How Ad Fraud Ruins the Internet

Author : Eli Martin

Date : July 13, 2016

If you're in the **digital advertising** industry, you've probably heard of ad fraud, but you likely haven't done anything to protect yourself or prevent it from happening.

Billions will be lost to ad fraud this year, and anywhere from three percent to 37 percent of ad impressions will come from bots. In fact, ad fraud is on its way to possibly becoming the second largestorganized crime enterprise. With the prospects of a high payout, low risk and relatively little effort needed, it's easy to see why so many organized criminals are looking to profit from ad fraud.

It's easy to think ad fraud will never affect you, but in fact, it can affect everyone. Even those just casually browsing the web. The more you know about ad fraud, the better you'll be able to spot it. Here's how ad fraud can affect the different types of Internet users.

Online advertisers

This part seems obvious. Of course you're at risk if you're a **brand** or website **advertising** online. But do you know *how* you're at risk? Here's the different types of ad fraud for online advertisers.

Search ad fraud

Fraudsters targeting search ads are often looking to target the most popular keywords with the highest cost per click (CPC).

Search fraudsters will build websites that are stuffed with the highest priced keywords in order to generate search ads. A **brand** who wishes to advertise against these keywords will then buy ad space on the fake sites, because it'll look like a reputable publisher.

Affiliate ad fraud

Cost per acquisition (CPA) ad fraud usually involves affiliate **marketing** programs. **Brand**s will reward affiliates who talk about their product or services and push people to the website, and then those affiliates are rewarded based on the acquisition of customers.

Affiliate fraudsters use bots to direct qualifying traffic to affiliate sites. Then, by employing cookies to track that traffic, if anyone makes a purchase, the fraudster is able to siphon away the commission from the actual affiliates.

Pixel stuffing and ad stacking

Ad stacking occurs when multiple ads are placed in the same space on a web page, but only the top one is seen. When a user visits the site, an impression is recorded for all of the ads, not just the top one, which means you might be paying even though your ad was never seen.

Pixel stuffing is similar to ad stacking. It involves placing ads or video in tiny 1x1 pixels so that they're virtually impossible to see, but when a user opens the page, the publisher is still credited with an impression.

Traffic fraud

Traffic fraud occurs when publishers buy fake traffic without the advertiser's knowledge. Most purchase from third-party sites, who usually have the highest percentage of fraudulent traffic.

Lead fraud

There are two types of lead fraud: humans and bots.

With humans, it's usually in the form of click farms resulting from those "work-from-home" scams. People are paid to click on your ads and then fill out forms, making you *think* you're gaining leads.

Meanwhile malicious bots can fill out forms, generate false ad impressions, serve spam or malware and trigger retargeted ads. They can even take over entire networks to form botnets and move a cursor to mimic human behavior.

Ad publishers

Most fraud can be traced back to the publisher who sent that traffic. Sometimes the publisher is run by fraudsters, but there are also some types of ad fraud that can affect reputable publishers without them even realizing it.

Domain spoofing

Fraudsters can actually change the URL of their sites to make advertisers believe that a fake site is instead a more reputable publisher. Then, because publishers see these sites and recognize the name, they'll pay the premium price to advertise there.

This essentially results in extremely high **advertising** costs with little chance of discovery or interaction. Plus, a **brand**'s ads could be placed next to some questionable content, which can damage your reputation.

Ad injection

Ad injection can occur in a few ways. Injected ads can be stacked on top of each other, or they can completely replace existing ads.

Injected ads that replace others are often in the form of a fake warning, such as an ad telling a user that their PC performance is lacking or that their computer needs to be updated.

Most obviously, injected ads can also appear where they aren't supposed to, making the relationship between **brand**s awkward.

Web browsers

You don't have to be an advertiser, publisher or a website owner in order to fall victim to ad fraud. Even just by browsing the web, you can become a victim. While it might not cost you reputation and **advertising** dollars, it can hurt your computer or lead to the theft of personal and financial information.

With **ad injection**, you might see ads that are offensive, or ads that ask to complete suspicious downloads. If a site has **stuffed pixels**, you might get stuck with a video ad playing in the background that you can't turn it off, which could drastically slow down your Internet. Or, if you end up on a **spoofed domain**, you could be on an unfavorable site you never meant to visit.

Detection and prevention

Some of these types of fraud can be very difficult to monitor and catch. However, there are a few methods you can apply to your **advertising** strategy to help you better detect and prevent ad fraud from hurting you.

- **Request transparency from your publishers.**Ask your publishers where their traffic originates. If the publisher has nothing to hide, then they should be able to be straightforward with you about their traffic sources.
- **Time your ads.**Bot fraud is more active during certain times of the day. Some bots are active from midnight to 7 a.m., and others are more active during the day to blend in with everyone at work. You can target your ads when bots are least likely to see them.
- **Use third-party monitoring.**Monitor the traffic coming to your ads in real-time, so that you can stop the fraudsters before they can click on your ads.
- **Assess your traffic constantly.**Always review your ad campaigns to see where the best clicks are coming from so you can adjust accordingly.
- **Search for your site in incognito.**This is a great way to make sure you know exactly how your site is displayed for others. It'll also most likely bring up any sites that have stolen your domain, or show you any ads that have been injected.
- **Think before you download.**Be wary of extensions, add-ons and toolbars. That's an easy way for fraudsters to install malware and get into your system.

Too much time and money is being wasted on ad fraud today. Fraudsters are becoming more

persistent and more sophisticated. The more aware you are of the workings of your campaign, the better you'll be able to fight and prevent these fraudsters from making you a victim to their schemes.

This article first appeared in www.entrepreneur.com