

Yahoo Used in Spyware Click Fraud Scheme

By Jim Hedger, StepForth News Editor, [StepForth Placement Inc.](#)

Through its Overture pay per click search division, Yahoo has been found facilitating fraudulent click activity generated by known [spyware](#) makers including 180solutions, Intermix, and Direct Revenue. [The Spyware - Click-Fraud Connection -- and Yahoo's Role Revisited](#), (Apr. 4, 06), shows how at least a dozen different spyware firms redirect Internet users searches through their servers, inserting Overture ad links on unrelated websites or with pop-ups triggered by those sites.

[Ben Edelman](#) is a researching PhD candidate at the Department of Economics at Harvard. In his follow up to a Sept. 5, 2005 paper, [How Yahoo Funds Spyware](#), Edelman documents a web of relationships between Overture and, "... a startling number of notorious spyware programs."

A recent graduate of Harvard's Law School, Edelman lays out his argument methodically, briefly explaining what constitutes click-fraud and ways in which it happens. He also notes that Yahoo has tried to sever its relationships with the offending firms, often unsuccessfully, as they (spyware makers) continue to include Overture code in their spyware programs. "When Yahoo terminates one fraudster, that fraudster's partners find another way to continue operations."

A few paragraphs down, he notes, "After I highlighted these vendors in my August [report](#), it seems Yahoo attempted to terminate its relationships with them. Yet 180 continued not just to show Yahoo ads, but also to perform click fraud, as documented." Eliminating spyware click-fraud is likened to a game of Whack-a-Mole. When Yahoo moves to shut down one channel, another is immediately opened.

Edelman calls the methods outlined in his study, Spyware Syndicated PPC Fraud. "Suppose X, the Yahoo partner site, hires a spyware vendor to send users to its site and to make it appear as if those users clicked X's Yahoo ads. Then advertisers will pay Yahoo, and Yahoo will pay X, even though users never actually clicked the ads."

Using four detailed case studies, conducted between Dec. 17, 2005 and Apr. 2, 2006, Edelman traces traffic generated on test PCs known to be contaminated with various spyware products. Using packet logs, screenshots, images and video, Edelman effectively demonstrates how each of his conclusions was drawn.

In one case, he shows a link inserted on a New York Times document anchored to the word "prime minister". The link was placed by Qklinkserver and would not appear on an uninfected PC. It was placed without permission from the Times. When clicked, the link sent traffic through Overture to a PPC advertiser.

The study names, Intermix, 180Solutions, Nbcsearch, eXact, Ditto, Look2me, Ad-w-a-r-e, Improvingyourlooks, Qklinkserver, Srch-results, Claria, InfoSpace, SurfSideKick, TrafficEngine, HotBar and IBIS, as companies directly involved in spyware click-fraud.

Edelman goes on to note, "Yahoo's problem results from bad partners within its network." Because it distributes advertising to third parties who might in turn syndicate those ads to others, Yahoo has no real control over how its ad codes are used to generate clicks.

The problem of click-fraud is an ever-present danger in pay per click advertising, one that troubles Google as well. David Utter at [WebProNews](#) quotes Google CEO Eric Schmidt saying, "Believe me, as a computer scientist, we have the ability to detect the invalid clicks before they reach advertisers", juxtaposing the quote against the [\\$90million settlement](#) Google reached in the Lanes Gift and Collectables class action.

Edelman closes his study with a realistic but stern warning. The problem is not going to go away. In fact, it is likely to get worse. The market for spyware vendors is drying up, mostly because consumers are aware of the problem and corporate advertisers no longer want to be associated with it. The spyware makers are increasingly turning to more complex systems, including the money-rich PPC market, to find susceptible targets.

Spyware makers have long been known leeches on the Internet. Some, such as Claria receive support from large venture capital firms such as US Venture Partners and Technology Crossover Ventures. In some cases, they have become parts of much larger companies, including some of the world's largest advertising firms. For example, Intermix is a division of News Corp and owns the social network MySpace.Com.

Now that several noted spyware makers have been shown to be involved with click-fraud scams, Yahoo and Google should be moved to immediate action. Aside from protecting the integrity of their PPC programs and maintaining the trust of their advertisers, they must be aware that the New York Attorney General's office is watching.

In a speech sponsored by TRUSTe and the International Association of Privacy Professionals, Ken Dreifach, chief of the Internet bureau in the New York State Attorney General's office, said that entities such as Google and Yahoo can be held accountable for how their affiliates use their content.

In an article published by [MediaPost](#), Shankar Gupta quoted Dreifach saying, "You don't want to ever assume that the existence of intermediaries, whether it's two or six, is going to immunize you from liability."