The Battle Against Bots

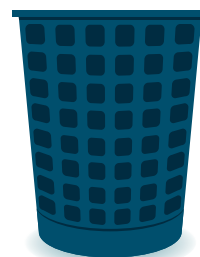The growing problem of bots on site and marketing fraud for companies

Fighting Back Against Marketing Fraud

KRISTINE LOPEZ
Director, product management
HUMAN

Marketing campaigns are only as good as the data marketers are making decisions off of. What happens if that very data is actually dirty with bots? Fraud follows the money, and there's a lot of it in digital marketing. Sophisticated bots infiltrate marketing campaigns through on-site traffic, lead generation and ads to make money. In all of the traffic and data marketers work with, bots get lost in the pack. This leads to endless downstream impacts, such as wasted retargeting budget and time trying to convert a non-human lead. Unfortunately, this is a common occurrence. In a survey we conducted with Renegade, we found two-thirds of marketers experienced some kind of marketing fraud and one-third experienced media buy fraud in the last year. So how can marketers fight back? This eBook dives into what marketing fraud is, how to spot it and what marketers can do about it.

The Battle Against Bots

The growing problem of bots on site and marketing fraud for companies

Brands are spending more in digital marketing every year. By 2025, advertising dollars are expected to top $300 billion according to eMarketer. Unfortunately, all that money has attracted the attention of cybercriminals and fraudsters who deploy sophisticated bots to deceptively engage in marketing campaigns to make money.

As reported by Alison Weissbrot for Campaign US in "Digital ad fraud will hit $35 billion globally this year," ad fraud will surpass credit card fraud "in part because the digital ad industry doesn't have as many safeguards and regulations around fraud as more established sectors." That makes it low risk and highly profitable for criminals, and it "is tipped to become the second most lucrative form of organized crime (behind drug trafficking) within the next decade, according to the World Federation of Advertisers," as Jessica Heygate wrote for Campaign US in "Inside ad fraud: What it takes to dismantle a $5.8bn enterprise."

Bots mimic real humans and simulate traffic by clicking on paid ads and search results to visit sites and mobile apps and fill out forms. That means money is wasted on acquiring, storing and remarketing to fraudulent traffic — to the tune of millions of dollars each year. And that's not all. Bot traffic also skews data and analytics, clouding customer insight and organizational decision-making.

Once bots are in a marketer's system, they can continue to wreak havoc. Not only does a marketer incur costs because the system increases efforts to reach illegitimate prospects, but there is the opportunity cost for efforts that could have been directed toward legitimate ones. It is important for marketers to understand the threats malicious bots pose and what they can do to fight them.

TODAY'S MACRO CHANGES LEAVE MARKETER'S EXPOSED

The digital ecosystem is at an inflection point. There are three compounding factors that are fundamentally changing how companies operate.

First-party data has always been the gold standard, but with the deprecation of the third-party cookie, it becomes even more important. It's mission critical for every brand and every publisher and any entity with a direct end user relationship to collect as much consented, legal, first-party data as possible. This data can help with selling, make targeting more precise, offer ways to emphasize and engage with users and inform strategy.

On site is the new front door. The massive digital transformation over the last few years has made our world increasingly connected. As a result, brands are fully committed to digital-first operations, which is why it is even more important to ensure the front door is locked against bot infiltration.

THREAT MODELS

A glimpse into some of the most prevalent types of marketing fraud threats
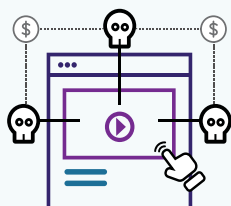
CLICK FRAUD

Sophisticated bots get paid to view and click on ads, and the marketer is none the wiser given their human-like tendencies.

RETARGETING DECEPTION

This fraud occurs when service providers have driven site traffic from sophisticated bots that then populate DMPs or CRMs and use the data to retarget bots. Fraudsters falsely claim the referral payments while marketers waste time and money retargeting these bots with ads.
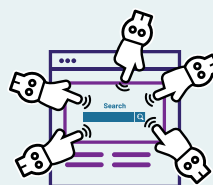
LEAD FRAUD

Fraudsters drive bot traffic to landing pages, typically with form fills, and emulate human behaviors to avert detection. When companies pay for leads, sometimes third-parties are tapped to meet expectations. Bots are then deployed and paid to fill out the form.

COMPETITIVE ASSAULTS

"Black hat" marketers invoke click bots to launch automated search queries, click on competitor ads to waste competitor budgets and diffuse targeted marketing efforts.

All marketing is outcome driven. That means that every dollar spent on advertising must be done with purpose, especially in digital. Chief marketing officers (CMOs) and marketing leaders must drive engagement and deliver profitable results with an incremental return on investment. As a result, many are also being held accountable for data cleanliness and compliance.

Ultimately, all three factors will make the impact and cost of bot fraud even greater.

BOTS. DON'T. CONVERT.

Marketing fraud is a bigger problem than most companies realize. According to a recent survey sponsored by Human and conducted by Renegade, two-thirds of marketers experienced some kind of marketing fraud and one-third experienced media buy fraud in the last year. While marketers rely on accurate data and insights into the customer's journey to inform future spending decisions, the consequences extend beyond ad spending.

It takes a number of strategies to deliver marketers the steady flow of leads needed to meet key growth metrics. Unfortunately, fraudsters can introduce themselves into these performance channels without much difficulty. They can drive bot traffic to landing pages, emulate behaviors to avert detection while siphoning budgets and contaminating the very insights needed to make informed choices.

Marketers leverage all the data at their disposal to buy media and move audiences toward conversion. The problem is bots look and act more like humans than ever before and interact with all aspects of marketing efforts. They contaminate data and put digital marketing investments at risk by skewing key performance indicators (KPIs) and metrics. Warped data and analytics in turn compromise a marketing team's ability to make accurate data-driven decisions.

Dirty data leads to fake leads. Time, money and opportunity costs are driven up when affiliates deliver automated bots, not humans. For example, a streaming service provider focused on new customer acquisition using data aggregated over years from previous products when it was launching a new service. However, the data was found to be over 10% fraudulent. If this vulnerability had not been identified, missed revenue opportunities on this targeting would have extrapolated to over $2 million annually.

Every year, more than $5 billion is wasted on fraudulent traffic. Paid marketing manipulation diverts funds and attention away from real humans who could convert to customers. Bots raise costs, lower conversion rates and reduce the marketing return of investment (ROI). Since brands rely on digital integrity, there is the added risk that consumers, investors and regulators could lose trust in the brand.
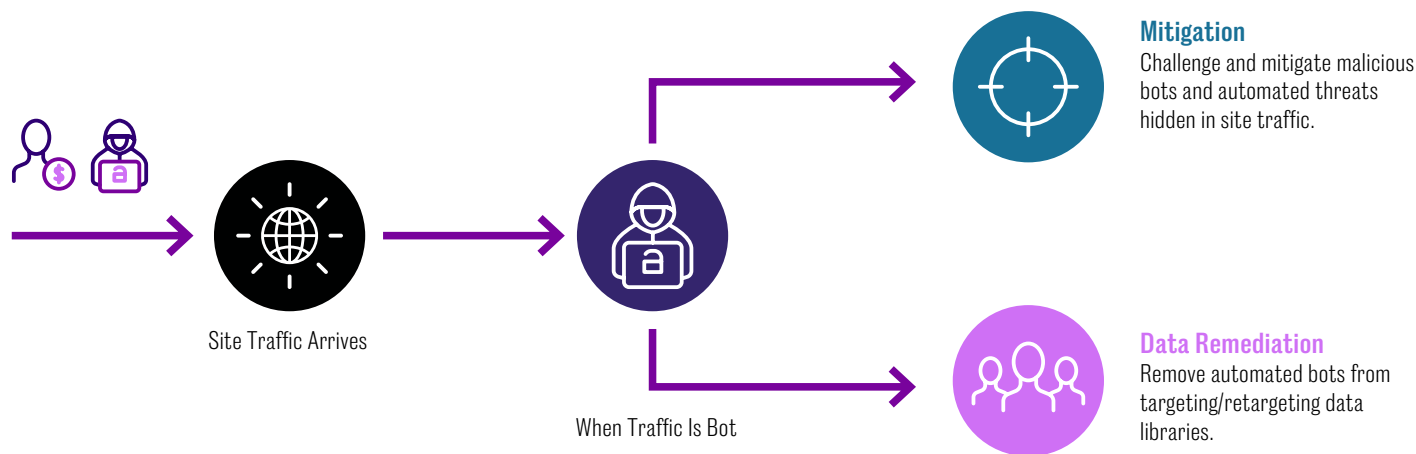
Every year, more than $5 billion is wasted on fraudulent traffic. Paid marketing manipulation diverts funds and attention away from real humans who could convert to customers.
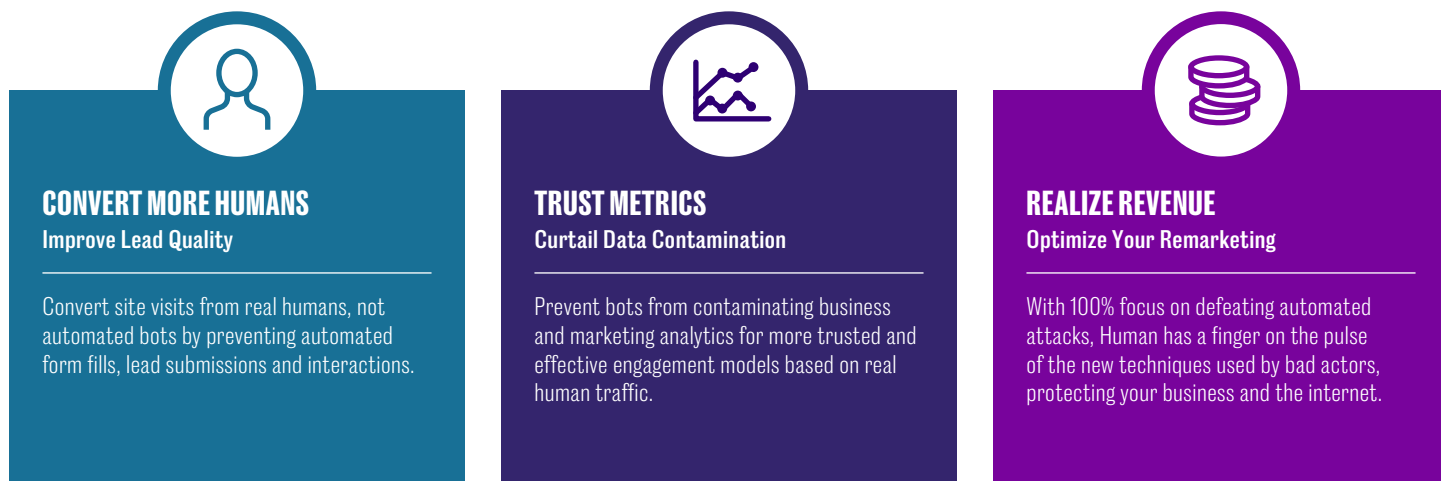
FIGHTING THE FAKES

While combating fraud can seem daunting, understanding how it operates, the avenues fraudsters use to enter marketing efforts, and how they make money on campaigns can give marketers a serious leg up to stop it.

HOW BOTGUARD FOR GROWTH MARKETING WORKS

Site Traffic Arrives

When Traffic Is Bot

Mitigation
Challenge and mitigate malicious bots and automated threats hidden in site traffic.

Data Remediation
Remove automated bots from targeting/retargeting data libraries.

THE HUMAN BOTGUARD FOR GROWTH MARKETING ADVANTAGE

CONVERT MORE HUMANS
Improve Lead Quality

Convert site visits from real humans, not automated bots by preventing automated form fills, lead submissions and interactions.

TRUST METRICS
Curtail Data Contamination

Prevent bots from contaminating business and marketing analytics for more trusted and effective engagement models based on real human traffic.

REALIZE REVENUE
Optimize Your Remarketing

With 100% focus on defeating automated attacks, Human has a finger on the pulse of the new techniques used by bad actors, protecting your business and the internet.

Taking control and addressing the problem head-on can have a dramatic impact on marketing campaigns and metrics. When a global automotive manufacturer noticed that sophisticated bots were skewing paid media conversion rates for their retargeting campaigns, they wanted to A/B test the impact of removing bot audiences from retargeting efforts. The campaign that used the Human marketing fraud solution improved both the volume and quality of digital interaction with the retargeting campaign, boosting the volume of conversions by 42% and the conversion rate by 57%. Automatically removing bots from retargeting campaigns also lowered the cost to reach better quality audiences, reducing cost-per-acquisition by 34%.

A first step is to find out if the numbers make sense. Are there odd or inexplicable traffic spikes on the website? Are conversion rates lower than expected? Are retargeting campaigns falling short? A "yes" to any of these questions may indicate a sophisticated bot problem.

Marketing fraud detection and prevention companies such as Human can help companies defend their digital marketing initiatives and lead generation efforts from bots. In contrast, BotGuard for Growth Marketing uses a modern defense strategy that establishes hard technical evidence to prove fraud. That means it not only protects clients but makes it harder and more expensive for fraudsters to pull off a crime and therefore safeguards a company's budget, reputation, security practices and compliance.

Contact Human today to learn more about BotGuard for Growth Marketing and how to prevent marketing fraud.