Eskimi DSP Anti-fraud Settings

In today's digital advertising landscape, combating fraud is a critical priority for maintaining the integrity and effectiveness of campaigns. Major industry players often rely on custom solutions for fraud detection, while others turn to trusted third-party services such as IAS, DoubleVerify, Pixalate, and HUMAN. At our company, we have developed an internal anti-fraud tool and collaborate with global exchanges that employ their own or third-party solutions to filter out fraudulent activities. This results in a robust, multilayered fraud detection system, combining our internal tools with the "filtered" traffic from exchanges and SSPs. As an Eskimi DSP user, leveraging the anti-fraud settings is essential to maximize the efficiency and credibility of your advertising efforts. Below, we provide a detailed overview of each option available on the approval page and their technical functionalities.

1. **Exclude New (Non-DMP) Users**

This setting is designed to filter out users who don't have a Data Management Platform (DMP) ID in the Eskimi system. By enabling this option, your campaign will prioritize users already present in our DMP, enhancing the targeting precision and reducing the risk of fraudulent activities.

2. **Exclude Users with High Daily Apps/Sites Count**

Eskimi DSP monitors bid requests for each user, and this setting kicks in when a user's daily Apps/Sites count surpasses a predefined threshold. By excluding users with unusually high activity, the system mitigates the risk of engaging with potentially fraudulent or non-genuine users.

3. **Exclude Users with High Daily Page Views**

Similar to the previous setting, Eskimi DSP evaluates the number of bid requests per user. If a user's daily page views exceed a specified limit, the system excludes them from winning bids. This helps maintain campaign quality and ensures engagement with authentic users.

4. **Exclude Fake Clickers**

To combat click fraud, Eskimi DSP employs a code implementation that distinguishes between genuine users and bots mimicking legitimate clicks. Users exhibiting suspicious clicking behavior are automatically disqualified from winning bids, safeguarding your campaign from fraudulent activities.

5. **Exclude Domain Spoofers**

This setting targets domains attempting to mimic popular websites with slight variations in variables or letters. By excluding these spoofed domains, such as forb1s.com instead of forbes.com, Eskimi DSP fortifies your campaign against potential fraudulent traffic.

6. **Exclude ads.txt Mismatching Apps/Sites**

This anti-fraud measure ensures that bid requests are accepted only from apps/sites where the Exchange or SSP sending the bids is present in the ads.txt list. For instance, if a popular website like foxnews.com lacks Eskimi in its ads.txt list, enabling this option will reject bids originating from Eskimi SSP via foxnews.com, preventing potential fraud.

By leveraging these anti-fraud settings, Eskimi DSP empowers users to maintain campaign integrity, enhance targeting accuracy, and safeguard against various fraudulent activities in the digital advertising landscape.

Revision #5
Created 29 March 2022 07:16:26 by Vladimir
Updated 11 June 2024 06:48:19 by Vladimir