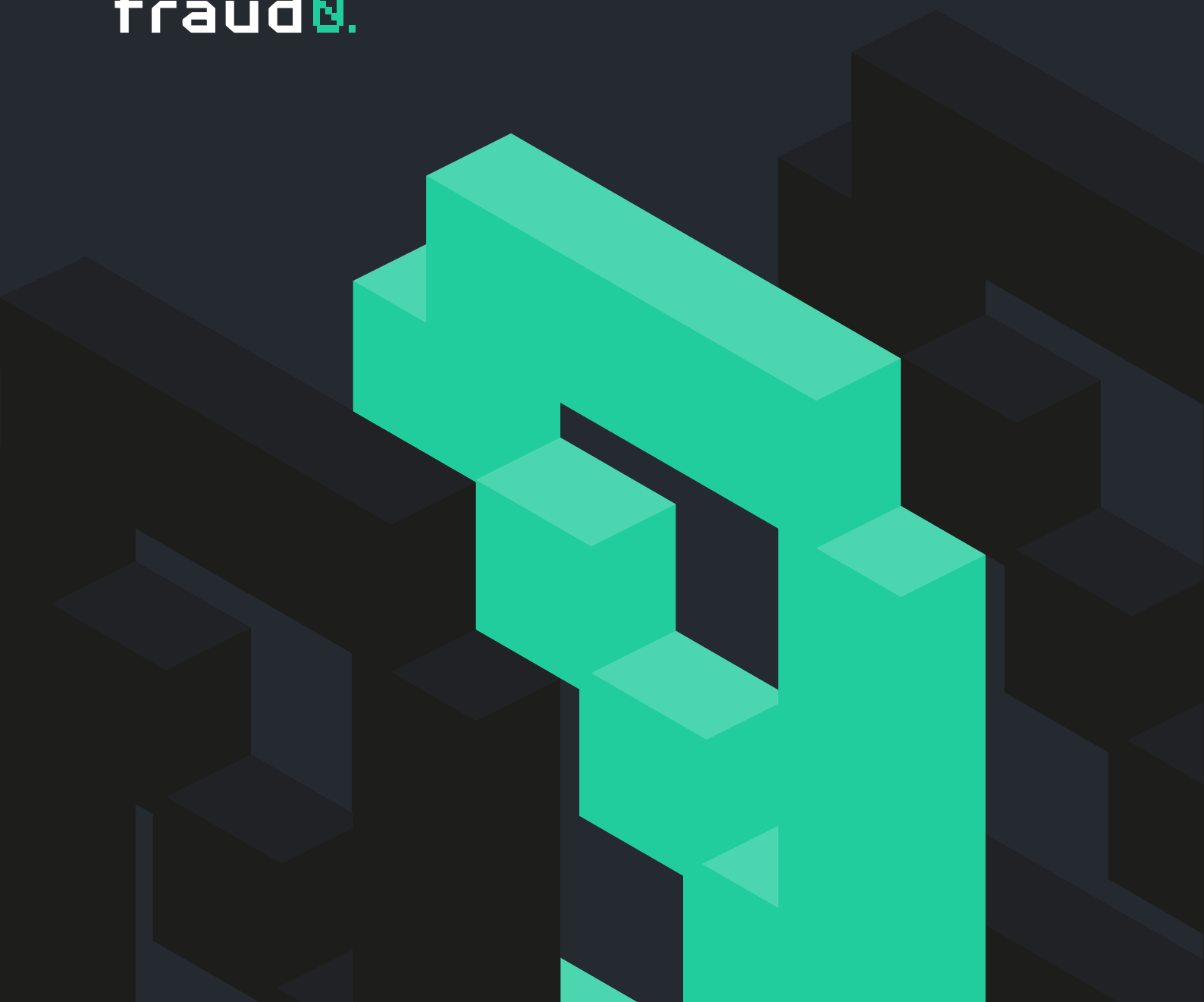
WHITEPAPER

Bot Attacks, Fraud & Fakes

The Impact of Bots on the End-Of-Year Business of E-commerce Companies

fraud0.



The Impact of Bots on the End-Of-Year Business of E-commerce Companies

Ahead of the upcoming Black Friday and Cyber Monday (BFCM), we've compiled insights on how e-commerce businesses are impacted by bots during the end-of-year shopping season and the challenges it poses.

In this whitepaper, our focus is on BFCM and the holiday season it kicks off as a peak time for fraudsters to maximize their revenue at the end of the year.

We highlight the specific challenges companies face from bots during BFCM, analyze the resulting impact, and outline approaches to counteract these threats.

Importance of Black Friday and Cyber Monday in E-commerce

Black Friday and Cyber Monday have advanced over time to become significant sales days not only in the USA but also in Germany. Between 2021 and 2022, we saw an impressive **22% growth in consumer spending in Germany**, with roughly **€5.7 billion in sales in 2022 alone.**[1]

€5.7 billion
of Black Friday & Cyber Monday sales in Germany, in 2022 alone.

In addition, these days herald the start of the Christmas shopping season. Research shows that **more than half of all consumers use these days to make cost-effective Christmas purchases, preferably online**. Thus, the BFCM days represent the peak for e-commerce, especially in segments such as electronics, fashion & accessories, leisure & hobbies, and home & furnishings.[2]

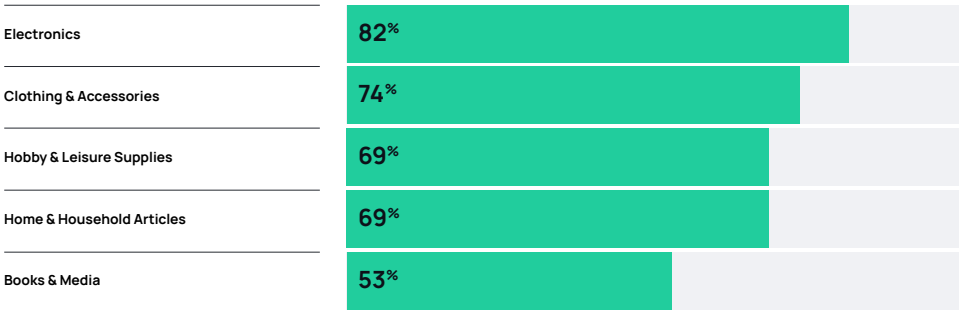
However, the growth of BFCM also brings significant changes for advertisers. Advertising costs experience significant jumps on these specific days:

- Increase of **76% in cost-per-mille (CPM)** for **meta ads**[3]
- Increase of **38% in CPM** for **banner ads**[4]
- Increase in ad spend for **Amazon Sponsored Products Ads by 58% - 79%**[5]

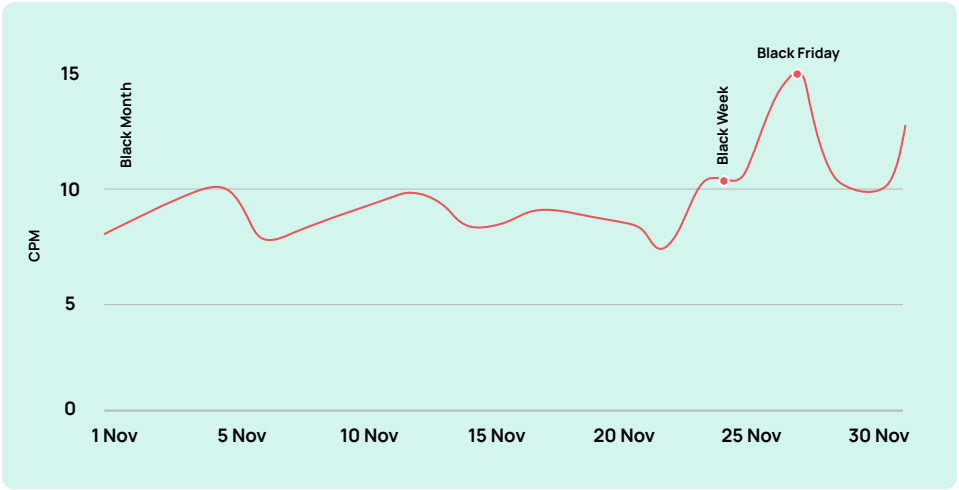
76% CPM
increased for **Meta Ads.**

But with the boom in e-commerce during this period, the darker side of the Internet also comes increasingly into play. Bot attacks increase during these sales days. The German Federal Office for Information Security (BSI) urges caution and warns in particular against bot attacks, including distributed denial of service (DDoS) attacks, during the BFCM and Christmas period.[6]

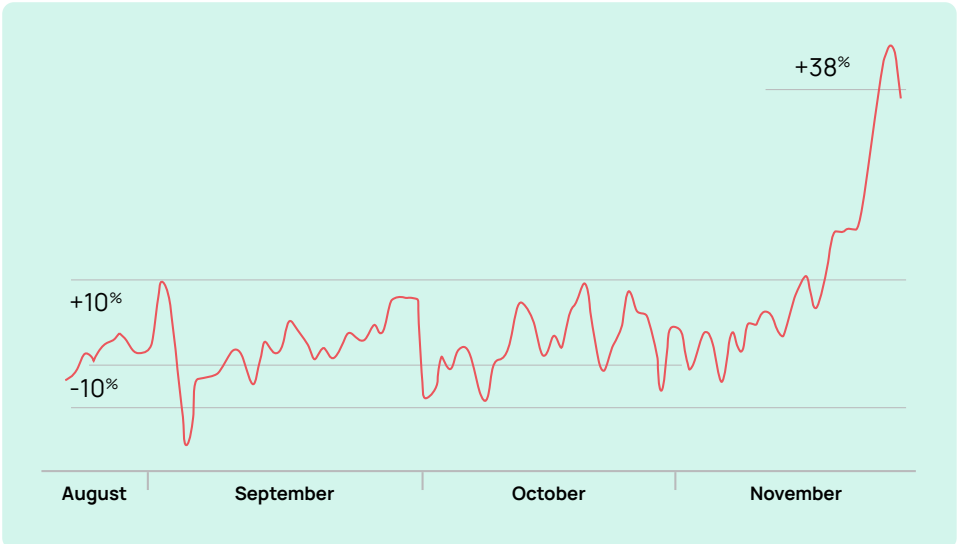
Most Popular Product Categories on Black Friday in Germany[2]



Increase CPM Meta Ads During BFCM[3]



Increase CPM Banner Advertising During BFCM[4]



Main Types of Bot Attacks During BFCM

As the year comes to a close, companies are expanding their resources on many fronts to meet increasing consumer demand:

- Increasing inventory levels or product availability
- Expanding server capacity to handle more website visits without technical issues
- Expanding customer service to handle a greater number of customer inquiries
- Increasing marketing and advertising activities to attract more customers

The tasks are numerous and distractions are high, which can lead to neglecting the issue of security during this time. As a result, cybercriminals see an ideal opportunity to strike through various bot attacks.

Such attacks can significantly reduce sales and customer confidence, highlighting the need to be aware of different threat scenarios, defenses, and prevention strategies. From intense DDoS attacks aimed at overloading websites, to disingenuous buying activities, to bots masquerading as authentic users to grab highly desired products before real buyers – **the spectrum of attacks is broad**.

Before we delve into these attacks in detail, we should look at the motivations and modus operandi of these bot attacks. With a more profound understanding of the methods used by the attackers, companies can prepare themselves more effectively and protect themselves and their customers more efficiently.

The Motivations Behind Bot Attacks

The period around BFCM is particularly lucrative for cybercriminals, as the increased volume of visitors and consumers' increased desire to buy offer optimal conditions for their schemes. In most cases, **the financial incentive is at the forefront of these bot attacks**, whether by gaining immediate access to customer data, purchasing and later reselling sought-after items, or sabotaging competitor websites to affect them financially.

1. **Financial benefit:** A large proportion of bot attacks aim to generate financial benefits, either directly or indirectly. Some bots are designed to secure items in large quantities and then offer them at a higher price. Others might aim to grab user information and sell it on the darknet or use it for fraudulent purposes.
2. **Market advantage:** In some cases, bot attacks are initiated by competing companies. The primary goal of such attacks is to impair the online performance of the rival and thereby redirect potential buyers to their own offering.
3. **Damage to image:** A successful assault on a company during intense buying periods can cause significant image problems and permanently damage consumer confidence.

The Most Common Bot Attacks

DDoS (Distributed Denial of Service)

DDoS attacks have been around for some time, yet they remain a constant priority cyber threat for businesses of all sizes.

How it works: In a DDoS attack, the cybercriminal uses a network of infected computers, commonly referred to as a "botnet", to perform a centralized assault on a specific website or web service. The main goal is to load the target server with a flood of requests so that it becomes overloaded and eventually fails.

Impact: DDoS attacks can cause significant financial damage to businesses, especially during high-traffic periods like BFCM. Even short downtimes can jeopardize potential business and permanently undermine customer confidence.

Scalping Bots

Recently, sniping bots have made a name for themselves, especially during big sales like BFCM. Their main purpose is to grab highly desired and often limited-availability items even before regular buyers can do so.

How it works: These automated programs are designed to react to sales offers with impressive speed. In fractions of a second, they can add an item to the shopping cart and complete the buying process, often faster than a human shopper can even review the product description.

Impact: The activity of such bots frequently leads to items in demand selling out within a very short time. This can annoy genuine buyers and damage the image of online sellers who fail to prevent such automated requests. In addition, resellers use these bots to offer items at inflated prices on the secondary market, allowing the fraudsters to make large profits, resulting in increased costs for the end consumer.

Credential Stuffing / Account Takeover

Reusing passwords across different platforms is a common mistake made by many users. This practice is deliberately exploited by cybercriminals to carry out malicious acts.

How it works: Criminals use automated programs to try out previously stolen or leaked credentials on various websites. If a set of credentials proves to be valid, the affected account is misused for fraudulent activities.

Impact: Successful credential stuffing can result in unauthorized transactions, data leaks, and a significant loss of trust. This highlights how bots use users' carelessness to their advantage.

Impression Fraud

In the digital advertising world, impressions are an important metric for measuring the visibility and reach of online ads. Unfortunately, there are also unethical methods used by fraudsters to manipulate systems in order to make undeserved profit.

How it works: Impression fraud can be done in several ways. In all cases, however, cybercriminals use bots to visit their own websites (so-called "MFA websites" (made for advertising / made for arbitrage)), thus artificially increasing the number of ad impressions and ultimately boosting their CPM revenues. Additionally, other forms of fraud such as ad stacking or pixel stuffing can be used to increase the number of embedded ad banners. Ad stacking involves placing multiple ads on top of each other in an ad space. Only the top ad is visible, but impressions are registered for all ads in the stack. Pixel stuffing refers to a tactic where fraudsters pack an ad into a tiny pixel (e.g. 1×1) so that it becomes invisible to users, but still generates impressions.

Impact: The financial impact of impression fraud is significant. Advertisers pay for ads that were never seen by real people. This not only leads to lost ad spend, but also skewed analysis data. Marketing teams can thus incorrectly assume that an ad is performing well when in fact its viewable reach is minimal. This can lead to misguided marketing strategies and budget allocations. Ultimately, impression fraud undermines trust in the digital advertising industry and leads to inefficient marketing spend.

Click Fraud

Although companies make significant efforts to attract customers through online ads, bots exist to undermine these marketing strategies.

How it works: Bots are programmed to systematically click on digital ads without any buying interest or actual curiosity for the advertised product. They are led to websites operated by fraudsters and simulate clicking on advertising banners on those sites. In the process, the fraudsters profit from the advertising revenue generated by the artificially generated clicks on their platforms.

Impact: These inauthentic clicks result in a loss of ad spend to non-human traffic while skewing data, preventing companies from determining the true effectiveness of their ad campaigns.

Fake Review Bots

In our connected society, customers increasingly rely on online reviews to make informed purchasing decisions. This has brought a rise in bots that aim to influence opinions through manipulated reviews.

How it works: These bots are designed to either leave praise for a particular product or present competing offerings in a bad light. They create accounts that resemble authentic users and then post reviews that often consist of pre-created blocks of text or are slight variations of real comments.

Impact: Such distorted reviews can significantly manipulate consumer buying behavior, as many make their choices based on online feedback. The result can be that products of inferior quality are purchased preferentially, or qualitatively superior items are avoided due to unjustified negative reviews.

Scraping Bots

While some bots cause immediate and obvious damage, scraping bots often operate discreetly in the background, extracting valuable information from websites.

How it works: These bots are designed to crawl websites and extract targeted data. In the context of BFCM, they mostly focus on product data and price information to gain a competitive advantage.

Impact: The collection of data by such bots can affect companies in many ways. Especially when competitors use this data, it can put the company at a disadvantage, for example by undercutting prices. In addition, the mass collection of data by bots can significantly increase web traffic, which can lead to increased hosting fees or even server overloads similar to a DDoS attack.

Impact of Bot Activity for Businesses During BFCM

Bot attacks are not just a digital nuisance. They have a direct impact on the sales, image, and credibility of companies in the digital market. They can also influence future business decisions by corrupting data.

It is critical to understand these consequences, both to capture the direct financial losses and to recognize the deeper implications for brands and their customer loyalty.

Bots Eat up the Ad Budget

During BFCM, many companies significantly increase their advertising investments to achieve maximum customer engagement. However, if a significant portion of these impressions and clicks are generated by bots, these additional advertising dollars go to waste. This means the company pays for impressions and clicks that never result in real sales.

Remarketing Budget Goes to Bots

It is not only during BFCM that companies waste considerable advertising resources on bots. These bots can now not only click on and view ads, but also accept and store cookies. In this way, they manage to permanently embed themselves in remarketing lists.

Incorrect Data Influences Business Decisions

Bots are often programmed to perform human-like activities. This includes browsing pages, clicking links, filling out forms, and even adding products to the shopping cart. Analysis tools, such as Google Analytics, often capture these bot activities as real user interactions.

During the BFCM, various effects of bots on online stores become apparent:

1. **Misleading traffic evaluation:** An unexpected increase in visitors could be falsely evaluated as the result of a successful promotion when in fact bots are causing the traffic.

2. **Misinterpretation of user behavior:** Because bots mimic human browsing behavior, retailers may incorrectly conclude that certain products or web pages are particularly popular, even though bots are behind most of the actions.

3. **Misallocation of advertising funds:** Due to the data distorted by bots, companies could invest in non-targeted advertising initiatives that focus on supposedly "in-demand" products, target groups and/or channels.

4. **Increasing bounce rates:** Bots tend to leave websites quickly, which increases the bounce rate. A high value could unfairly alarm companies and indicate that the website is not attractive to visitors.

5. **Distorted conversion metrics:** Bots can go through the buying process without completing a purchase, which lowers the conversion rate. A low conversion rate could be wrongly interpreted as a problem with the website or offer.

Overall, the data distorted by bots can lead to incorrect or misguided business decisions. This can have significant financial and strategic consequences, especially in high-revenue periods like BFCM.

About fraud0.

Our software not only helps companies detect automated bot activity, but also ensures the integrity of digital marketing efforts. Learn more about the benefits fraud0 offers your business below.

Cleaned Analysis Data

As a security software, fraud0 can be loaded without the prior consent of your visitors while remaining GDPR-compliant. This gives us data on 100% of your traffic, whereas other analytics tools can only measure a fraction of it due to a consent requirement. Additionally, through our Usercentrics integration, you also get insights into the bot-cleaned statistics of your Consent Management Platform (CMP).

In our Analytics Suite, you get detailed information about your traffic and can thus make data-driven decisions based on a valid data foundation.

Better (Online) Marketing

fraud0 helps you identify bots in real time using more than 2,000 data points. Detected bots are automatically excluded via IP address on all your channels (e.g. Google Ads, Facebook, TikTok etc.) and with the help of Negative Audience Lists from further retargeting. Additionally, you can ensure that your pixels are only fired at validated human users, keeping your marketing audience clean.

In our Analytics Suite, you get detailed information about the traffic of your different channels and, based on your own metrics, you can allocate ad budget more efficiently and effectively, optimizing your channel mix.

Clean Sales Funnel

Protect all your forms from bots and flag fake leads. With our real-time bot detection, you can prevent bot data from nesting in your CRM. This saves your sales teams valuable time and allows them to focus on real, human leads in the future.

At the same time, you can ensure that no real user data ends up in your systems unintentionally through bots. In numerous instances, bots use real people's data, which has made it into the darknet through various data leaks in the past. This can pose a high data protection risk for companies.

Test fraud0 for 7 Days Without Any Obligation

Convince yourself of our results and test fraud0 for 7 days free of charge and **without obligation.**

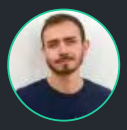
Test now for free

Happy Customers

"Great software. And interesting to see what a single line of code reveals about the traffic quality on our sites!"

Saif Jarad
Founder & CEO at Chain Reaction
CHAIN REACTION

"Eye opening! Our paid campaigns were hit by 19% of fake traffic. fraud0 gives us back control. Great software."



Felix Koleber
Co-Founder & CEO at Levia Blanket
LEVIA

"Single line of code on our website gives us visibility on how much fake traffic we are buying. Transparency and efficiency with fraud0 rocks!"

Lena Heil
Senior Digital Marketing Manager at Merz Aesthetics
MERZ AESTHETICS

List of Sources

1 Handelsverband Deutschland (HDE) - Black Friday und Cyber Monday

2 Idealo - Black Friday Umfrage 2023

3 Confect.io - Why lead generation is smart during Black Month

4 AdLibertas - CPM Swell: Black Friday & Cyber Monday

5 Perpetua.io - How to Prepare Your Black Friday Cyber Monday Marketing Strategy 2022

6 Bundesamt für Sicherheit in der Informationstechnik (BSI) - Die Lage der IT-Sicherheit in Deutschland 2022

fraud0.

Bot Attacks, Fraud & Fakes