Now, however, software and services from firms such as WhosclickingWho.com, PPCTrax.com, Clicklab.com and ClickFacts.com are helping to discern the real visitors on the Web from the imaginary ones.

"There is a lot of click fraud on the Internet," said Danay Escanaverino, director of marketing at Global Resource Systems in Plantation, Fla., a pioneering firm in the Web marketing field.

Many kinds of click fraud occur online. Some of it is perpetrated by competitors of a business, who click on their rivals' ads repeatedly in order to drive up their costs and even try to push them into insolvency. Another malicious fraud occurs when hackers click on ads or search for key words they know have been purchased for keyword searches, such as "car dealer" and "Chicago."

Perhaps the most egregious click fraud comes from Web sites that bill their advertisers for an imaginary number of clicks, simply to boost their advertising revenue.

"The primary question for marketers is, 'How do you determine which of those clicks are from real customers?'" said John Enright, vice president of marketing at Affinity Internet in Ft. Lauderdale, Fla., a Web services provider for small businesses.



The threat of fraudulent clicks is dominating the consciousness of the online ad industry today. The obsession is to "identify malicious vs. legitimate traffic before it adversely affects the network," said Karen Regan, a spokeswoman for Mazu Networks Inc. in Cambridge, Mass., which makes software to track malicious behavior on networks.

The new software is helping contain the problem, experts said.

"You can monitor the visitors to a site or an ad and determine what search engine they used, whether it was Google or Yahoo! or Ask Jeeves," said Pam Watkins, president of Fueled Communications in Dallas, an Internet marketing firm.

The tools also can help determine where a user entered a Web site -- an important fact, because many do not enter via the main page, but through links they may have seen elsewhere, or received in an e-mail from friends. The software can examine which parts of a Web site visitors trolled and how much time they spent there.

Controls can even prevent fraudulent clicks while they are happening. WhosClickingWho.com shows pop-ups to warn clickers if they are repeatedly clicking on the same ad.

Advertisers want these kinds of protections because the ad-click business has become a \$4 billion-a-year industry. The biggest portion of Google's revenues comes from word-search clicks, so it, as well as Yahoo!, have implemented in-house measures to ensure the integrity of the data. Google is also said to have refunded clients who were apparently overcharged for clicks.

Companies with a major online presence, like NYTimes.com, USAToday.com, Weather.com, iVillage.com and others use a service from Tacoda, a company in New York City, to segment, target and measure online ad campaigns, a Tacoda spokesman said.

Some related issues worry online advertisers in addition to click fraud. One of the metrics used to measure the traffic of a Web site is the number of "unique visitors" -- that is, how many different individuals visited a given site in a given time frame. This contrasts with the total number of clicks, which includes repeat visits by prospects.

Many consumers use anti-spyware software to eliminate cookies -- the mini-files deposited on the hard drives of Web users that are employed by sites to track unique visitors. Now, advertisers are fighting back with new technology. United Virtualities, also in New York City, has developed a backup ID system for cookies set by Web sites and advertising networks. The technology, called the Persistent Identification Element, is tagged to a user's Web browser. It provides advertisers with a unique identification, just like a cookie, and the tags cannot be deleted by any commercially available anti-spyware software today.



"All advertisers, Web sites and networks, use cookies for targeted advertising, but cookies are under attack," said Mookie Tenenbaum, founder of United Virtualities. "They are being erased by 40 percent of users, creating serious problems. PIE will give publishers and third-party providers a persistent backup to cookies, effectively rendering them unassailable."

The PIE software is contained in just one line of code, he said.

Tenenbaum said that from the advertiser's point of view the erasure of cookies constitutes a threat to an array of server-side applications, not just advertising, but also site registration and traffic counting.

