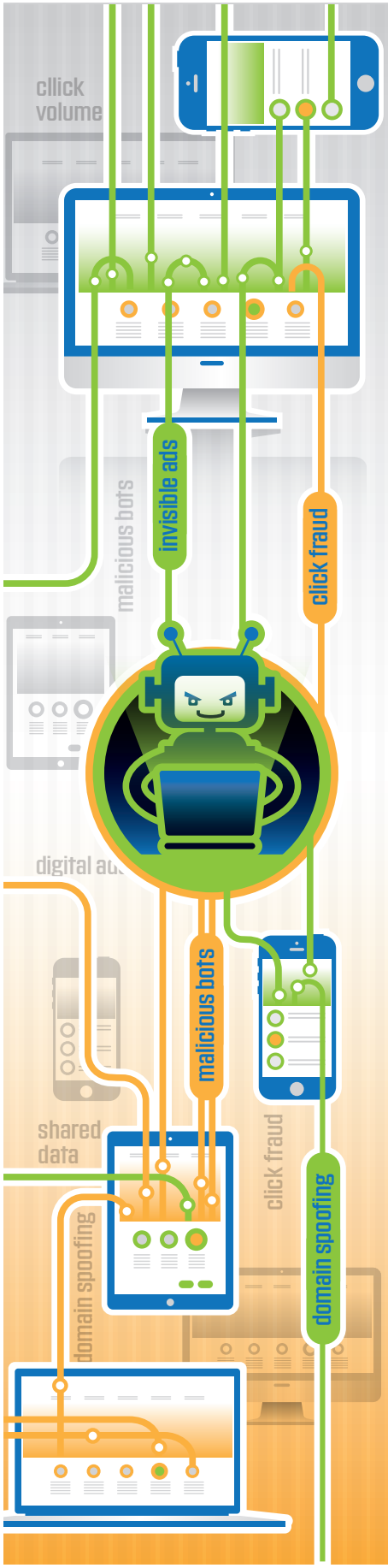


AD FRAUD CAN WASTE YOUR BUDGET, HURT YOUR BRAND AND SINK YOUR DIGITAL AD CAMPAIGN

PASKILL STAPLETON & LORD
Enrollment Marketing for Higher Education

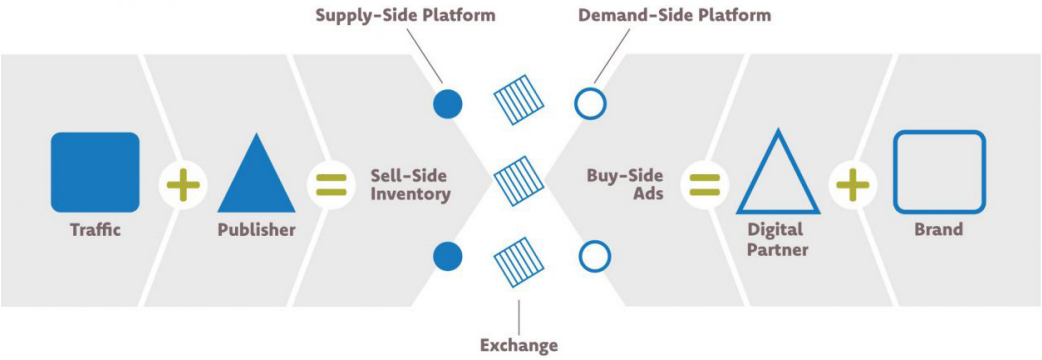
When you make a $250,000 digital ad buy, you strategize, design, and budget carefully to move your target audience through the conversion funnel. But you probably don't add a line item for organized crime or plan to take out an ad on an unsavory website. If you did, you probably wouldn't set aside as much as 40% or $100,000 of that budget. But if you aren't aware of ad fraud, you might end up doing just that.

A recent study found that as much as 40% of internet traffic is from bots (programs designed to mimic human activities often at the center of ad fraud schemes). Bot traffic is a problem because digital advertising, the commercial lifeblood of the internet, is driven by programs designed to read web traffic and serve targeted ads in a matter of milliseconds. That non-human traffic is often at the center of ad fraud schemes. A different study found that ad fraud schemes will cost advertisers $42 billion in 2019.

HOW IS AD FRAUD POSSIBLE?

Ad fraud, like so many other negatives brought on by the internet, is an example of malicious actors twisting the promise of technology. Digital advertising relies on a supply chain of independent entities cooperating by sharing data to overcome the scale of the internet and provide sophisticated, targeted advertising. But it is that very openness, scale and reliance on data that makes the system vulnerable to fraud.

Consider programmatic advertising (when the purchasing process is automated and nearly instantaneous). Experience dictates that the most effective ad arrives as the consumer is considering a purchase. In the physical world, this is achieved by displaying an ad where there's a high level of purchase intent, such as an ad near a busy shopping center or in a store's checkout aisle. But online, websites can identify and track a visitor's every move and place a string of ads throughout their entire decision-making process. This all occurs in milliseconds as a user is browsing search engines, reading articles, watching videos, and engaging with their community on social networking platforms. The digital marketing supply chain makes this possible through a series of platforms and open exchanges that connect brands (or more likely their digital partners) with publishers.



DIGITAL AD FRAUD - DIGITAL MARKETING SUPPLY CHAIN

All of the intermediaries stand to make more money from a higher number of impressions and click volume, and that opens up vulnerabilities for fraud throughout the entirety of the digital advertising process.

Here are some of the most common forms of ad fraud, but keep in mind fraudsters innovate and adapt constantly, so the list is not exhaustive or mutually exclusive.

DOMAIN SPOOFING

Domain spoofing is any scheme that reroutes ads to a different website than expected, normally with the goal of maximizing traffic. The consequences can range from a waste of money to a brand safety disaster.

The simplest way to do this is to take advantage of an ad system where ads are placed before a publisher's data is verified. Hackers can supply attractive but false information about their site and get an ad placed. The brand might think they are advertising with a well-known publisher, but the ad is actually served to a completely different website.

Sometimes publishers manipulate their role in the process in more subtle, programmatic ways, like placing a custom iframe on a different site that displays the ad posted on the legitimate site. This can be a big problem if a publisher owns both a low traffic, but brand-appropriate site and a second site that is more heavily visited and hosts content that would hurt the brand, like pornography or hate speech. In that case, the wasted money is probably secondary to the potentially serious blackeye for the brand, especially if the situation gets wider notice.

FRAUDULENT INTERACTIONS (CLICK FRAUD)

Click fraud used to mean "click farms" of actual people clicking on ads, filling out surveys, watching videos, etc. Today, bots pose an even larger threat. Malicious bots are programs that infect devices and perform tasks in the background, sapping computing power from legitimate tasks. Each bot instance can be controlled by one controller, creating a botnet of individual programs that can be used to create fake traffic to scam advertisers.

Researchers have uncovered botnets that number in the hundreds of thousands of devices, but hard statistics are difficult to come by since more than one bot can be active on one machine. But it is clear that the scale of botnets can threaten the legitimacy of even well-known internet properties.

Unsophisticated bot traffic can be easy to spot. Some known examples include spikes in traffic at 3 AM or high numbers of visitors simply opening and closing a webpage. However, as hackers understand what triggers suspicion, they adapt their algorithms to mimic mouse movements, browsing behaviors, and virtually any other interaction.

INVISIBLE ADS

There are a variety of ways publishers can technically display an ad while making it functionally invisible to a viewer. For example, some publishers will stack or tile 10 or more ads on top of each other and then collect the revenue from displaying more ads. They could also display the ad off-screen, so it is served to visitors, but never actually seen. Publishers could also reduce ads to one pixel, which is not visible to any viewers.

Detecting this type of fraud is difficult, because the ad is going to the correct domain and perhaps it is even served to legitimate traffic. One red flag is when the size of the ad doesn't makes sense for the publisher (a large ad served to a mobile platform, for instance). However, more sophisticated publishers will manipulate the data sent back to the advertiser to show the ad as displaying at the proper size. Your sales data, though, should tell a different story, so tracking ad activity through to the expected uptick in sales is critical.

HOW DO I COMBAT THIS?

Most advertisers work with a partner to place their digital ads. It is critical to open a conversation with your digital partner to make sure they have steps in place to combat ad fraud. Specifically, you should be asking about your partner's ad fraud tech stack, which is simply the toolbox of technologies, approaches, and policies that a firm uses to avoid fraud while still driving results. Some of the most important steps are listed below.

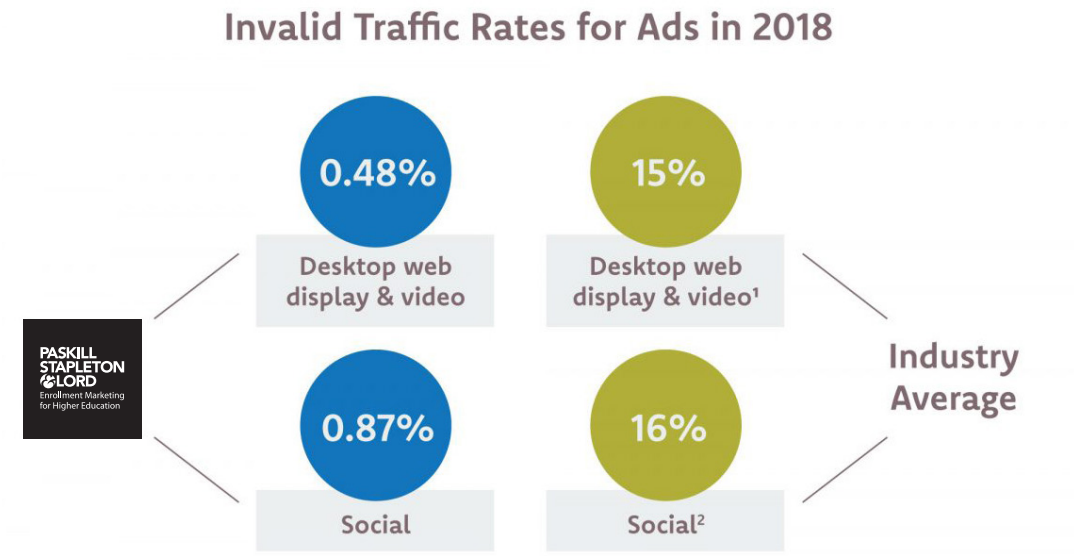
BLACK LIST, WHITE LIST, DIRECT BUYING AND PMPs

A white list dictates to a programmatic DSP which sites an ad can appear on and a black list dictates which sites an ad should not appear on. The lists can be general or segmented by industry or demographic vertical based on an individual campaign or ad. Managing this capability helps make sure ads end up in an appropriate environment with the added benefit of reducing the likelihood of the ad being displayed to a site that uses bots.

Similarly, you can purchase ad inventory directly from the inventory owner. Publishers may have a Private Marketplace (PMP) or header bidding. Both often involve working directly with the publisher which reduces the possibility of fraud. However, any of these tactics will only aid in reducing the volume of invalid traffic.

VALIDATE EVERYTHING

There are a variety of tools and processes that a digital partner should adopt to identify anomalies and verify the self-reported data provided by advertising suppliers. For many advertisers, performing these checks in-house is not possible, so it should be something you look for from your partner. They usually have access to a somewhat costly third-party validation service. These services are available to validate everything from brand safety and impression tracking to fraudulent impressions, viewability, and invalid traffic tracking.



1. Pixalate (June 26, 2018). The state of Invalid Traffic IVT In Programmatic: Q2 2018. http://blog.pixalate.com/state-of-invalid-traffic-ad-fraud-programmatic-q2-2018
2. Pixalate (April 8, 2019). Mobile App Fraud: Invalid Traffic (IVT) by Category. http://blog.pixalate.com/mobile-app-fraud-trends-invalid-traffic-ivt

DIGITAL AD FRAUD - INVALID TRAFFIC RATES

You can also perform a simple data comparison to check for red flags. For example, if your ad clicks are up 400% but your online sales are actually down 1% over that same period, something is probably amiss.

INSIST ON MAKE-GOODS

You or your digital partner can insist on make-good clauses for ad fraud when negotiating with any provider of digital advertising inventory, whether direct or through a DSP. Many companies may not have the spending power to negotiate these terms up front but if you work with an agency that has a specialization in digital media buying, you can benefit from the total spending power of your media buying agency. Having this language in place means once you've identified the fraudulent traffic, you can actually do something about it by having more impressions served that are seen by actual humans, not bots. This step is critical for maximizing your digital advertising budget and ensuring you're not one of the many companies having their budgets siphoned off. Avoiding fraud is still the first priority, due to the headline risk, but having a partner that is aware of fraud can help lessen the financial risk as well.

ABOUT THE AUTHOR

BRIAN AITKEN
Managing Director,
New York Paid Media and Analytics