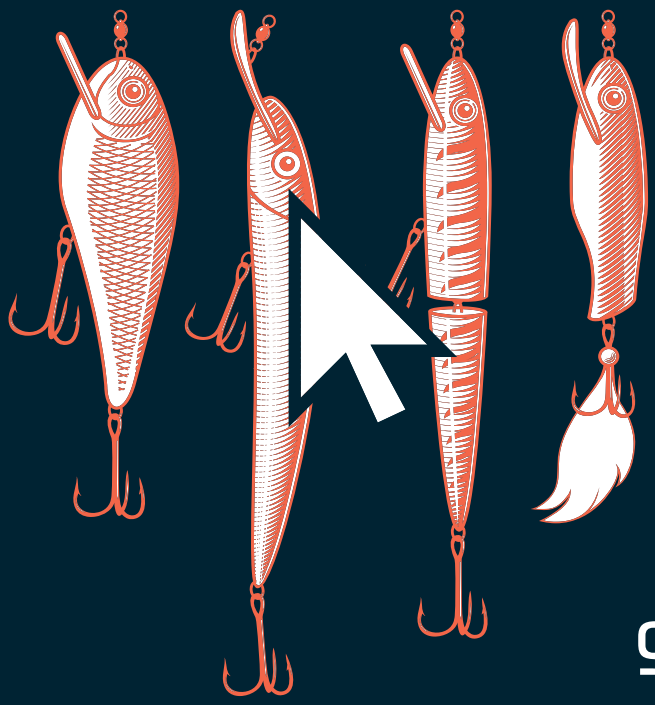
admonsters

PLAYBOOK

How Clickbait Ad Scams are Devised & Impact Publishers' Sites

An Admonsters Playbook | October 2022 |



Sponsored by:

geoedge
Add Integrity

What's a Playbook?

A playbook is an extension of what the AdMonsters community has been doing at our conferences for 20 years. A playbook solidifies what has made our events "must attend" for many digital strategists. By bringing people together to share learnings and best practices in a focused way, people can create a plan and avoid hours—if not days—of doing research on their own.

The AdMonsters playbook concept takes existing AdMonsters content (from conferences and AdMonsters.com) and, with the help of the AdMonsters community, "crowd sources" a document that outlines best practices on a particular topic. Our belief is that this will allow for a free exchange of ideas with the benefit of curation for accuracy. This document does not get into specifics around individual solution providers intentionally.

Great effort has gone into writing the playbook in a fashion that applies to as many publishers as possible without becoming too general. In a technology-driven industry like digital advertising, information quickly becomes obsolete. The intention is that, based on the feedback of the AdMonsters community, the next playbook will start to take shape and, with additional contributors, grow in both depth and breadth.

TABLE OF CONTENTS

1. THE STATE OF CLICKBAIT ADS

Users care about the experiences they have with the ads that appear on the sites they visit, and when they see that those experiences are unsafe and beyond their control, they take matters into their own hands. Installing an ad blocker is one of the more extreme measures users can take – but it's all too common. As many as 42% of users in the US now implement ad blockers on at least one of their devices, according to Backlinko. Worse, 60% of users aged 18 to 24 use an ad blocker, preventing publishers from monetizing sessions with this critical cohort, a significant risk no publisher can afford.

Compounding the challenge, publishers today face an uptick in user churn, which is often a direct result of an increase in clickbait ads that appear on their sites. ***Our survey found that 69% of publishers report clickbait ads appearing on their sites, despite their best efforts to screen for them.***

While most publishers say they see the full range of clickbait ads on their sites, some of the worst forms -- malicious extensions and misleading product offers -- are the most frequently seen. Nearly one-quarter of all publishers said they've received reports from users who experienced scams by clickbait ads that appeared on their sites, a clear indication of the problem's urgency.

A desire to fill all inventory is partly to blame for poor ads, as over half of respondents in this survey say they strongly or somewhat agree that they feel pressured to run lower-quality ads to make revenue goals. According to the survey, 47% were told to leave an ad up that they would have preferred to take down.

But those fill rates come at a high cost. When we asked survey respondents about the impact of clickbait ads, most said that they take a hit on their brand's reputation, prompt user churn, and hobble the publisher's ability to enhance the user experience.

How are clickbait ads getting on sites? What is the impact of such ads on the user experience? The publisher's brand reputation? To better understand the extent of the problem, we surveyed 148 publishers about their experiences with clickbait ads on their sites. A key goal is to understand why it occurs and whether or not publishers have the tools they need to eradicate it from their properties.

2. KEY FINDINGS

- **76%** of publishers say users have reported clickbait ads on their sites.
- **69%** of publishers say that clickbait ads appear on their sites. Only **18%** say that the problem is rare. **68%** say clickbait ads appear either time-to-time or fairly regularly. **43%** of publishers say the number of clickbait ads has increased over the past 12 months.
- **24%** of publishers report that their users experienced scams due to a clickbait ad that appeared on their sites.
- ***Malicious extensions*** and ***misleading product offers*** are the most frequent scams.
- Over half **(54%)** of respondents say they strongly or somewhat agree that they feel pressured to run lower-quality ads to make revenue goals. **47%** were told to leave an ad up that they would have preferred to take down.
- The most frequently cited impacts of clickbait ads on the publisher are: Diminishing the brand reputation, prompting churn, and undermining the publisher's strategy to enhance the user experience.
- Still, checking the quality of ads is mainly manual, as **78%** of respondents say they check reports they receive manually and remove them on a case-by-case basis.
- While clickbait is on the rise, only **39%** of publishers say they will hire additional resources to help them tackle the challenge in the next 6 to 12 months.
- Nearly one-third of all publishers are unfamiliar with cloaking—the scammer's key tactic for avoiding detection on a website.

3. DEFINING CLICKBAIT ADS & THE SCHEMES THEY LEAD TO

This report uses the term "clickbait" to define a range of fraudulent activities meant to deceive users through digital advertising. Generally speaking, clickbait ads pique a person's interest, then lead them into a social engineering scheme. Typically, clickbait ads piggyback off of current topics, such as rising energy costs or celebrity news and endorsements.

Post-click ad scams

Most common are post-click social engineering schemes, which entice users to enter into a scam based on trending topics, such as crypto or investment opportunities. We refer to such scams as social engineering because users willingly click and engage with the ads.

These ads can lead to a variety of scams, such as:

- Prompt users to pay for items for products and services that don't exist or work as promised. At present, financial scams are widespread. These schemes lead consumers to believe they are investing in bitcoin, but the fraudsters simply pocket their money.
- Steal PII data, such as credit cards, by presenting the user with a page that looks legitimate, such as a fake payment page
- Schemes to obtain sensitive information that can sell on the dark web
- Ransomware

How does clickbait enter the programmatic ecosystem?

Typically, bad actors purchase a license on a DSP and launch a warm-up phase where they pose as legitimate advertisers—i.e., they upload code that calls a legitimate ad that leads to a legitimate website. When we say legitimate, we mean that neither the ad nor landing page/website contains malicious code.

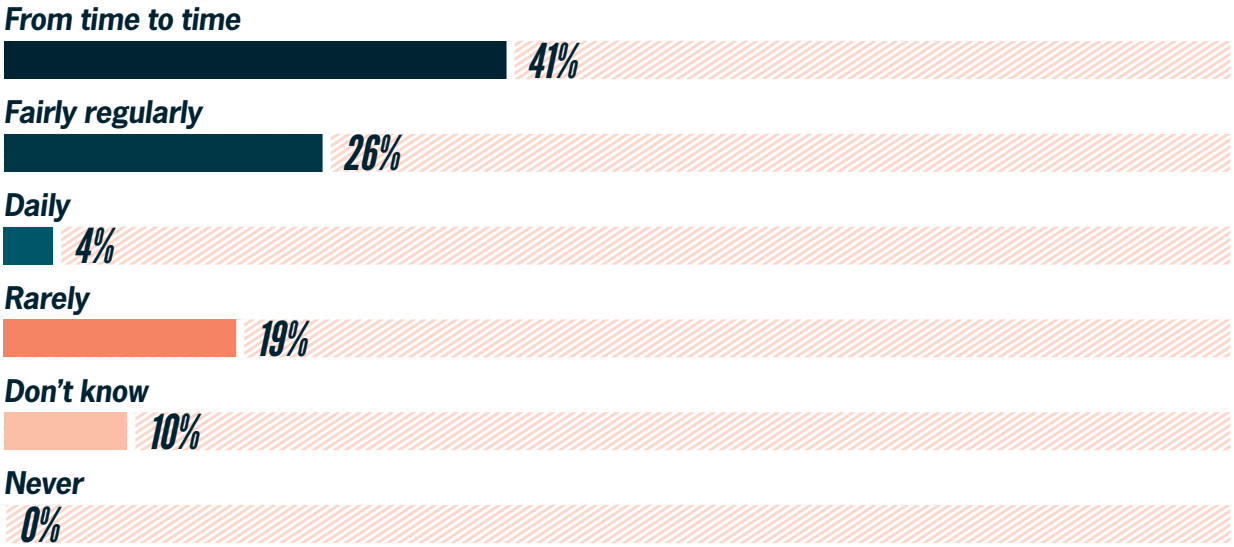
Most DSPs conduct a probation period for new advertisers. During this period, the DSP will look at a new advertiser's campaigns to determine if they're legitimate. Bad actors will not deploy any attacks so that the DSP approves them for continued advertising. Once they're flying below the radar, fraudsters switch the code in the background, a tactic known as cloaking (since the scam is hidden behind a cloak).

The extent to which the perpetrators of social engineering scams will go explains why so many people across the globe fall victim to these scams.

"Today's scammers go to great lengths to wrap their ploys in a cloak of legitimacy," explains Amnon Siev, CEO at GeoEdge, the leading ad security, and quality solutions provider. "They mimic fake news sites as landing pages and launch websites for the so-called companies behind the clickbait ads. They even create fake LinkedIn profiles for the company's leaders listed on the About Us page. Some will create fake news sites that include reviews from people who claim to enjoy fabulous success. They'll even launch Google Search ad campaigns for users who Google the company's name on the ad to ascertain if they're legitimate."

4. CLICKBAIT ADS AFFECT ALL PUBLISHERS

How widespread is the problem? When we asked how frequently clickbait ads appear on their sites, we heard:



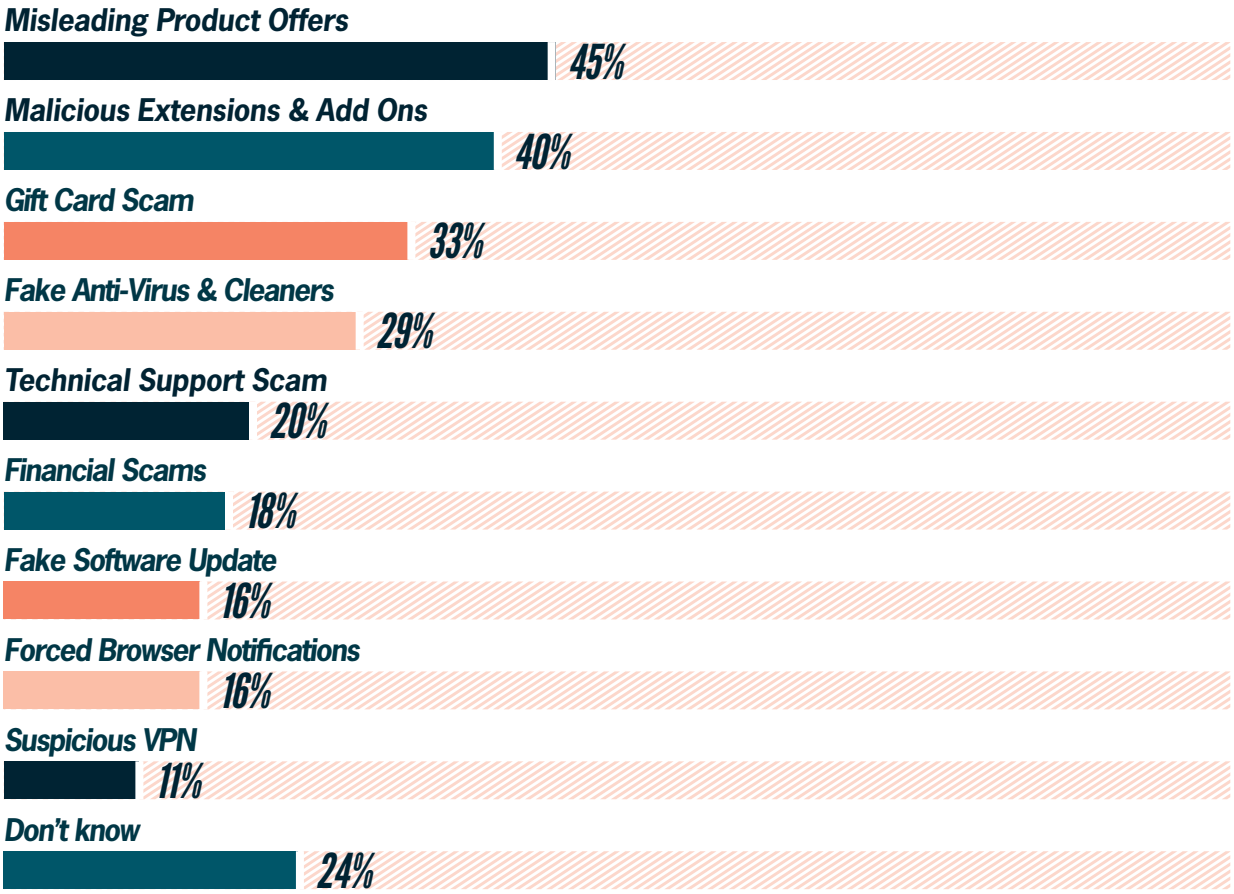
When we asked if the publisher has seen a rise in clickbait ads over the past 12 months, 43% said yes. We're not surprised that 10% of respondents couldn't say how frequently clickbait ads appear on their sites, given the vast number of ads placed via programmatic channels and the difficulty of tracking them.

43% of publishers say they've seen a rise in clickbait ads on their sites over the past 12 months.

Types of Clickbait Ads

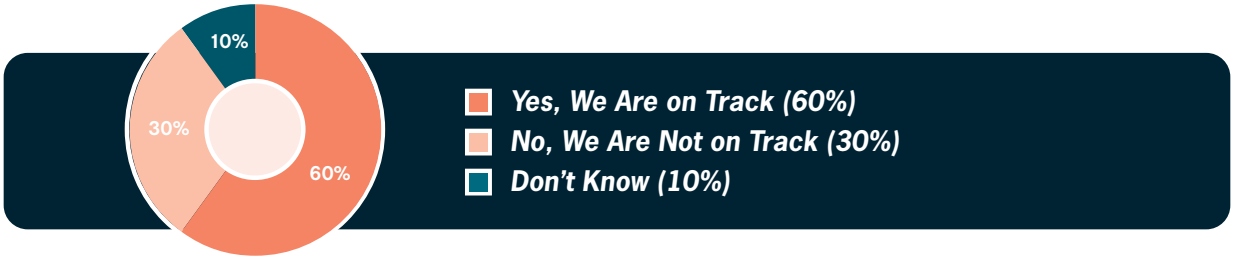
Clickbait ads seek to create urgency in users to prompt them into the scam funnel. Ad content can range from "virus detected" pop-ups to unique opportunities to invest in a hot stock or company.

When we asked which types of clickbait ads have appeared on respondents' sites since the start of 2022, publishers told us:



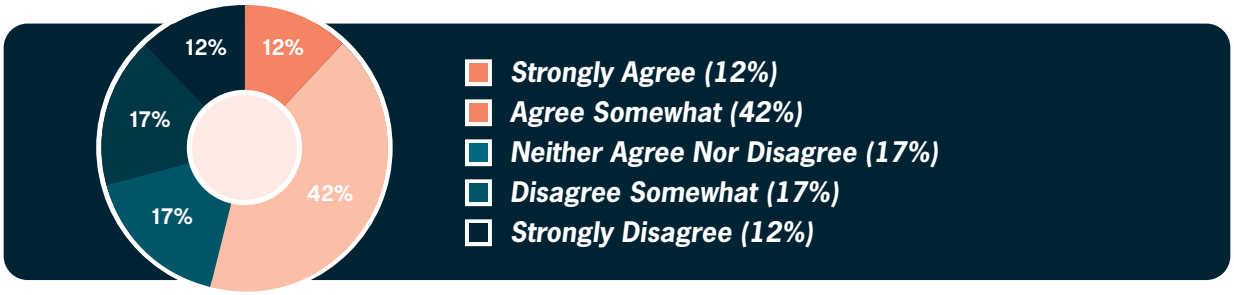
PRO TIP: *Scammers know that many publishers have ad quality systems to spot-check ad creatives and assess their legitimacy. To succeed at their trade, the scammers must somehow circumvent those protections. Cloaking refers to various mechanisms that allow scammers to cherry-pick the users who see their deceptive ads while attempting to remain hidden from anti-malvertising detection companies. In such cases, fraudsters will "fingerprint" users to ensure they're scam worthy. The way to stop these fraudsters is to detect fingerprinting and check creatives multiple times.*

Why do clickbait ads end up on publisher sites? Is it a result of publishers seeking to fulfill inventory at any cost? When we asked whether or not their companies were on track to meet their revenue goals for 2022, we heard:



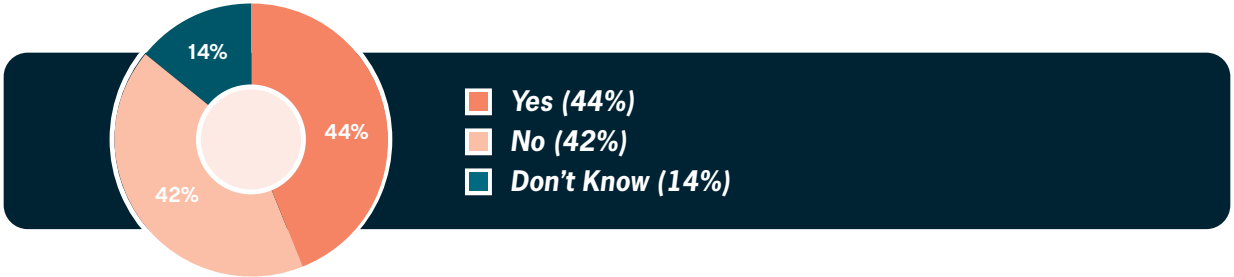
54% ***of respondents strongly agree or somewhat agree that they feel pressure to run low-quality ads when they fall short of their revenue goals.***

Probing further, we asked the respondents to what degree do you agree with this statement: "I feel pressure at times to run low-quality ads when we fall short of our revenue goals." They responded:



PRO TIP: *Develop a long-term monetization strategy. Craft a framework to articulate what brand-suitable advertising means for your brand and audience. Discuss questions such as: Is this advertiser type or content category of interest or offensive to our users? Look for a tool that allows you to create and apply granular rules to enforce security, content, and user experience standards. To cultivate strong relationships with your audiences, publishers must deliver safe, engaging, and relevant advertising that works for your brand.*

How severe is the user churn challenge publishers face at the moment? We asked respondents if they've noticed an uptick in user churn over the past 12 months. Here's what we heard:

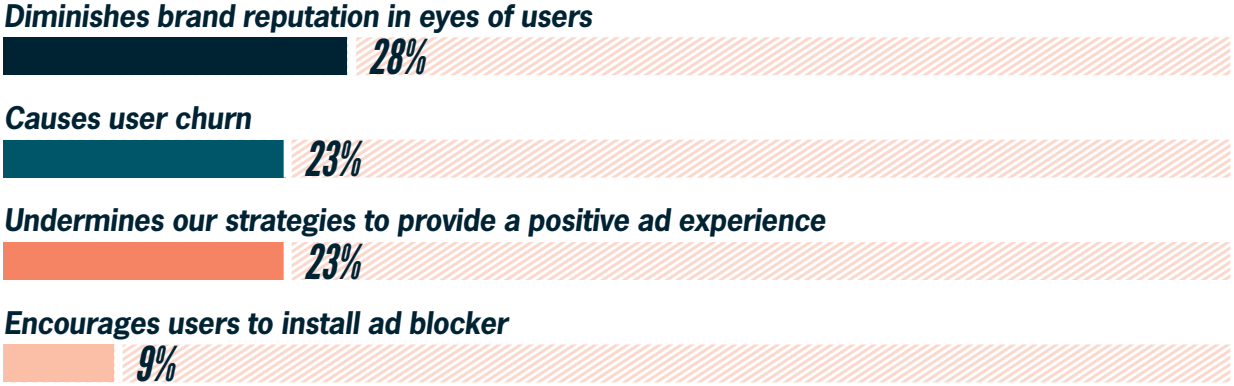


Every ad counts towards retaining user loyalty, engagement, and revenue. Eliminating clickbait creative and boosting ad quality translates into revenue upside– and enables a publisher's brand to stand out. When a user-first approach informs ad quality decisions, the benefits are felt by publishers and users alike.

5. IMPACT OF CLICKBAIT ON PUBLISHERS

We know that clickbait ads, and the fraudulent schemes they lead to, harm audiences and are equally damaging to the sites on which they appear. Unfortunately, publishers don't recognize the severity of clickbait on their sites. We asked publishers specifically about the damage clickbait ads wreak on their brand reputation, user loyalty, and monetization ability. The most frequently cited impact of clickbait ads on the publisher are: Diminishes the brand reputation, prompts churn, and undermines the publisher's strategy to enhance the user experience.

In your opinion, what is the impact of clickbait ads on your site? We heard:



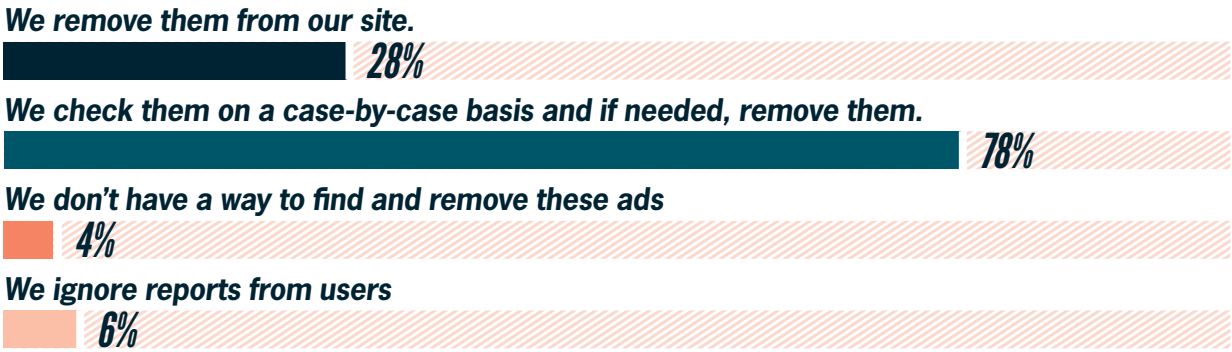
Enforcing ad quality is a largely manual process, as

78% OF PUBLISHERS

look at reported ads and remove them on a case-by-case basis.

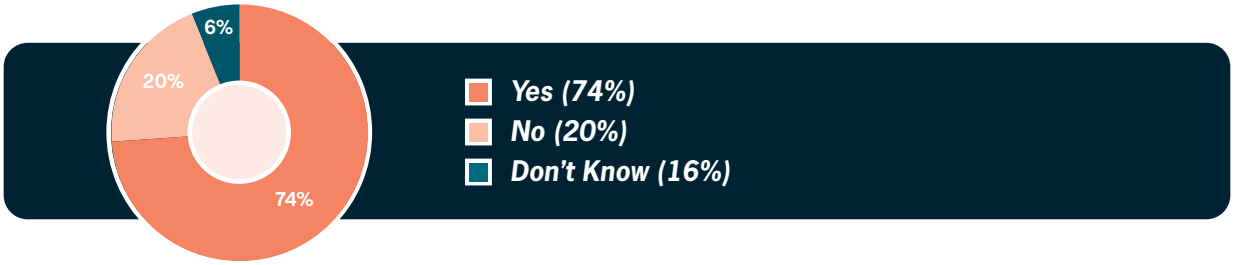
PRO TIP: *Checking ads to ensure brand suitability is ripe for automation, as the number of ads placed via programmatic advertising is too great for human oversight. What's more, the number of users who report clickbait ads pales compared to the number of users who actually see them. Publishers who solely rely on user reports are missing countless instances of clickbait ads that violate their ad quality standards.*

When we asked the respondents how their companies handle ads reported by readers, we heard:



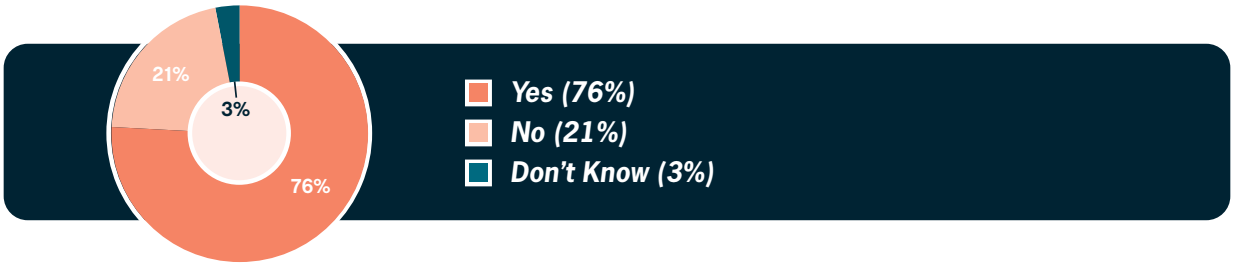
Clearly, publishers are keen to remove clickbait ads from their sites, as 74% of respondents said they provide a feedback loop for readers to report clickbait ads.

We asked: Does your site have a feedback loop so readers/users can express their opinion on the quality of ads that appear on your sites?



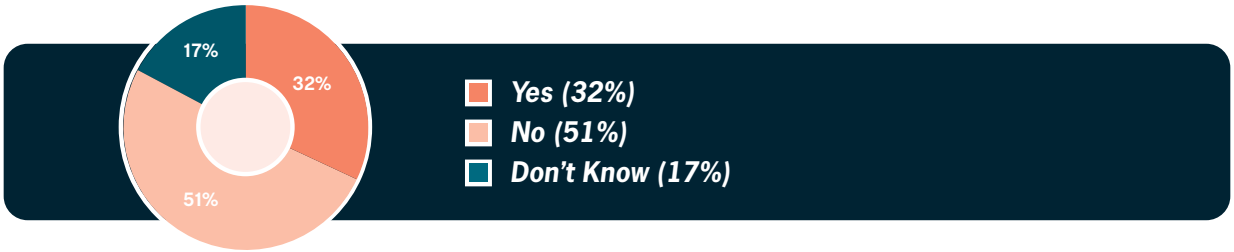
But do users take advantage of those feedback loops?

We asked: To the best of your knowledge, have users reported seeing clickbait ads on your site?



How fully closed are those loops? Publishers hear about clickbait ads on their sites but less about the scams behind them.

We asked: Do you know of any instances in which people complained on social media about clickbait ads or scams that have appeared on your site?

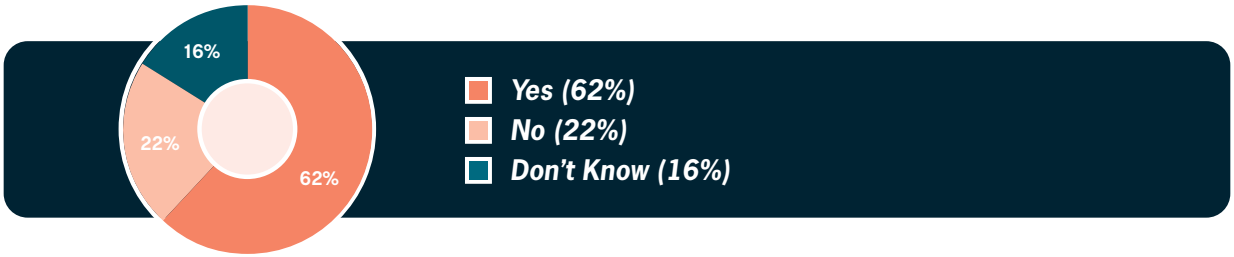


PRO TIP: *Don't rely on users searching for an email address to report poor ads. Include functionality within the ad unit itself that allows users to report bad ads directly to the AdOps teams (and not Google or third-party platforms). This approach will help build trust by starting two-way conversations between the user and publishers.*

Although publishers say they have feedback loops and that they receive information regarding poor ad experiences, it's clear that the process is not effective. The fact that nearly a third of publishers learn about scams on their sites via social media shows the need for a more accessible and integrated way to identify clickbait ads.

Publishers often hear about clickbait ads and scams that appear on their sites for the first time when a user complains about it on social media. That begs the question:

Do publishers understand why users churn? To find out, we asked them:



PRO TIP: *Consider deploying a real-time user feedback tool on your site. GeoEdge's Report by the User removes the guesswork from the process of creating positive ad experiences. Publishers can learn instantly about any ads users are unhappy with and can inform future ad strategies with those insights*

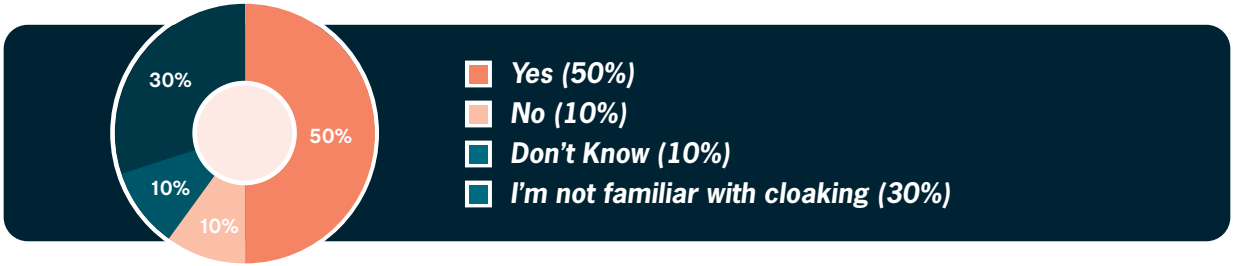
6. PUBLISHER PREPAREDNESS IN THE FACE OF CLICKBAIT ADS

NEARLY ONE-THIRD OF ALL PUBLISHERS

are unfamiliar with cloaking—the scammer's key tactic for avoiding detection on a website

Bad actors have a few ways to exploit the ad delivery system. However, at present, their favorite tactic is to disguise themselves as legitimate advertisers (aka "cloaking") and to calculate which users are "scam worthy" in selecting which ad to show them.

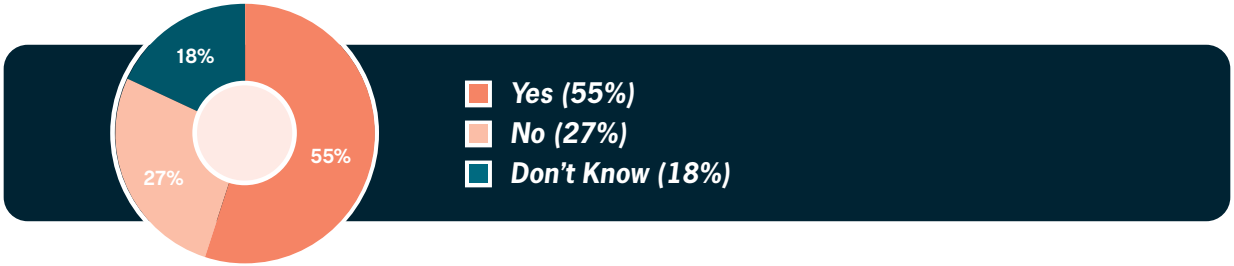
When we asked respondents specifically about cloaking, about half said they have the tools to detect it. More disturbingly, we found that nearly one-third of respondents are unfamiliar with the term:



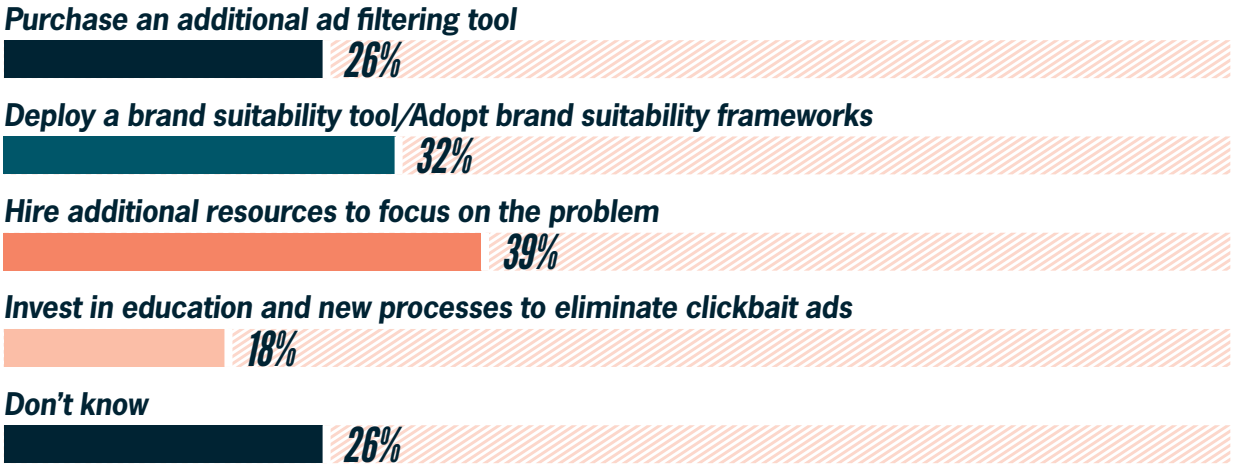
PRO TIP: *Cloaking can be difficult to detect and requires a multi-pronged approach, including assessing the content of the innocuous ads and their associated landing pages. Cloaking ads tend to feature text that is not related to the page's content or is of keen interest to users.*

Many ads lead to landing pages that have no relation to the ad itself, which is why publishers must check the entire flow of the creative. While most publishers report using an ad quality tool to monitor the ad and its landing page for quality purposes, such devices won't catch cloaking if they only review the ad and landing page once. To catch cloaking, a solution must check both the ad and landing page.

Looking ahead to the next 6 to 12 months, will your company focus on eliminating clickbait ads and scams on your site?



If eliminating clickbait ads and clickbait schemes is a top priority in the year ahead, which approach is your brand most likely to take? (Check all that apply)



7. THE PLAYBOOK

- Adopt an anti-clickbait solution that extends across the entire ad delivery process, meaning it can monitor the content and images on both the creative and the campaign's landing pages. Dangerous clickbait categories should be automatically blocked: Malicious Extensions & Addons, Financial Scams, Misleading Product Offers, Brand Infringement, Forced Browser Notifications, Fake Antivirus & Cleaners, Fake Software Updates, Suspicious VPN, Gift Card Scams, and Tech Support Scams.

- Review the same campaign creative multiple times, emulating different scenarios to determine if "legitimate" ads you see were merely decoys. GeoEdge finds that upon scanning the same ad multiple times, they're often directed to a decoy and other times to a malicious landing page. This is why performing a single scan is far from adequate.

- Deploy a multi-layer detection tool that looks at different attributes of an ad to determine its legitimacy. If the scammer has launched a decoy article unrelated to the creative, it's possible to proactively detect and block the ad. Deploy a detection engine that knows how to look for and detect fingerprinting—an indication of cloaking in real-time.

- Look at the structure, images, and text of the sites that ads lead to in order to assess if something is a bit off. You can block only the offending ad if a site is fake.

- Ensure your Ad Ops team is up-to-date on new and evolving ad quality challenges. From financial scams and brand infringement to post-click-cloaking attacks—your team should be aware of the latest threats to your audience. Keep your team on the same page with the latest lexicon to accurately define the bad ads which seek to wreak havoc on your audience.

- Empower your users to report clickbait ads directly to you. GeoEdge has launched the "Report by the User", which displays a bell icon in the corner of the ad that users can click on to report unwanted, offensive, or otherwise inappropriate ads. Once clicked, a report is sent to the publisher immediately. This closed loop helps the user feel heard and builds trust between the user and publisher. Input that comes directly from the audience creates a framework for providing consistently relevant and engaging ad experiences, leading to a sustainable, profitable digital ecosystem.

8. ABOUT THIS SURVEY

Types of Sites Represented:	
General news	19%
Business	6%
Sports	12%
Lifestyle	19%
Entertainment	12%
General	12%
Tech	6%
Financial	12%
Other	5%

Number of Employees in Company	
1 to 49	14%
50 to 499	52%
500 to 999	18%
1,000 to 4,999	12%
5,000+	4%

Respondent's Level of Seniority:	
C-suite	5%
Vice President	13%
Director	33%
Manager	46%
Other	3%

Does your site rely on digital advertising to fund its operations?	
Yes	87%
No	11%
Don't know	2%

To what degree does digital advertising fund your site's operations?	
Almost 100%	13%
75 to 99%	22%
50 to 74%	40%
Less than 50%	20%
Don't know	5%

To what degree does digital advertising fund your site's operations?	
Ad network	38%
SSPs	48%
Programmatic	62%
Direct deal with an advertiser	65%
House ads	57%
Content recommendation widgets	26%
Other (please specify)	0%

The global leader in strategic insight on the future of digital media and advertising technology. Through our conferences, website, and original research, we offer unparalleled in-person experiences and unique, high-quality content focused on media operations, monetization, technology, strategy, platforms and trends. We provide a forum to share best practices, explore new technology platforms and build relationships.

AdMonsters has built its reputation on providing objective editorial leadership based on deep, real-world expertise. We have continued to evolve our editorial strategy to address the changing needs of the market and, as a result, AdMonsters has attracted a highly focused audience who are at the forefront of the industry, and leading marketing partners have found AdMonsters to be a powerful channel to reach these decision makers. Today, our portfolio of integrated media solutions includes industry-leading live events, our innovative Connect content solutions, email marketing programs, and more.

AdMonsters is part of the Access Intelligence family of companies.

For more info:
See admonsters.com
Follow us on Twitter: @AdMonsters
Facebook: facebook.com/admonsters

Media contact:
marketing@admonsters.com
Sponsorship contact:
sales@admonsters.com

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/apps offer a clean, safe and engaging user experience, so publishers and app developers can focus on their business success.

App Developers and 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.

To learn more, visit: **www.geoedge.com**

sponsored by: