WEB MARKETING

How to Combat Online Ad Fraud

by Benjamin Edelman

MARKETERS ARE LEARNING that advertising online can be like going down a rabbit hole into a world where many things are not what they seem and tricksters are all too quick to make your ad dollars vanish. One advertising network I recently examined found that at least 14% of its online ad placements were tainted by fraud or violations of its policies.

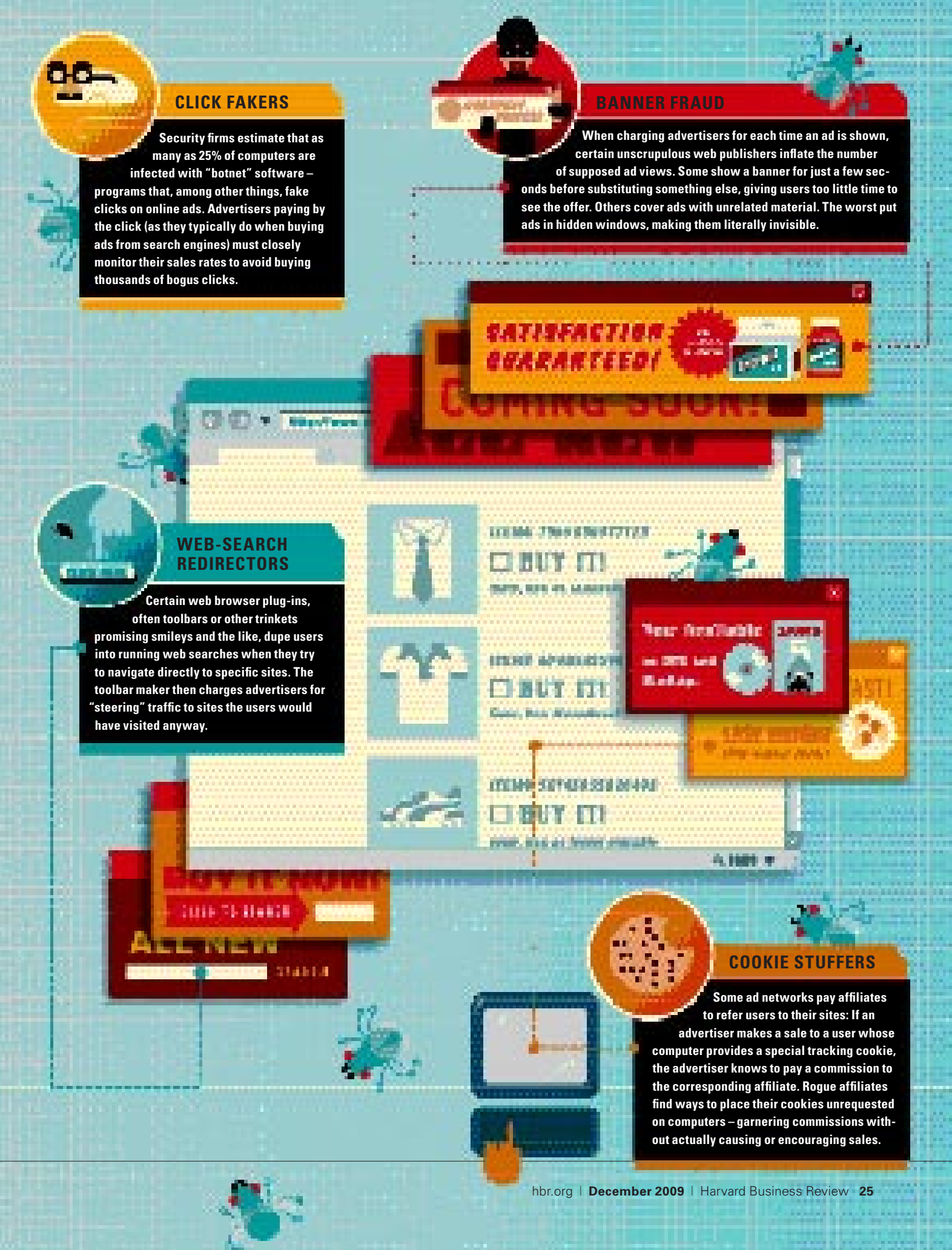
Understanding the pitfalls can offer a measure of protection. Advertisers should redouble their efforts to verify partners' identities and practices and should question measurements of ad effectiveness, which can be completely inaccurate even while being very precise.

Delaying payment to publishers and other partners provides additional protection. A delay should be long enough to give the advertiser or network a chance to detect fraud but short enough to keep honest publishers interested in the advertiser's business – 150 to 200 days would have been best for one ad network I recently studied. With the resulting savings, the advertiser can offer a bonus to retain honest publishers.

Delaying payment cannot replace the detailed, specialized work of exposing deceptive marketing practices. But in addition to adding leverage, it demonstrates a serious commitment to uncovering the truth. For advertisers just beginning to realize the importance of protecting themselves from fraud, paying in arrears is a good first step.

Benjamin Edelman (bedelman@hbs.edu) is an assistant professor at Harvard Business School. An expanded version of this article, with specific examples and perpetrators, will appear on HBR.org in November at http://blogs.harvardbusiness.org/hbr/now/2009/11/dark_underbelly_of_online_ads.html.

Reprint F0912D



CLICK FAKERS

Security firms estimate that as many as 25% of computers are infected with "botnet" software – programs that, among other things, fake clicks on online ads. Advertisers paying by the click (as they typically do when buying ads from search engines) must closely monitor their sales rates to avoid buying thousands of bogus clicks.

BANNER FRAUD

When charging advertisers for each time an ad is shown, certain unscrupulous web publishers inflate the number of supposed ad views. Some show a banner for just a few seconds before substituting something else, giving users too little time to see the offer. Others cover ads with unrelated material. The worst put ads in hidden windows, making them literally invisible.

WEB-SEARCH REDIRECTORS

Certain web browser plug-ins, often toolbars or other trinkets promising smileys and the like, dupe users into running web searches when they try to navigate directly to specific sites. The toolbar maker then charges advertisers for "steering" traffic to sites the users would have visited anyway.

COOKIE STUFFERS

Some ad networks pay affiliates to refer users to their sites: If an advertiser makes a sale to a user whose computer provides a special tracking cookie, the advertiser knows to pay a commission to the corresponding affiliate. Rogue affiliates find ways to place their cookies unrequested on computers – garnering commissions without actually causing or encouraging sales.