fraud0.

Apr 2022

Fraud in E-Commerce

Impact of bot traffic on your business

www.fraud0.com

Table of Contents

01 Introduction

Every e-commerce website on the Internet has a bot problem - yours included!

Let us start with a fact: Every e-commerce website on the Internet has a bot problem - yours included! According to our data, 57% of global Internet traffic is generated by bots.

Bots visit your website regularly for various reasons: Some simply want to ping your server to check its uptime, but some bots are more malicious in nature. These bots want to harm your website, your advertising budget or even your whole business in various ways:

- Crash your server via DDoS attacks
- Steal credit card details of your customers
- Scrape your prices to benefit your competition

However, the biggest impact of criminal bot attacks on e-commerce is ad fraud.

The bot problem is growing by the day, and more and more money is being wasted from your advertising budget.

The following white paper highlights the significance of bot traffic and shows you exactly who is attacking you, how they do it, and what the impact of the attacks is on your business.

We will also show you why you should protect yourself from bot traffic and how you can do t.

16%
of all clicks are fake or low-quality

Automated bots are programmed to click on your ads and continuously drain your marketing budget just to fill the pockets of fraudsters. According to our own data, 16% of all ad clicks are invalid or low-quality.

>40%
of businesses lose 3% - 10% of revenue

Over 40% of businesses lose between 3% and 10% of their revenue to automated bot attacks.

$81
billion in losses expected 2022 from ad fraud

Malicious bots are largely responsible for the majority of the $81 billion in losses expected in 2022 from digital advertising fraud.

02 Bot Operators

Bots are usually operated by one of the following three groups:

- Competitors
- Resellers
- Criminals

While it is true that all bot operators have a criminal intent, the motivation and scale of their attacks differ greatly.

Competitors are in most cases constantly interested in your content in order to undercut your prices and gain a competitive advantage, while Resellers are mostly seasonally interested in your inventory and limited-edition product drops.

The highest criminal motivation have fraudsters and hackers, trying to defraud you of your advertising budget and compromising your customers' accounts. This group harms your business the most.

Competitors

Competitors use bots to gain a competitive advantage and increase their market share. This can happen in two ways: First, competitors use price scraping bots to determine the current prices of your products. This gives them full price transparency in the market and enables them to dynamically undercut your prices.

Second, competitors use content scraping bots to gain market insights. This may be the case when they expand into other markets and want to determine which products are sold at which prices and how the products are communicated to the target audience.

Resellers

Resellers actively and regularly use bots on e-commerce websites. The best-known cases are "sneakerbots," which focus on limited-edition sneakers from major brands such as Nike and Adidas. But so-called "Grinchbots" are also frequently used during the holiday season to hoard as much inventory as possible of items that are in high demand.

In both cases, the aim is to reduce the availability of these items and create a secondary market where resellers can charge higher prices due to the high demand.

Criminals

The last and most intrusive group are criminals. They exploit the data and functionality of e-commerce websites in a variety of ways. It starts by brute forcing credentials to gain access to existing customer accounts to steal personal data and payment details or use this data for fraud. It goes on by crashing an e-commerce website through DDoS attacks, committing gift card and loyalty point fraud, to creating fake accounts and using cracked credit card details.

But it does not have to be someone trying to hack your e-commerce website. Most fraudsters work for you unnoticed, hidden in the wide world of the Internet, clicking your ads with automated bots in order to earn a part of your digital ad spend. These criminals often set up fake websites, stack multiple ads on top of each other and let bots click them just to defraud you out of your money.

The impact of criminal bot activity on e-commerce is far-reaching. Upset customers locked out of their accounts or defrauded, higher customer service costs due to the increasing number of complaints, and even higher IT costs as the company has to investigate the incident and fix vulnerabilities in the infrastructure. However, the biggest impact of automated bot attacks from criminals is undoubtedly ad fraud.

03 Bot Anatomy

Before we dive into the threats of bots, we need to understand their functioning and anatomy. Nowadays, it is becoming more and more difficult to detect bots, as they are becoming more and more sophisticated, very good at covering their signature and better and better at imitating a real human being.

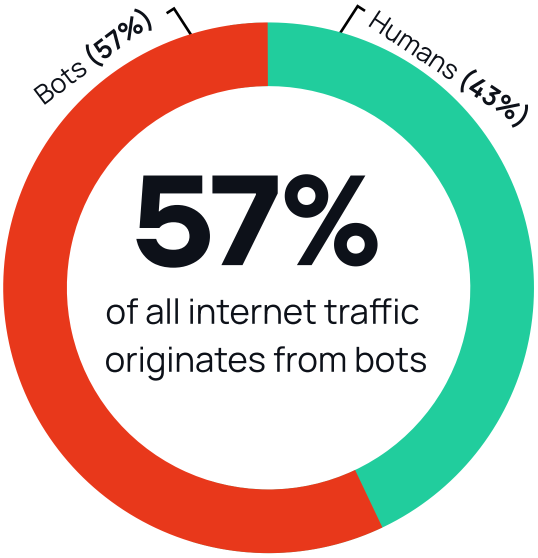
BOT ACTIVITY ON THE INTERNET

It should come as no big surprise that the majority of internet traffic these days originates from bots. While some automated traffic is welcome, such as search engine crawlers, the vast majority of bot traffic is malicious and attempts to harm businesses in various ways. According to our data, 57% of global Internet traffic is generated by bots in one form or another.

ORIGINATING COUNTRY

A few years ago, bots could be easily identified by their location. Most were deployed in emerging markets such as India, Thailand and Bangladesh. As the cost of servers from Google, Microsoft and Amazon increasingly dropped, bot operators also switched to these more powerful data centers. Nowadays, most bot traffic comes from Western countries, first and foremost the USA.

Bot Activity on the Internet



Originating Country E-Commerce Bot Traffic

USA	67.3%
Germany	9.2%
China	6.4%
India	4.5%
Other	12.8%

FAKE BOT IDENTITIES

Google Chrome is the most used browser in the world with over 65% market share. It is not surprising that bots pretend to be exactly this browser in order not to be detected immediately.

> Our data shows that over 70% of all bots identify themselves as Chrome browsers via their user agent string.

Fake Identity E-Commerce Bot Traffic

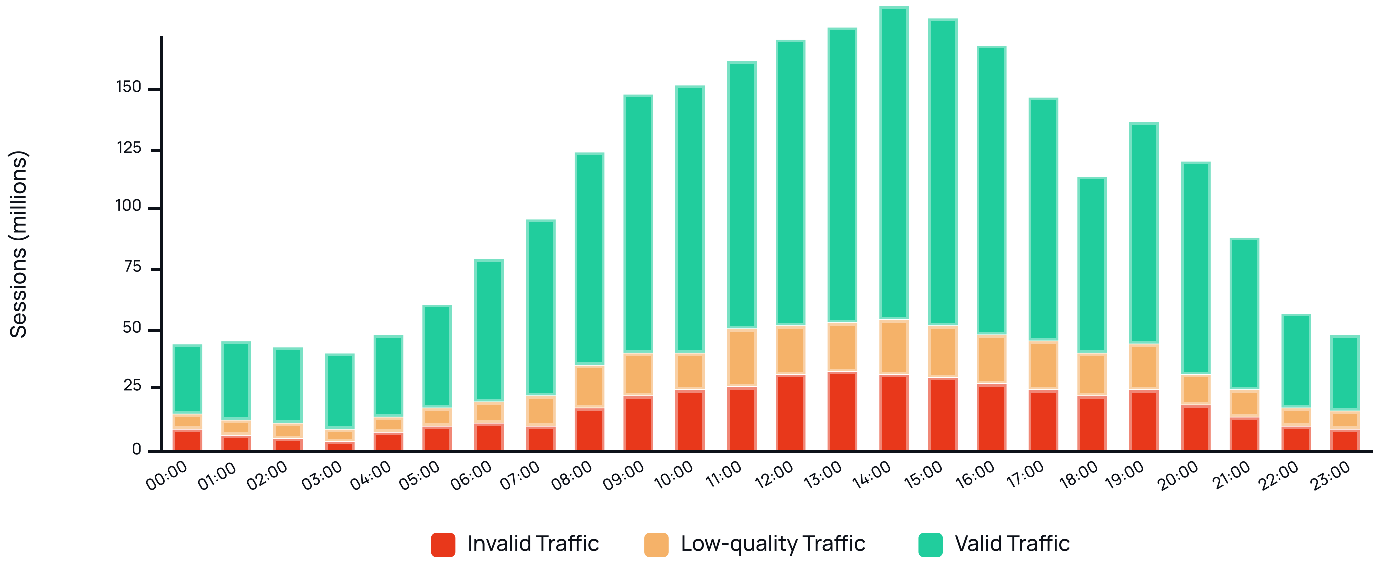
Chrome	73.1%
Firefox	11.4%
Safari	5.8%
Samsung Internet	3.6%
Other	6.1%

BOT ACTIVITY FOLLOWS THE STANDARD WORKDAY

While bots used to be consistently active during the day and night, this behavior has changed. Bot activity has adapted standard working hours and shows a bell-shaped curve with activity peaking in the morning hours and less activity during the night.

This has made it much more difficult to detect outliers based on temporal activity, as bots mimic human behavior and thus infiltrate visitor statistics without hindrance.

Bot traffic daily activity



04 Bot Threats for E-Commerce

After taking a look at bot operators and understanding bot behavior, it is time to look at the most common threats from automated bot traffic on your e-commerce website.

WEB SCRAPING

73% of businesses experience web scraping attacks by bots at least weekly and 20% even daily, making web scraping the top bot attack type[1].

Malicious web scraping can harm your business in several ways. The two most often used methods are price and content scraping.

73% of businesses experience web scraping attacks by bots at least weekly and 20% even daily.

Price Scraping

Price scraping bots are most often used by competitors to undercut prices and increase their sales. Lower priced competitors monitor your prices constantly and quickly adjust their own.

Impact on Your E-Commerce

While it is difficult to quantify the financial impact of scraping bots, it affects your market share, revenue, and your overall business success due to competitors' gaining an unethical advantage.

Content Scraping

Content Scraping bots gather content from the website and use it elsewhere. This content can be used to set up a fake website used for various ad fraud schemes or even phishing attacks, mimicking your well-known e-commerce brand.

Impact on Your E-Commerce

Scraping and republishing content can do serious damage to a business' search engine optimization (SEO) due to duplicate content. It can also lead to loss of revenue for the company, for example, if it is paid data.

[1] State Of Online Fraud And Bot Management, Forrester Consulting, (Jan 2021)

SKEWED ANALYTICS

Based on your analytics reports you make business decisions and develop future strategies, so you must have reliable data at your hands. With the majority of your e-commerce traffic coming from bots, this data gets skewed.

Bots infiltrate your reports, leaving you with uncertainty about whether the data is truly meaningful about your audience. They even consent to your cookie banners, which also skews your opt-in reports.

Impact on Your E-Commerce

Gaining the wrong insights and making the wrong business decisions based on inaccurate and skewed analytics data can dramatically harm your e-commerce business.

How to detect bots with your own analytics

To detect fake bot traffic within your analytics, you have to look for patterns.

These could be:

- Spike in new visits
- Spike at unusual times (e.g. at night)
- Low average session duration (< 1-2 sec)
- High bounce rate (>98%)
- Unusual user-agent string
- Drop in your conversion rates
- Increase in direct and referral traffic

After you successfully identified the abnormal patterns, make sure to exclude them from your future reports.

WASTED AD SPEND

The biggest concern with bot traffic for your business is fake clicks on your advertising campaigns. Not only does it cost you money, but it is also the cause of skewed remarketing lists, polluted analytics, and can even mess up your opt-in rates. The goal of fraudsters who use bots to click your ads is to move money from your advertising budget into their own pockets.

To make their bots look and act like a human and have a “browsing history”, bot developers want their bots to collect cookies and remarketing pixels from a variety of different websites and e-commerce stores.

Simply put, bots pretend to shop online. They visit various (e-commerce) websites, consent to cookie banners, add high-value items to their shopping carts to be seen as potentially valuable customers, and are therefore also tagged for remarketing. The more “browsing history” a bot has, the more it looks like a real human when infiltrating your data.

16% of all clicks are fake or low-quality

Impact on Your E-Commerce

Our data shows that 16% of all ad clicks are fake or low-quality. The consequences for you as an advertiser are mainly high cost-per-clicks (CPCs) and overall higher advertising expenses due to the fake ad clicks.

It is also a vicious spiral for your ad campaigns: Bots click on your ads and drain your advertising budget, only to be added to your remarketing lists and steal even more money.

Bot Threat	Impact on Your E-Commerce
Credit Card Fraud Attackers use stolen credit card details on the internet. But they often do not know the CVV number (three-digit security code on the back of the card) and therefore have to brute force three-digit combinations until they are successful.	• Angry, scammed customers • Damage to the brand • Forensic investigations into the security breach
Credential Stuffing Attackers also use lists of compromised usernames and passwords on the internet. Once the attacker has successfully breached an account, anything of value (payment data, customer's personally identifiable information (PII), loyalty points, etc.) is used for resale on the dark web or to defraud the customers.	• Angry, scammed customers • Damage to the brand • Forensic investigations into the security breach
Scalping / Denial of inventory Resellers use Sneakerbots and Grinchbots to buy limited edition products and hoard as many items as possible that are in high demand. This locks out real customers and creates a secondary market where resellers can charge much higher prices than you can.	• Angry, frustrated customers • Possible brand damage due to "false claims" regarding your inventory
Creation of Fake accounts Bots are able to create fake accounts on any e-commerce website. These fake accounts are then often used in combination with fake credit cards to defraud people.	• Fake data in the CRM • Skewed reports • Damage to the brand when a cracked credit card is used
Gift Card Fraud Attackers use bots to brute force gift card codes. These codes are then either sold on the secondary market at a mere fraction of their value or used to obtain items fraudulently.	• Angry customers • Higher customer service costs • Damage to the brand
DDoS Attacks The goal of Distributed Denial of Service (DDoS) attacks is to overwhelm a server and take it down completely. For this purpose, the attackers use giant botnets and send request to your website millions of times per second.	• Loss of revenue, as real customer cannot purchase anything while your website is down • Damage to the brand

05 Impact of Bots on E-Commerce

In this white paper, we have shown you that the impact of bot traffic on e-commerce is growing every day and is also very multi-faceted.

You can not only suffer severe brand damage, but also make wrong business decisions, upset your loyal customers and lose a lot of money due to bots.

Ad fraud is by far the biggest financial impact on e-commerce, with over 40% of businesses losing between 3% and 10% of their revenue to automated bot attacks.

RECOMMENDATIONS

But how can you protect your e-commerce business from bot traffic? As there is no one-size-fits-all answer to this question, here are some tips:

- Block outdated user-agents
- Investigate your own analytics data and look for abnormal patterns
- Monitor for failed login attempts
- Pay attention to public data breaches
- Implement a fake traffic blocking solution

Protect your e-commerce website, and more importantly your advertising budget, from bot attacks today by signing up for a free 14-day trial at fraud0.com.

14 days free trial

fraud0.

How we can help

fraud0 helps businesses minimize risks associated with advertising fraud by analysing data discrepancies and behavioural anomalies combining real-time scoring, behavioural analytics, device fingerprinting, honeypots, browser challenges and further undisclosed techniques.

Discover how fraud0 can help your business eliminate fraud and increase sales and revenue.

Sign up for 14-day free trial