



Go direct to ...

IDG.net SERVICES  
& PARTNERS  
FREE Newsletters  
Compare Prices  
CIO  
ComputerWorld  
PCWorld

THE STANDARD  
ARCHIVE:  
NEWS & ANALYSIS  
Money & Markets  
Tech & Telecom  
Media & Marketing  
Policy & Politics  
Columns

THE STANDARD  
ARCHIVE:  
PRINT EDITION  
Past Issues

SEARCH

GO

IT topics at IDG.net

- [E-Business](#)
- [Personal Computing](#)
- [Programming & Development](#)
- [Networking & Systems](#)
- [Mobile & Wireless](#)
- [Security](#)
- [Enterprise](#)
- [Management & Careers](#)



## Bogus Clickers Are Cheating Ad Networks

By Jacob Ward  
Issue Date: Apr 19 1999

**Net advertisers may have bigger problems than declining click rates. Now they have to unravel the mysteries of the phantom click.**

When is a click not a click? On banner networks like **DoubleClick (DCLK)**, **LinkExchange** or **Flycast** ([dossier](#)), member sites get fees when users click on member banners placed on those sites. But a growing number of clicks are coming not from potential customers, but from pieces of shareware that mime customer behavior and help their users collect the fees. It's easy, it's cheap and it's legal.

Banner Brokers, a Malibu, Calif.-based ad network, found that it was losing a chunk of money to the scam each month. "We discovered that a group of hackers was killing us. And I mean killing us," says VP Dan Clements. "We thought phantom clicks accounted for under 10 percent of our traffic, but it turns out to be anywhere from 10 percent to more than 20 percent. There's no way to know." Clements stumbled on a site that offers a piece of banner-clicking shareware to hackers, along with a list of easy targets. Among the targets were ValueClick, LinkExchange and his own company's site. So Clements had his lawyer fire off a letter to the site's creator, Jason Pearsall.

"We're providing the gun," replied Pearsall in a January e-mail, "but whether one person shoots another person with it is not our liability."

Those shootings are happening all over the Web. Banner Brokers discovered that a Xoom.com site registered to John Lee in Pasadena, Calif., was getting paid for false clicks. During his last fee period (the last half of December), Lee received \$50.36. "We went into the IRC chat room, found him there and e-mailed him that we'd be shutting down his membership," says Clements. "Within five minutes he was in our system, trying to pull his social-security number off our books - but we'd already frozen him."

Rather than file a potentially fruitless lawsuit, Clements offered Pearsall's group - Fort Myers, Fla.-based Team Asylum - a payoff to reveal its methods.

According to Team Asylum, the scam works like this: A group

IDG.NET T  
Updated 1:

[SCO boosts with acquis](#)

[Amazon ha higher sale:](#)

[AOL Time V strong Q2 c SEC probe](#)

[i2 wraps up earnings fo](#)

[Software s: slide](#)

[DHS had lit sign Micros security fla](#)

[Business O rival Crysta](#)

[California j: settlement](#)

[EDS adds M analysis to](#)

[AOL sells di business fo](#)

7/24/03

of 200 hackers sets up identities in an Internet Relay Chat room, whereupon each member downloads the shareware. Each hacker launches a Web site that carries banner ads from an ad-network customer, often in exchange for a per-click fee.

Each hacker can then use a command that fools the banner network into thinking that all 200 IRC users have clicked on a banner on the hacker's own site. The program can be tailored to seem very realistic. If all goes well the hacker receives a fee for each click. Some hackers aren't in it for the money; they just like the game.

Don Sausa, a member of Team Asylum, agreed to take part in Clements' project. "We tested the program on other companies with dummy accounts," says Sausa. "So far, the banner companies don't detect false clicks."

Deb Whitman, VP of marketing and member services at LinkExchange, says the scam is a common annoyance but claims it's not a serious problem. "It happens, but we absolutely catch it," she says. "We police it to make sure our members aren't being harmed."

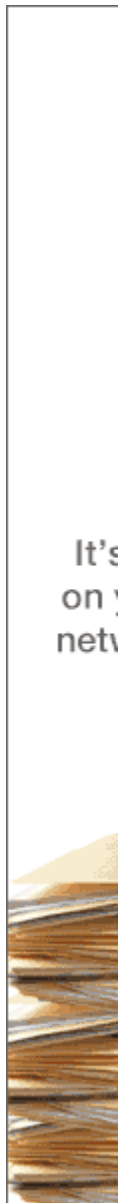
A report Team Asylum issued to Banner Brokers, however, pinpointed LinkExchange as the most susceptible network of a group that included ValueClick, DoubleClick, 24/7 Media (TFSM) and Flycast. According to that report, "Microsoft (MSFT)'s LinkExchange has the poorest verification system tested so far."

Emanuel, a hacker-turned-informant, says in an e-mail that as LinkExchange and other companies upgrade their protective measures, hackers make constant improvements to the shareware, which is known as BC. "They do know about cheaters, and they keep trying to develop a system that would eliminate any chances of false clicks," Emanuel writes. "However, BC script just released a new version, [in which] each click ... appears to be random."

Fraud has inspired ValueClick to change its typical member profile, says Guy Hill, director of business development at the company, which got an "able to detect false clicks" rating from Team Asylum. "We've had to move away from the smaller pool of sites," says Hill, who also notes that ValueClick now accepts only a few foreign-language sites. "These days, we turn down 80 percent of the sites that apply."

To shore up the industry's defenses, Banner Brokers' Clements will announce at Internet World this week the formation of AdCops, a database of hacker identities that banner networks would share on a subscription basis.

Banner networks, which rely on proprietary technologies to maintain a competitive edge, are not accustomed to discussing



such matters with their rivals. That may have to change. "We haven't talked about it much with other sites," says LinkExchange's Whitman. "We'd be open to the possibility." If the banner networks don't team up, phantom clickers may find it easier to remain a step ahead.

You don't need a library card to access one of  
libraries of IT White Papers on the pla

[Home](#) | [Service Agreement](#) | [About Us](#)  
Copyright © 2001 IDG.net. [IDG.net Privacy Policy](#)