Click-through fraud hits
Simon Hayes
The Australian
JULY 27, 2004

A HUGE jump in click-throughs on an online advertisement is normally good news for the average small business, but for Perth software developer Dave Hawley a leap in visits to his site meant bad news.

The problem was that the extra traffic was not translating into sales at anywhere near the rate he expected, and his company, OzGrid Business Applications, was paying to have the Google AdWords advertisements displayed on sites affiliated with the search giant. Hawley is not sure of the cause, but suspects he was the victim of the latest scam to hit the internet – click-through fraud – which occurs when competitors or owners of sites that receive commission for displaying banners, artificially inflate traffic generated by the advertisements.

Advertisers on Google and other search engines pay to have their listings displayed ahead of others on a per-click basis. Advertisers on the Google AdWords network pay for their advertisements to be displayed on third-party sites that have affiliate agreements with Google.

"I had a problem with a high click-through rate without those clicks being converted into sales," Hawley says. "We were getting 50 to 100 clicks a day on a certain ad that were not converting into sales at the same rate as ads displayed on the Google search engine."

Hawley found that when he removed his advertisements from Google network sites, and displayed them only on the search engine, click-through rates fell, and return on investment rose.

"We were paying $200 in a week, so I pulled the plug straight away," he says. "We decided not to run our ads on other peoples' sites."

Despite the use of web bots and so-called pay-to-click work-from-home schemes operating in some developing countries, search operators say they are winning the battle against click fraud.

Google says it has deployed technology to crack down on the problem.

"We apply our expertise in search technology to the click fraud problem, and employ a dedicated team to analyse clicks," a Google spokeswoman says. "If we determine a click is fraudulent, we will not charge the advertiser.

"Google takes this issue very seriously, and we continually work to improve our detection mechanisms for fraudulent clicks."

In June, a San Francisco man, Michael Bradley, was arraigned in a US Federal Court on charges of extortion and wire fraud in connection with a software package he claimed could allow users to defraud Google.
The 32-year-old is alleged to have tried to extort $US150,000 ($210,000) from Google, claiming he had developed a tool that would create fraudulent clicks. He has pleaded not guilty.

Click fraud appears to be limited in Australia so far.

Overture's Australian managing director, Mel Bohse, says the company, which has been operating in Australia for six months, had not received any complaints.

"Overture uses proprietary click-protection technology, so if we believe the clicks come from a machine or from people without a bona fide interest, we would look into it further, and the advertiser would not be billed," she says.

"We have experienced no difficulties and have had no complaints."

Chris Brooks, general manager of Sydney affiliate marketing company clixGalore, says it has deployed technology to stop click fraud.

Affiliate programs pay website operators to host ads, and pay them for every visitor who clicks through to an advertiser's site.

"Fraud does happen, but we have the technology to prevent it," he says. "You have to be aware of it, but if you have the technology in place, it deters people."

This report appears on australianIT.com.au.