How advertisers and publishers are unwittingly falling victim to ad injection

Author : Julia Smith

Date : March 1, 2016

Ad injection – the malicious practice of injecting unwanted ads onto browsers without the site owner’s permission – is yet another challenge the digital advertising industry has to contend with.

A recent study by **Google** concluded that 5.5% of unique IP addresses that accessed **Google** sites showed some form of ad injection, and over 50,000 browser extensions are guilty of injecting ads.

The growth in ad injection is a problem for both advertisers and publishers. Disappointingly, some buyers bake the costs of ad injection into their marketing plans and even allow ad injection inventory within their insertion orders.

This leaves the unsuspecting publisher suffering financial losses due to ad injection, as they do not receive the revenue from ads purported to be sold on their domains.

More importantly, in a time when there is downward pressure on CPMs, imbalance between demand and supply, and revenue lost to digital ad fraud, publishers need all the help they can get to manage and fight against this growing threat.

So the first step to fight against the practice of ad injection is to understand exactly what it is and how it works.

Injected ads can manifest in various forms, including an ad that is inserted on top of another ad that has already appeared or one that replaces another entirely. It can also comprise of an ad that appears on a web page that is not intended to display **advertisements** at all. Initially, software infects users’ browsers before being distributed by affiliates who drive more installs through marketing, malware, or even social media. Once there is the required reach, the injection companies work with a number of ad networks and affiliate programmes to distribute ads to users, and generate revenue based on performance via a revenue share model.

The scale and impact of ad injection is on the rise and the key issue lies with the ad injection perpetrators – often built from a complex web of different businesses within the **digital** ad ecosystem – who have become increasingly difficult to detect. However, the industry can fight back against the ad networks that are known to be profiting from this malpractice. Should they be named and shamed? Google did just that, recently naming three ad networks known to be part of the ad injection cycle.

Yet again, a call needs to made to the programmatic platforms, trade associations, browser technologies, advertisers, and publishers to stand firm against the illicit activity of stealing. We wouldn’t allow someone to steal from our bank account without acting on it so why should we allow this to happen within our industry?

//