The publisher's guide to winning the fight against clickbait

Tactics for user experience and protection

DIGIDAY

geedge
Add Integrity

The publisher’s guide to clickbait

For publishers, delivering a positive user experience is paramount to ensuring loyalty and safeguarding monetization opportunities. Programmatic ad sales are a strategic revenue channel for publishers, but given the volume of ads that move through these channels, it’s becoming increasingly difficult to control the quality of the ads that end up on a given site.

Over time, the number of clickbait, offensive and misleading ads on publishers’ sites is increasing. **According to research by GeoEdge and Digiday, 76% of publishers reported that the user experience on their sites had been impacted by ad quality challenges, and 66% reported that it negatively impacted their revenue.** For digital publishers, recognizing that user protection and user experience go hand in hand is crucial, and being aware of any gaps in either is critical.

In order to maintain a positive user experience and optimize revenue, publishers need actionable insights — they need to know how clickbait operates, how to flag it and how to prevent it from getting on their site in the first place. In this guide, GeoEdge and Digiday present tactics for publishers that will help them win the fight against clickbait.

Establishing guidelines to win against bad ads

One first step in creating an engaging user experience is to define what constitutes a bad ad.

Amnon Siev, CEO at GeoEdge, suggests one approach to this is to "create a list of values you want to reflect to your audience, then translate that into guidelines about what ads should be shown on your site."

These guidelines should be specific about what is and isn't acceptable, and should include specific categories that aren't in line with the brand's messaging or values.

News publishers, for example, are likely to want to establish guidelines related to politically charged content. Siev noted that during the last U.S. national election cycle, for example, "GeoEdge had publishers implementing lists of keywords that lean Republican or Democrat based on their brand messaging." Other publishers, if they prioritize being an impartial source, might decide that blocking all political content is more in line with their values.

However, ad guidelines must also evolve. While many of the guidelines are likely to stay the same, current events and trending topics impact the content of ads that come through programmatic channels. It's unlikely that publishers would be able to foresee the possibility of ads related to topics such as international conflicts and political events.

Tactics and insights

Ads should reflect the same values as editorial content. Use brand values as a starting place to come up with ad guidelines, including elements such as political content, competitors and categories that should and should not be allowed in ads on the site.

Ad guidelines should be regularly reviewed and changed to reflect evolving contexts.

A closer look at clickbait

While every publisher maintains different standards for brand-suitable advertising, the threshold for user protection is not subjective. Preventing clickbait is critical to the user protection equation.

According to GeoEdge, clickbait is deceptive creative engineered to intentionally elicit clicks through manipulation and psychological engineering.

Types of clickbait include financial scams, misleading product offers, brand infringement, fake antivirus and cleaners, among variations.

Aside from full-scale audience alienation, clickbait damages a site's metrics, which discourages high-quality advertisers from buying inventory, and ultimately impacts CPMs and overall revenue. To prevent damage to user experience, publishers must own all these touchpoints with their audiences, from the editorial content to the ad content and all accompanying landing pages.

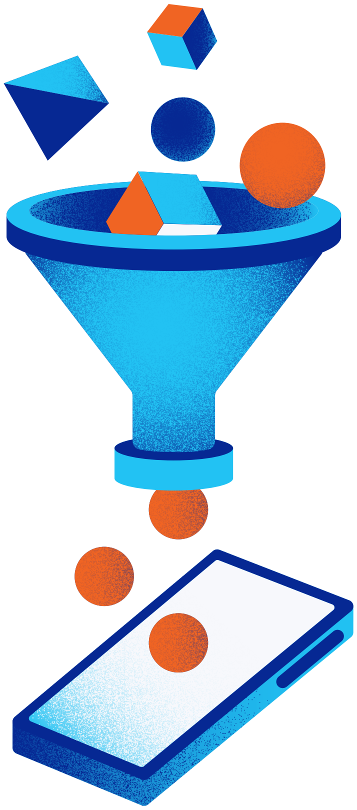
Steps for accurate and real-time categorization of clickbait

Once a publisher has determined its ad content guidelines, the next step is to implement them into the specific ad filtering tools or mechanisms. Ad content filtering is initially done on the publisher's ad server, where they select the categories of ads that are and aren't allowed. And while the ad server is a good place to start, even with these filters in place, miscategorization results in bad ads slipping through filters.

This is primarily due to an ad's categorization being based on what the advertiser declares for their own campaign. This means that advertisers might state their campaign is an entertainment campaign, but it's actually clickbait related to cryptocurrency — a frequently blocked category. In such a case, the ad would not be blocked by the ad server and will end up on the publisher's site.

The initial step publishers can take to prevent miscategorizations is by working with SSPs who prioritize ad quality to ensure accurate categorization and blocking. "Every publisher has their own definition of what a bad ad is," said Siev. "Publishers must communicate their ad quality guidelines to ensure their SSPs know what they expect to get from them."

However, to achieve the most control to deliver the necessary level of user protection, publishers are leveraging real-time blocking ad-quality tech solutions. These solutions base ad categorization on analysis of the actual content of the ad and its landing page, rather than what advertisers declare. They also are equipped to handle the scale of programmatic transactions in real time to ensure that bad ads are prevented from getting through filters.



Tactics and insights

Publishers are working with SSPs dedicated to ad quality to improve the categorization of ads based on their own standards and guidelines.

Real-time ad quality solutions analyze the true nature of ad content to determine their suitability.

Ad landing pages are a core part of the clickbait puzzle

To identify clickbait and other bad ads before they end up on site requires an understanding of how these ads operate.

Ad quality discussions are often limited to what appears within a publisher's content. But an equally important part of the equation and user experience is the landing page to which bad ads take the user. While all clickbait ads are intrusive to the user experience, most actually deliver deception or scams through the post-click landing page.

"Specifically in the case of clickbait, what you see promoted in the ad and what's on the landing page are not the same thing," said Siev. "As a user, if you have this experience, you feel like you've been misled, and that's automatically correlated to your trust of the publisher."

The post-click experience needs to be considered in ad quality monitoring efforts, not only because of potential misalignment with landing page content, but also because landing pages are becoming increasingly popular vehicles to deliver scams to users in recent years. Ideally, there should be consistency across all user touch points, which encompasses editorial content, ad content and more.

If publishers monitor ads before they go on their sites, they need to be sure to check the landing page in addition to the ad creative itself. Ad quality tech solutions can help this process immensely, specifically those tools with the ability to check page code and content automatically. In programmatic channels where huge volumes of transactions are occurring, this is a critical feature to be able to keep up.

Tactics and insights

All user touch points need to be taken into account, and that includes ad landing pages.

It's crucial that ad security solutions check that landing pages, in addition to ad creative, uphold guidelines before allowing an ad on the site.

Understanding fraudster tactics

Scammers have developed tactics to slip through publishers' tools and systems, so it's important to understand these methods in order to stay ahead of them.

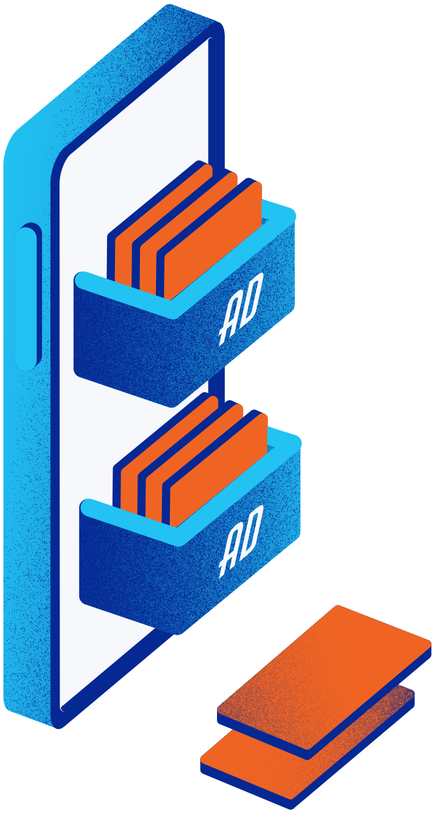
One common method starts with a warm-up stage. Scammers will launch a campaign with creative and a landing page that are harmless in order to get approved on the ad platform.

Once this stage is over, which can take a few days up to a few weeks, scammers then use a process called cloaking which enables them to evade ad policies that prohibit things like dietary scams, trademark infringing products and deceptive advertising like malware.

A cloaked scam relies on device and user fingerprinting to identify specific users that are qualified to be scammed. These users will be redirected to a deceptive landing page where the scam takes place. All other users that don't fit the targeted parameters, or non-human environments, will never be served the deceptive landing page.

As scammers grow more sophisticated in their methods to bypass ad quality tools, publishers are turning to vendors that provide solutions with more sophisticated methods to proactively catch them.

Because cloaking scams are designed to evade scanning tools, robust tools are required to keep users safe from scams delivered using this method. Real-time blocking capabilities are needed to stop cloaked attacks by identifying them before the deceptive landing page content loads.



Tactics and insights

Just because an advertiser ran an innocent campaign initially doesn't mean that future campaigns will be clean.

Solutions from ad quality vendors with real-time blocking capabilities are necessary to identify cloaked attacks before they're delivered to users.

Real-time blocking capabilities must rely not only on ad code analysis but on post-click and anti-cloaking engines.

Checklist for reinforcing site integrity

When it comes to choosing an ad-quality partner, there are three key components that publishers should consider.

Inventory transparency:
Ad-quality tools need to provide transparency into all the ads served through programmatic channels across a publisher's assets. For example, they might provide screenshots of all programmatic creative, landing pages and additional components of an ad to give publishers complete visibility.

Landing page analysis:
In addition to analyzing ads based on campaign creative, ad quality tools should also factor in the content and code of the landing pages ads lead to and the post-click experience. This is especially critical to winning the fight against clickbait.

Customizable:
Ad-quality tools should enable publishers to define and manage sets of specific filtering rules and conditions and apply them to the needs and requirements of each of their audiences. The tool should offer various filtering options with modes ranging from fully automated blocking of security threats to semi-automated content categories and manual content review. Some publishers also require the flexibility across their digital assets to implement different rules for each site.

As more inventory transacts through programmatic channels, publishers must balance the short-term benefits of unchecked ad sales with the long-term impacts that bad ads, such as clickbait, are having on user engagement metrics and the overall user experience.

Publishers that are adopting tactics and tools that centralize the user experience — ensuring a consistent and safe experience across their editorial and ad content — are maintaining programmatic as a strategic revenue stream, and they are successfully protecting their brand integrity.

As GeoEdge's Siev put it, "By ensuring clean and engaging ad experiences, publishers are ensuring that advertising enhances the user experience of their site, and doesn't detract from it."

About GeoEdge

GeoEdge's mission is to protect the integrity of the digital advertising ecosystem and to preserve a quality experience for users. GeoEdge's advanced security solutions ensure high ad quality and verify that sites offer a clean, safe and engaging user experience, so publishers can focus on their business success.

Publishers around the world rely on GeoEdge to stop malicious and low-quality ads from reaching their audience. GeoEdge allows publishers to maximize their ad revenue without quality concerns, protect their brand reputation and increase their user loyalty. GeoEdge guards digital businesses against unwanted, malicious, offensive and inappropriate ads — without sacrificing revenue.

www.geoedge.com

DIGIDAY | geoedge

Add Integrity