NETACEA

The Bot Management Review: How Are Bots Skewing Marketing Analytics?

Contents

INTRODUCTION

Businesses waste a great deal of money serving customers who do not exist. Each bot that arrives on a site may not be much of a problem—assuming, of course, it is prevented from disrupting the site or buying up goods for resale. But the sheer number of bots means that there is a considerable cost in serving them. Even if a business prevents every attempt at fraud, whether it's account takeovers or checking stolen card details, there is a cost in serving bots.

This cost goes beyond the infrastructure necessary to serve bots. If bots and real customers look just the same, what does that mean for making decisions based on what customers are doing on a site?

Marketers make decisions based on data, but if the data is inherently flawed, can marketers be making good decisions? If marketing teams base their strategies on flawed data, can they have any chance of success?

We find that marketing teams are often first to recognise that a business has a bot problem, even before security, because they have visibility of traffic to the site and mobile app. Unfortunately, security teams and marketing teams, with their very different functions, are rarely in close contact. The threat of bots means security teams and marketing teams need to work together: the marketing team may uncover the problem, but the responsibility for fixing it lies with the security team—and the security teams' budget.

To understand this problem better, we asked businesses based in the USA and UK, across the eCommerce, telecommunications, entertainment (including online gaming and streaming), travel and financial services markets to consider the effect of bots on their analytics. We wanted to understand not only the impact of bots on a business' bottom line, but how it compares to ad fraud, a more deliberate attack that enjoys a higher profile. Netacea conducted this survey in collaboration with independent B2B research specialist Coleman Parkes. 440 businesses were surveyed, with turnovers ranging from $350m to over $7bn.

EXECUTIVE SUMMARY

Security, it is said, is everyone's responsibility. Security teams may for example, create policies that best protect a business, but it is up to employees to implement and follow many of those policies to keep the business safe. For example, as good as a password policy is, you undermine it by writing login details on a Post-It and attaching it to a monitor.

But, this works in other ways too. Security teams aren't always best placed to detect threats. Bots that do their very best to disguise themselves as customers may not be easily spotted on the network, but may show up afterwards in marketing analytics data. The only way to fix this is if the marketing team works with the security team to fully understand the problem and implement a solution. Without this partnership, one team knows there is a problem but doesn't have access to the solution, and the other isn't even aware of the problem.

Of course, this is only a problem if skewed analytics, as caused by bots, is a big problem. We decided not only to ask, but to compare it to one of the biggest problems facing marketers today: ad fraud, also known as click fraud.

This is such a problem that some see it as potentially making the entire online advertising industry untenable. Even those with less apocalyptic views see it as a major problem, making decisions on online advertising very difficult.

Among our respondents, ad fraud was a problem for 73% of businesses and cost an average of 4% loss in revenue.

Skewed analytics was a problem for 68% of businesses and cost an average of 4.07% loss in revenue.

It turns out that these two problems, one widely understood and reported on, and one far less so, are almost identical in their effects on businesses. This is true across the sectors we asked: eCommerce, telecommunications, entertainment (including online gaming and streaming), travel and financial services. None were immune to the problems of bots.
Across all sectors, a majority of respondents reported a financial loss.

These losses were often down to bad decisions. At least half of businesses reported running special promotions based on incorrect data, ordering new stock due to incorrect data, or even burning through a marketing budget thanks to bots.

Bots are persistent troublemakers for businesses. They are at the root of account takeovers, card fraud, and the automatic buying and selling through third-party sites. But the problem goes beyond that. Even if businesses can effectively deal with the problem of bots directly, they are indirectly causing big losses on a scale similar to one of the biggest problems facing marketing teams today. Only through marketing and security working closely together is there hope of fixing this.

SKEWED ANALYTICS AND AD FRAUD – WHAT’S THE DIFFERENCE?

First, we need to differentiate between what we mean by skewed analytics and ad fraud.

Skewed analytics is the result of bot activity on websites. Bots visit websites for a number of reasons—to scrape data from the site, to add to a search engine, to attempt to take over accounts or to buy items from the site to be resold elsewhere. Whether the bots are successful or not, this means there is traffic on the site that is not from real customers. The intent of the bot operators is not to skew analytics, but it can affect the decisions that businesses make without them knowing.

Ad fraud is when a bot imitates legitimate traffic, generating web views. Those paying for advertising are wasting their money advertising to automated computer processes. In fact, the WFA predicts the ad fraud market will be worth $50 billion by 2025.[1]

Different types of fraud include:

- Click fraud, where fake clicks are generated for pay-per-click advertising
- Impression fraud, where video ads are displayed to no one
- Retargeting fraud, where a bot can mimic a human’s intentions, and receives niche targeted ads that are manipulated with false clicks or similar

The point of ad fraud is to manipulate the ad market—unscrupulous ad networks can take business away from those who are being far more honest. Criminals turn a profit by hosting genuine ads on fake sites with low-quality copied content and faked automated visitors, and by offering services that click on rival ads, eating up the competitor’s advertising budget through bot activity.

This manipulation and other bot activity can also lead to skewed analytics. Marketers use the way people are using a site to make decisions—where are people arriving from? What are they doing when they are here? What does that tell us about our strategies? This data is incredibly important.

Unfortunately, if a great deal of bot traffic exists on a site, and goes undetected, it will alter the data. If you don't have an accurate view of customers' behavior on your website, you are likely to make poor decisions about their buying journey and have little understanding of what they want and need from your website.

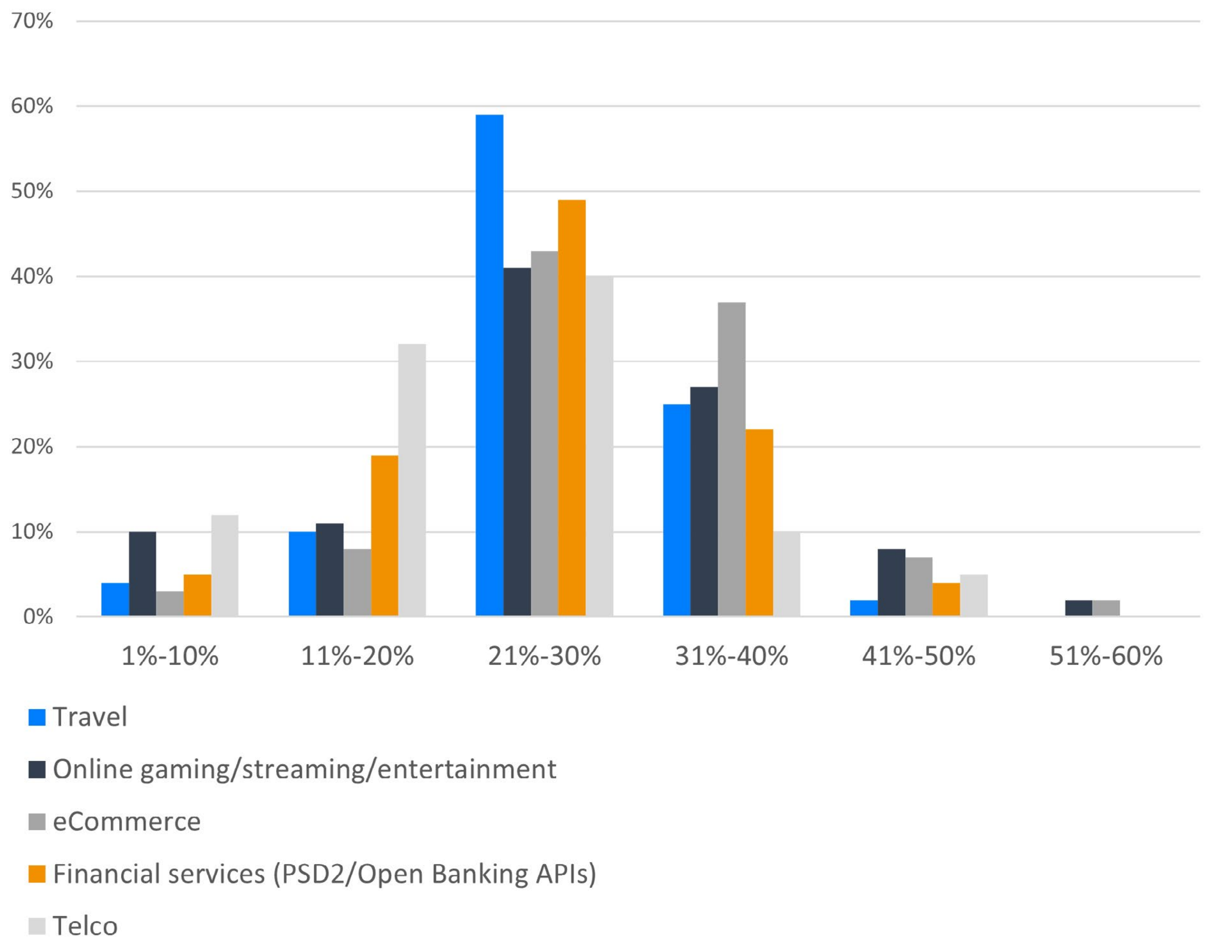
Both ad fraud and skewed analytics are problems that businesses will have to tackle. We want to know if they are meeting these two different, related challenges, and how well they are doing.

Source: Ad Fraud Statistics 2021

HOW DO MARKETING ANALYTICS INFLUENCE DECISION MAKING?

Most businesses base around a quarter of their marketing decisions on analytics. This is higher for eCommerce (30%) and online gaming (27%), businesses that rely more on reacting in near real-time to what their customers are doing on their sites, but only 6% of businesses say that less than a tenth of their marketing decisions are made using analytics.

We suspect this number is a little underreported, as digital ad sales account for two-thirds of media ad spending in the UK and over half in the USA. However, even if we take this finding at face value, there are a lot of decisions being made using analytics. This is understandable, as you can receive feedback quickly and tune decisions based on this feedback—if the analytics are correct.



Q1 What proportion of your marketing decisions do you estimate are based on analytics?

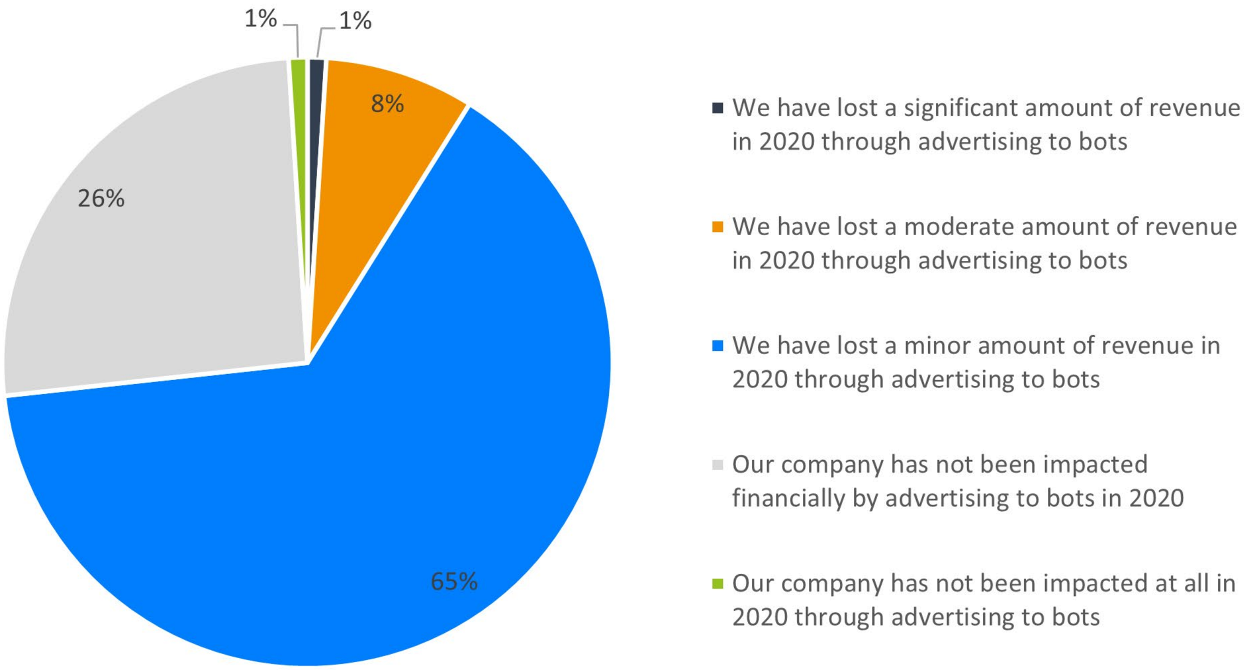
A KNOWN PROBLEM: LOSSES DUE TO CLICK FRAUD

Around two-thirds of businesses say that they have lost at least a small amount of revenue by advertising to bots, with 8% losing a moderate amount of revenue. Only around one-in-four said that they had not been impacted, financially or otherwise.

Of the sectors surveyed, telcos were the outliers, with 22% saying that they had lost a moderate amount of revenue, and 35% saying they had not been financially affected at all. Telcos had it both better and worse than other businesses when it came to ad fraud.

We also asked businesses to estimate their financial loss as a percentage of online revenue due to advertising to bots. The average business thinks it has lost 4% exactly, though there was a wide spread of answers here. Thirty percent of businesses say that they have lost 5% or more online revenue, and only around 4% say that it is as low as 1%.

With these results, it's fair to say that ad fraud—the targeted type, where the harm caused is direct—is widespread and is affecting a business's bottom line. This is as we would expect from such a well-reported issue.



Q2 Which of the following statements best applies to your company?

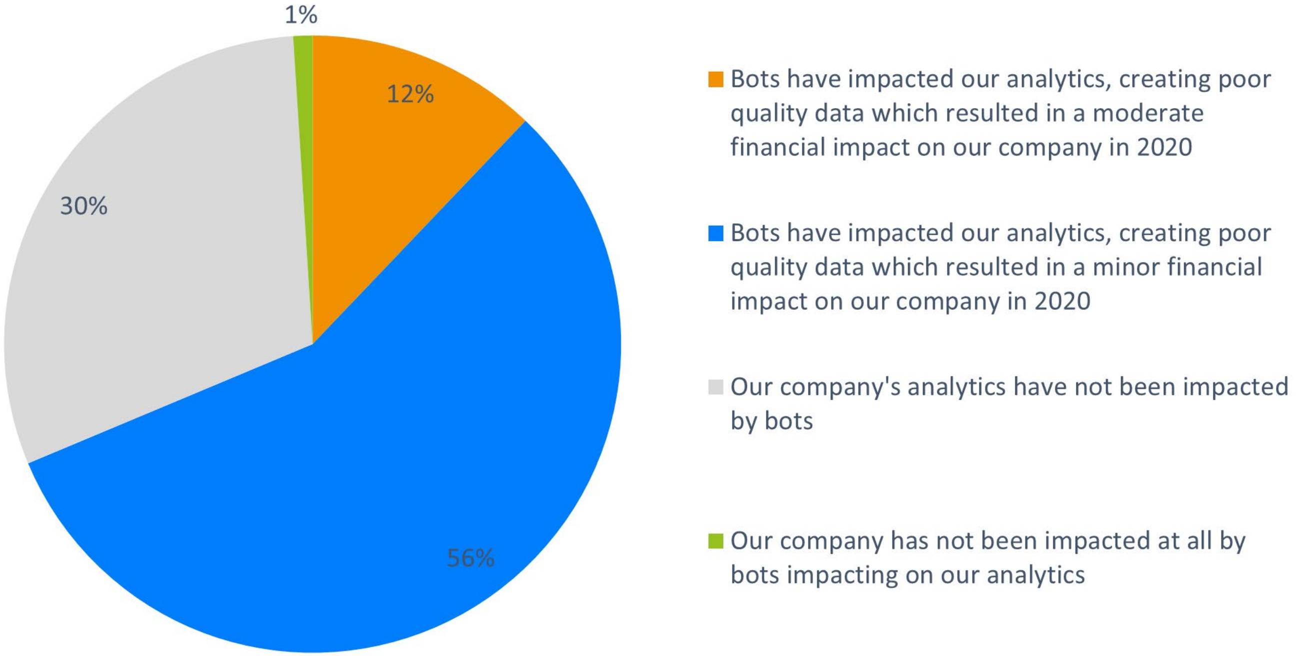
Those who have been affected and those who have not detected any effect are impossible to separate here, and we suspect many are unaware of the problem. This report is based on research into what businesses know about, and the scale of the problem could be even higher.

THE SILENT THREAT: SKEWED ANALYTICS

How does the well-known problem of ad fraud compare to the lesser publicized problem of skewed analytics?

We found that 68% of businesses say that they have suffered a financial impact due to bots. This is fairly consistent across all organizations, but travel and eCommerce firms had it slightly worse. Almost no businesses say that they don't know the impact of bots on their business, and just under a third say they have seen no effect.

This is a very similar result to ad fraud. Both ad fraud and skewed analytics are having a noticeable impact on around two-thirds of businesses.



Q3 Which of the following statements best applies to your company?

When it comes to the average loss these businesses are making, the number is actually very slightly higher than click fraud: 4.07%. We see telcos, eCommerce and travel businesses reporting slightly higher losses than other sectors.

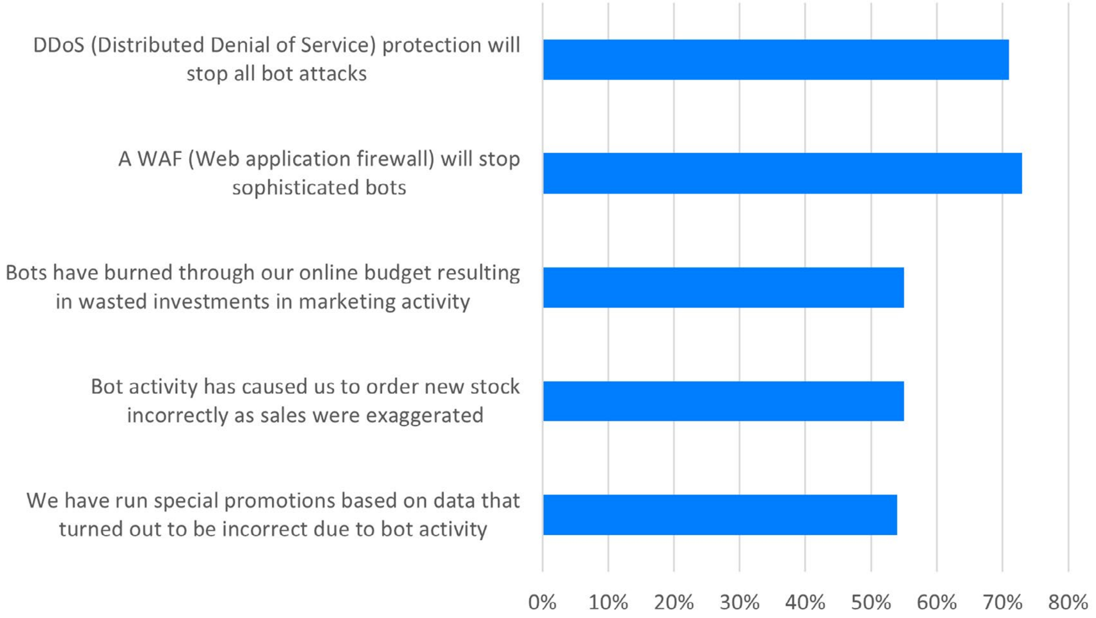
Click fraud and other types of automated ad fraud enjoys a far higher profile than skewed analytics, but businesses are reporting that the financial impact of skewed analytics is greater.

We also wanted to know in more detail what effects businesses had noticed thanks to skewed analytics. Over half of respondents have:

- Run special promotions based on incorrect data
- Ordered new stock due to incorrect data
- Wasted investment and "burned through" a marketing budget thanks to bots

Around two-thirds of telcos say they experienced skewed analytics due to bot activity, while a similar proportion of eCommerce businesses have wasted budgets thanks to bots.

While skewed analytics may be an under-reported problem compared to ad fraud, businesses are aware of the issue and can see that is detrimental. Unfortunately, while they are aware of the consequences, they are less aware of how to fix the problem, with a majority believing that DDoS protection and web application firewalls (WAFs) are enough to stop bots. DDoS protection will stop botnets, not bots, and WAFs will stop less sophisticated bots, but a dedicated bot solution is necessary to fix this problem.



Q4 Do you agree with these statements?

CONCLUSION

Ad fraud is a well-understood phenomenon that dominates the marketing headlines. Some have even predicted that online advertising is doomed thanks to the practice. Any decision that a marketer makes about online advertising needs to take the possible effects of ad fraud into account.

But our research suggests that skewed analytics cause just as much damage to businesses. An equal number of businesses say that they can see the effects of skewed analytics, and the average loss to revenue is very slightly more than ad fraud.

It's perhaps easy to focus more on ad fraud than skewed analytics. One is a direct attack designed to derail a business, while the other is far less direct. Assuming that businesses can prevent bot attacks such as account takeovers, the secondary effects of bots can seem more benign. But our research shows that they are both equally damaging to businesses. One, perhaps because it enjoys greater visibility and is easier to understand, gets all the press.

Even worse, our research shows that those making marketing decisions don't understand how they can avoid making bad decisions based on bad data from bad bots. It's crucial that marketing teams and security teams work closely together to fix the problem. Marketing teams are often best placed to identify the problem, but security teams are needed to fix it. This closer relationship shouldn't just be a one-time meeting, but an ongoing process where the teams work together to ensure that the business is using the best possible data.

If they don't, marketers run the risk of clamping down on ad fraud, but at the same time, ignoring a threat that is just as dangerous to their business.

BEST PRACTICE RECOMMENDATIONS

If you suspect bots are skewing your marketing analytics, we recommend asking these questions to identify a potential issue.

- **Has the number of new sessions to your site spiked?**

  An abnormally large number of new sessions alongside high bounce rate and low session duration is an indicator of automated traffic activity.

- **Is your average session duration below three seconds?**

  A recurring low session duration may not be due to the speed of your website, but crawlers scraping your site for images and content.

- **Is your average bounce rate high?**

  Whether it's site-wide or on a selection of pages, a high bounce rate of between 95% and 100% implies the presence of bot traffic.

- **Has your conversion rate dropped?**

  A spike in new sessions without an increase in conversions will reduce your overall conversion rate.

- **Has direct and referral traffic increased?**

  These two channels are common sources of bot traffic and where you are likely to see the highest spikes in traffic.

If there is a problem, it's not enough to simply ban bots from your site—not every bot is bad, and this action could tank your SEO. It's important to have visibility of all traffic on your website, and have control over the visitors that are allowed through.

As not every bot is bad, it's important to accurately categorise the types of traffic on a site, and have insight into how the human and bot traffic is behaving on a site.

What are bots costing your business? Head to Netacea's bot calculator to find out today.