https://blogs.wsj.com/cmo/2015/05/06/ad-injection-yet-another-challenge-for-online-advertising/

CMO TODAY

Ad Injection: Yet Another Challenge for Online Advertising

By Jack Marshall
May 6, 2015 8:00 am ET

The digital media world is battling ad fraud, ad blockers, and ads that aren't viewable. There's another, less-talked-about challenge: ad injection.

Ad injectors are computer programs that insert ads — or replace existing ones — on Web pages as users browse the Internet. If users add a toolbar to their browser, for example, there's a chance that software might "inject" extra ads into the pages they visit, even if those pages don't regularly feature ads. Wikipedia's pages might be covered in banners, despite the fact they don't usually carry advertising.


DAVID CHESKIN/ZUMA PRESS

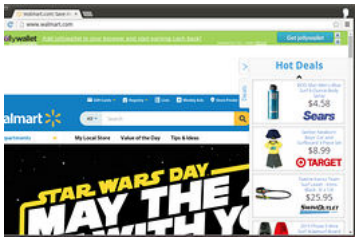
Many users aren't aware that the software they add to their browsers might behave this way, and say it's detrimental to their browsing experience. According to Google, the software can also pose serious security and privacy risks.

Ad injectors are also problematic for online publishers because they allow marketers to place impressions on their sites and alongside their content without paying them to do so, potentially costing them ad revenue.

Even the sites of retailers and other companies are affected.

Google says it has received more than 100,000 complaints about ad injectors appearing in its Chrome browser since the beginning of 2015 alone. To better understand the scale of the problem Google, in collaboration with the University of California, Berkeley and Santa Barbara, created an ad injection "detector" and placed it across Google sites for several months in 2014 to identify "tens of millions of instances of ad injection."

In total, Google said 5.1% of page views on Windows and 3.4% of page views on Mac showed signs of ad injection software during its study. It tracked ads from more than 3,000 brands appearing through ad injectors, including Sears, Walmart, Target, Ebay and others. The companies could not immediately be reached for comment.



GOOGLE

The research also unveiled the "tangled web" of ad networks and middlemen that profit from injected ads, Google said.

"Everybody has known about ad injection, but we're finally getting an idea of how many parties are involved and that there isn't a simple solution to handle this," explained Kurt Thomas, a research scientist at Google.

For example, ad injection software is often distributed by a network of affiliates that bundle it with popular downloads or hide it in malware. Then, middlemen called "injection libraries" help fill the newly created ad space by selling it on to advertising networks, which may then resell it to other networks and ad exchanges, which in turn sell it on to marketers or agencies that purchase ads on their behalf.

It's a complicated chain that often results in ads for major brands being displayed on major publisher sites without the consent of users.

"We want to shed light on this issue so publishers can take action," Mr. Thomas said.

Google itself says it's attempting to combat the issue by cracking down on deceptive extensions for its Chrome browser. It's also telling advertisers about the practice, and sharing the names of some of the companies involved. During its study, Google found 77% of all injected ads passed through one of three ad networks.

"We strongly encourage all members of the ads ecosystem to review their policies and practices so we can make real improvement on this issue," a blog post from the company read.

As with many of the challenges in the online advertising ecosystem, however, fixing them is much harder than identifying them.

Share this: http://on.wsj.com/1Jp8dmC