HUMAN

The New Frontiers of Fraud

Marketing Fraud 101

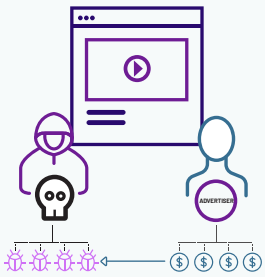
Threats to Brands

Leading DSPs, SSPs and exchanges have formed strong partnerships with bot mitigation and bot prevention leaders, greatly reducing the prevalence of fraud running through programmatic platforms. Many brand advertisers believe they are insulated from marketing fraud through programmatic advertising. Unfortunately, they are not.

Marketing fraud goes way beyond just programmatic display and video. Marketers rely on a host of tactics—like search and social—to attract the interest of their customers. All channels are susceptible to fraudsters, and most platforms are unable to catch this fraudulent behavior or stop it.

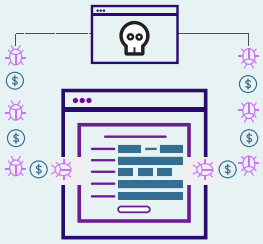
Threat Models

A glimpse into some of the most prevalent types of Marketing Fraud threats



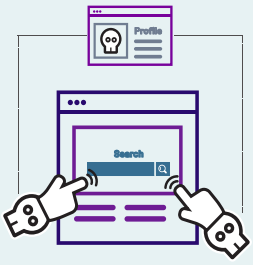
Brand Ad Skimming

Bad actors mix legitimate traffic with fake bot interactions to make their network of traffic more attractive to agencies and advertisers in return for higher CPMs and more revenue.



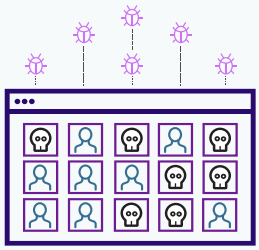
Fake Audience Database

Malicious actors wreak havoc on a brand's audience databases by automating bots to input fake user data, in exchange for a cost per form fill payout or even to benefit from giveaways. Fake bot or incentivized sign-ups steal money and lead to a weaker database of customers for brands.



Search Fraud

Marketers looking to mess with competitors' budgets and metrics can invoke click bots to launch automated search queries, click on ads to waste competitor budgets, and diffuse targeted marketing efforts. Fraudsters can even build the profile of their bots by clicking on search ads. While this isn't revenue-generating, it further develops their profile to look like a human for their next attack.



Look-Alike Audiences

Brands expanding their reach by purchasing audiences behaviorally similar to their core audience sometimes unintentionally invite bad actors who have built up profiles to look like that audience. While brands think they are building awareness with an extended, but vetted audience per their matching criteria, bots are getting in through the back door.

Case Study

A leading brand advertiser uncovered a significant amount of its annual budget was being compromised by sophisticated bots. HUMAN narrowed the source to specific IPs via display advertising vendor. The brand shifted its campaign strategy to eliminate the fraudulent source and systematically removed the previous bot users/sessions from their targeting and CRM systems. These changes delivered significant cost savings and improved return-on-investment (ROI). Using a simple estimation of the marketing Lifetime Value of the previously lost budget, the brand valued the recovered revenue by converting real human traffic, at 24% of its annual marketing budget. This, coupled with improved conversion rates, delivered a robust 12X ROI on their platform and effort costs.

HUMAN is a cybersecurity company that protects enterprises from bot attacks to keep digital experiences human. To learn about how our BotGuard for Growth Marketing product can protect your enterprise from Marketing Fraud, visit **www.humansecurity.com.**