Unmasking the shadows

Invalid traffic 2024

fraud0.

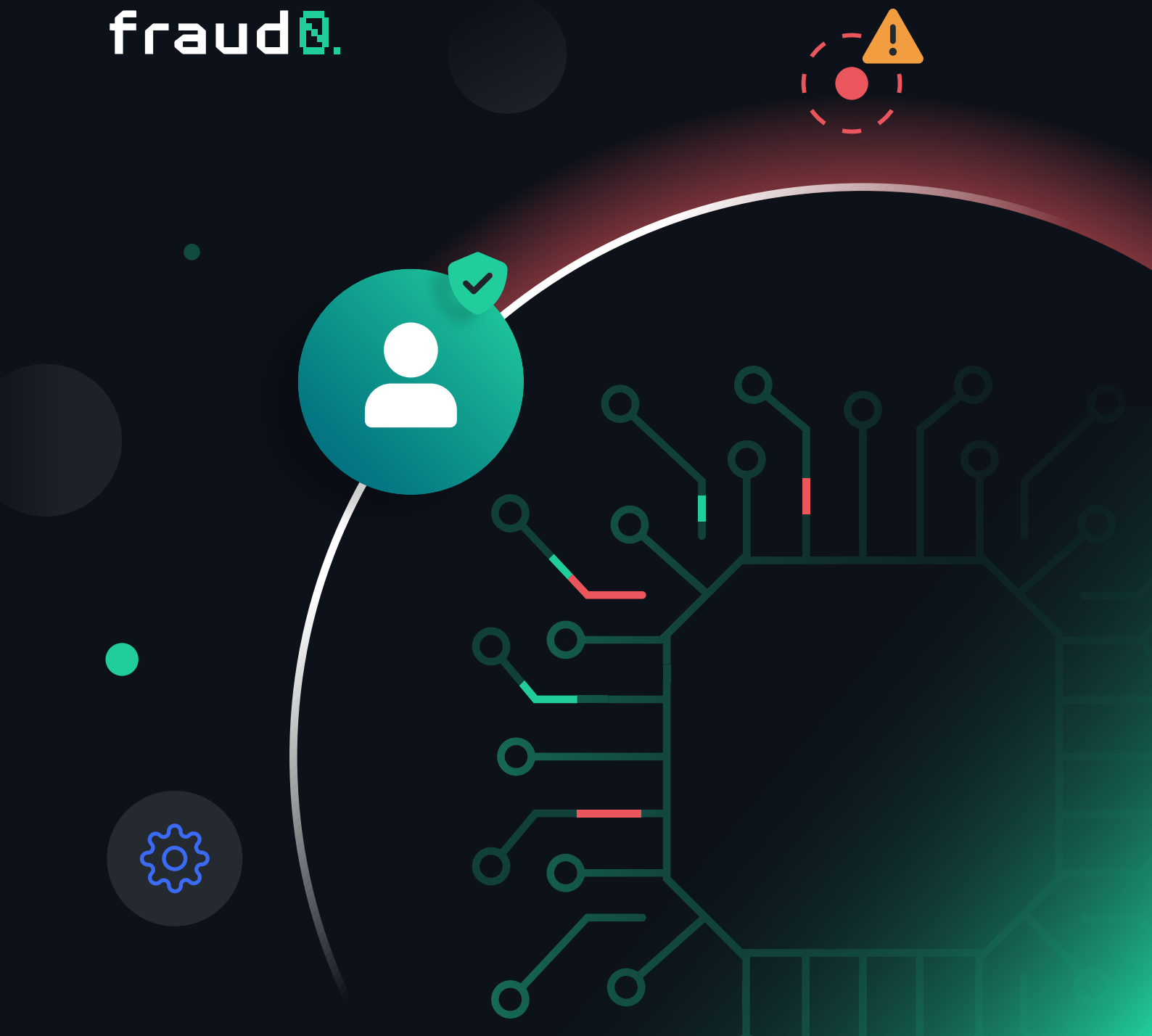


Table of contents

Mar 27, 2023

"Given that modern AI can solve any 'prove you're not a robot' tests, it's now trivial to spin up 100k human-like bots for less than a penny per account."

— Elon Musk

"Digital fraud is literally the bad guys' ATM machine – they just withdraw cash. Every year $600 billion more of marketers' digital budget refills it."

Dr. Augustine Fou —

Leading cybersecurity and ad fraud researcher & fraud0 advisor

2.0

Introduction

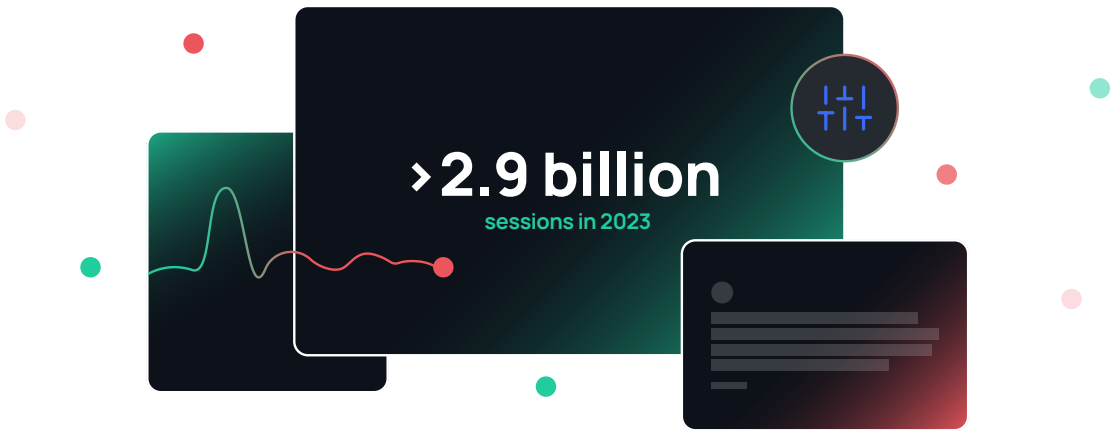
Digital transformation has revolutionized the business world, enabling companies to leverage AI for growth and efficiency. However, this also creates new challenges and risks, especially in the realm of digital advertising. One of the most pervasive and persistent threats is invalid traffic, which refers to any clicks or impressions that are not generated by genuine human users.

This report provides a comprehensive overview of the invalid traffic and bot landscape across various industries. It will examine the causes, types, and effects of invalid traffic, as well as the best practices and solutions for detecting it. By doing so, this report will equip readers with the knowledge and tools to effectively manage and mitigate the risks of invalid traffic.

fraud0's AI-powered algorithm analyzes millions of requests, data points, and behavioral patterns every day in real-time providing actionable information about the traffic. For this report, we took this data from our largest **100+ customers** and analyzed a total of over **2.9 billion sessions in 2023**. It is important to note that we have excluded crawlers, such as the Google Search Engine Crawler, from the invalid traffic data in order to obtain more meaningful results.

What is invalid traffic?

Invalid traffic (IVT) refers to any user or website visitor with no intention or capability to convert into a paying customer. This includes a range of activities including, but not limited to, bot-based traffic, manipulative page refreshes, and deliberately misleading users.



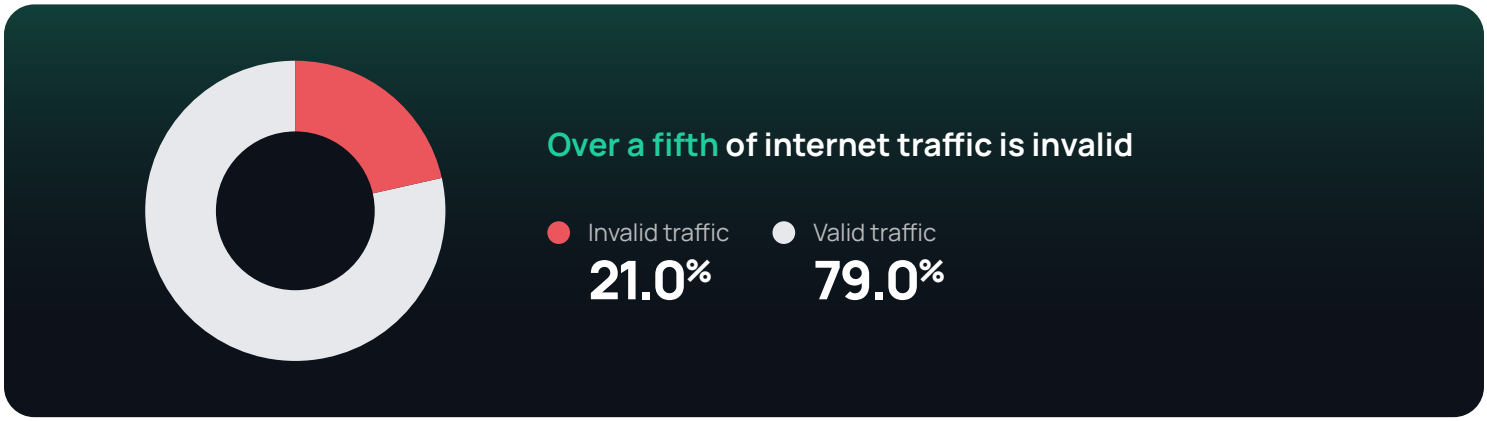
General findings

Chapter 2

Over a fifth of internet traffic is invalid

We analyzed a sample of more than **2.9 billion sessions** from fraud0 customers in 2023 (January 2023 - December 2023).

Here are our findings:



Or to put it another way, **1 out of 5 website visits** is not a real person, but an automated program (bot) with no intention or capability to convert into a paying customer.

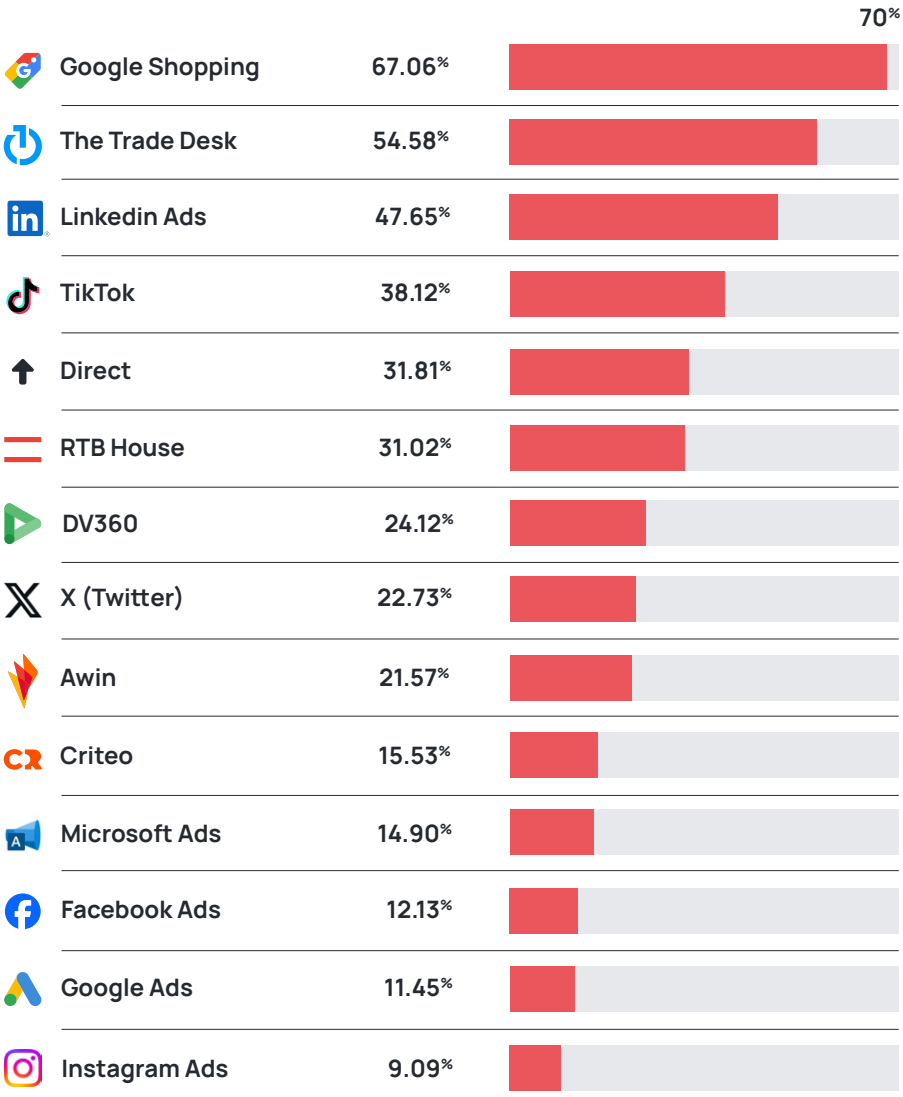
These findings are derived when measuring directly on the domain. During assessments of "in-ad" engagements through programmatic channels, we observe a much higher incidence of bot traffic, often exceeding 90% alongside other fraudulent activities such as pixel stuffing. These sites are entirely fraudulent with no humans even knowing that they exist.

For more details please visit **FouAnalytics Practitioners**.

Certain channels are significantly more affected than others

Invalid traffic is a major threat across all digital marketing channels – no channel is exempt. Its uncontrolled presence means wasted ad budgets and has negative consequences such as ineffective campaigns, skewed analysis, and misleading attribution.

Invalid traffic by channel



Invalid traffic by channel (grouped)

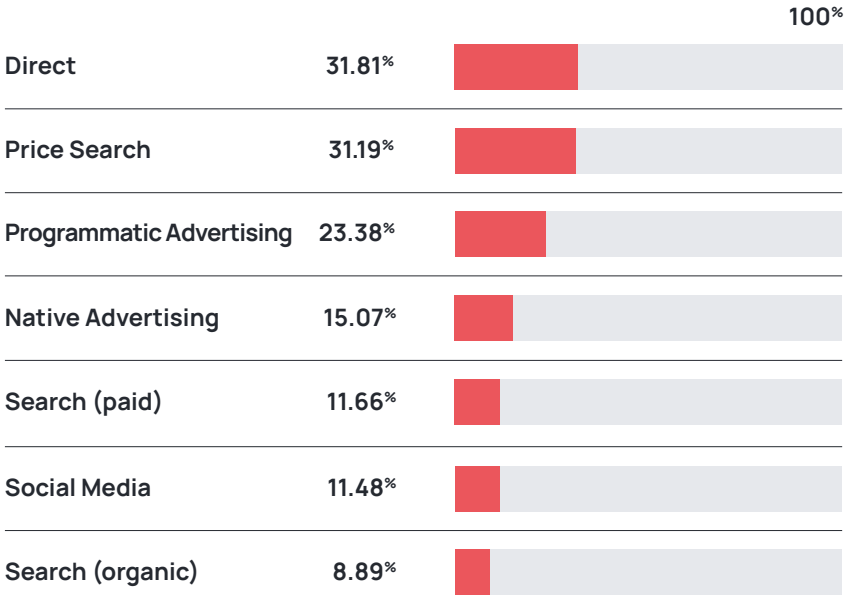


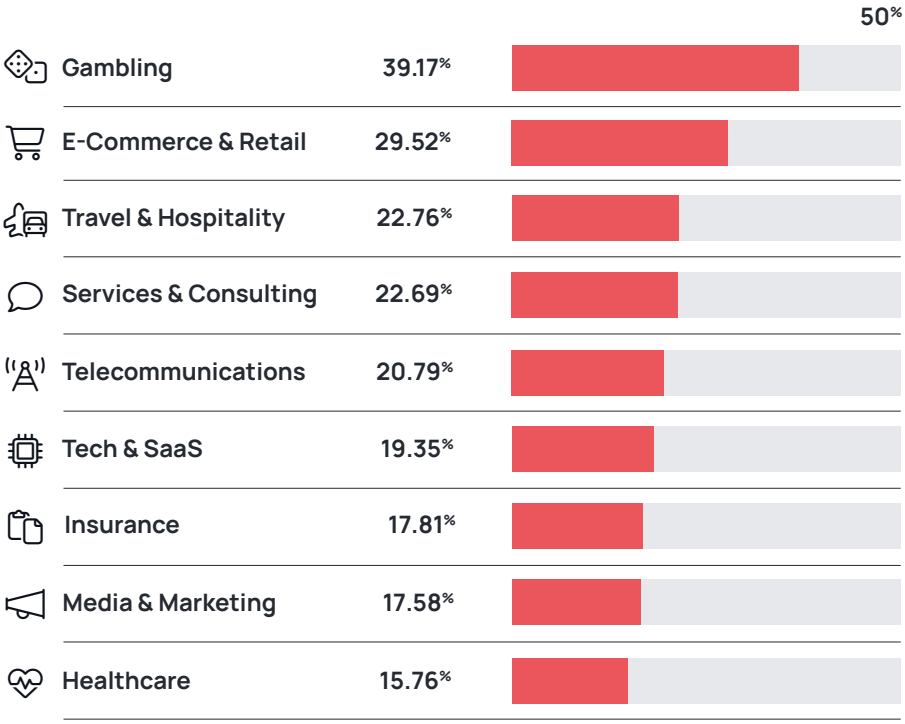
Chart information

To give you a better overview of the individual channel categories, we have grouped them for you.

Significant discrepancies can also be seen between industries

The issue of invalid traffic and bots naturally affects every industry. But there are some significant differences in terms of the extent. For this report, we have clustered our customers into the categories listed below.

Invalid traffic by industry



Bots are also included in your consent data

Nowadays, bots are imitating humans to such a degree that they are also programmed to give consent on websites.

Consequently, they also appear in the CMP statistics. In cooperation with **Usercentrics**, bots can be flagged in this data and provide precise insights.

usercentrics

Invalid traffic in CMP data

10.55%

Most traffic pretends to come from Germany

The majority of invalid traffic originates from Germany. However, this does not necessarily mean that the persons are also physically located in Germany. Cybercriminals often use data centers or proxy servers to organize bot attacks, so the analysis of web traffic in different countries is likely to reflect proxy locations rather than the actual locations of the attackers.

The result is not surprising, as the majority of companies in this evaluation come from Germany. Attackers also benefit from lower latency when they choose proxies that are closer to their targets – a key advantage when conducting high-volume attacks.

1st **Germany**

2nd **U.S.A.**

3rd **Singapore**

Invalid traffic by originating country

Germany	63.83%
USA	11.26%
Singapore	6.21%
Austria	3.12%
France	2.41%
Other	13.17%

No detectable preference among the devices

Using a method called device spoofing, fraudsters can make traffic from data centers look like it's coming from real devices belonging to real people. It is reasonably expected that attackers predominantly mask their traffic to try to avoid detection.

Invalid traffic by device type

Desktop	Smartphone	Other
29.12%	32.03%	38.85%

Device spoofing is a cybercrime technique that involves changing the identity of a device to imitate another device or user.

They manipulate a device's unique identifiers, such as the MAC address, the IP address, the GPS location, the user-agent string, the caller ID, and the technical device details. Fraudsters use device spoofing to trick systems, networks, and devices into believing that their device is authentic and trustworthy.

When it comes to the distribution of operating systems, cybercriminals follow the market. Both Windows and Android are market leaders (>70% in desktop and mobile) and are therefore more often abused for invalid traffic in order to get buried in the crowd and not attract attention in the corresponding analyses and security systems.

However, we also see a large proportion of invalid traffic that disguises its device type so that it cannot be clearly categorized.

Invalid traffic by OS

Android	48.88%
Windows	12.26%
macOS	9.96%
Linux	9.17%
iOS	1.96%
Other	17.76%

Industry deep dive

Chapter 3

Travel & Hospitality

As digital transformation continues to redefine the travel and hospitality industry, bots have emerged as both facilitators and disruptors. These automated programs can handle everything from customer service inquiries to online check-ins, offering efficiency and convenience. However, their capabilities can also be maliciously employed to exploit vulnerabilities, causing significant operational and financial challenges.

Over a fifth of traffic
in the Travel & Hospitality industry is invalid

Invalid traffic
22.76%

Top bot attacks

Scraping

Bots are used in the travel and hospitality industry to scrape price and availability information from websites, such as those of hotels, airlines, and travel agencies. For the travel and hospitality sector, where pricing is a significant differentiator, the unchecked activity of price-scraping bots can have detrimental effects on profitability and brand integrity. Rival companies, price collectors, and metasearch platforms are using this scraped data to undercut prices or manipulate their pricing strategies. This can lead to a loss of revenue due to artificially lowered prices or price wars. Furthermore, constant undercutting or perceived price volatility can undermine a brand's value and reputation.

Inventory hoarding

Fake reservations on travel and hotel websites block inventory until it is sold out without the intention to buy anything. Bots are repeatedly reserving seats on flights or rooms in hotels. In the worst-case scenario, this can result in an airplane or a hotel not filling its capacity, even though there would have been enough demand. Inventory hoarding can thus have a direct negative impact on business and customer satisfaction, as it can lead to a loss of revenue, reputation, and trust.

Credential stuffing / account takeover

Cybercriminals employ bots to gain unauthorized access to customer accounts by automating login attempts using stolen or easily guessed passwords. Airlines suffer from these problems, as malicious bots try to enter users' accounts and steal the accumulated air miles. The same applies to hotels or booking portals that offer a reward point system. In addition, the real customer information can be used for fake reservations but is hardly or not at all recognizable for the respective companies.

Polluted analytics & audiences

Invalid traffic ends up in the analysis tools and pollutes your performance data, analytics and KPIs, giving you a false impression such as the Look-to-book ratio. This data is then used to make marketing decisions or to optimize conversion. However, it does not usually lead to an uplift in performance, as the data and the focus are not on real people.

Furthermore, if bots are included when your audiences are created, your campaigns will continue to be increasingly served to bots. Therefore, it is important to clean your data and make decisions based on it.

DDoS attacks

DDoS (Distributed Denial of Service) attacks aim to disrupt the normal functioning of a web service by overwhelming it with a large number of requests from multiple sources. In the case of the travel and hospitality industry, the attack can prevent customers from entering the website or significantly increase loading times, causing customers to close the page.

This leads to a loss in sales, as bookings are not made. But also because customers first look at competitors the next time they search due to a damaged reputation.

E-Commerce & Retail

E-commerce platforms are exposed to significant risks from invalid traffic, in this case bots. These platforms offer multiple opportunities for attacks. They hold a lot of customer data, including personal information, contact details, and payment data, and at the same time, they serve ads, making them a sitting duck for ad fraud. In addition, they have valuable product information such as description texts and price information, which is highly favored by scraper bots.

Almost one-third of traffic
in the E-Commerce & Retail industry is invalid

Invalid traffic
29.52%

Top bot attacks

Scalping

Scalper bots are designed to buy or reserve limited availability goods, highly desirable goods, or digital goods, usually within seconds of their release. Event tickets, sneakers, or tech products like the PlayStation 5 are particularly affected.

Fraudsters use these bots to secure their inventory and at the same time create an artificial demand that drives up prices on the secondary market, where they subsequently resell the goods at a multiple of the original price.

Inventory hoarding

Bots are adding high-demand products to the shopping cart without completing the purchase. Many businesses provide the opportunity to reserve the shopping cart for a certain period of time. After this time, the bots repeat their approach.

This creates a false stockout and prevents real customers from buying the products. Ultimately, this leads to customers buying from another company.

Wasted ad spend

Ad fraud in the context of e-commerce refers to the deliberate manipulation or fraudulent activities conducted to deceive advertising platforms, advertisers, or metrics systems. The goal is to generate revenue through fake clicks or impressions.

AI is a real game changer here for fraudsters. It can create a so-called "Made for Advertising" (MFA) site in just seconds. Through methods like domain spoofing, the fraudster manages to get companies to place ads on their site. Finally, fake traffic is bought and directed to the page to imitate real impressions and clicks on the ad.

Scraping

Scraper bots are automated programs designed to systematically scrape or harvest data from websites. While scraping can have legitimate uses, these bots are often employed for dubious activities.

In the case of the e-commerce & retail industry, the bots scrape price information to undercut prices and gain a competitive advantage or steal content to create fake stores.

Polluted analytics & audiences

Invalid traffic skews your performance data, analytics, and KPIs, giving you a false impression of your campaigns and performance. Nowadays, bots can already give consent, which means that your CMP data is also polluted. Data-based decisions are essential, but bad decisions are made with polluted data.

Domain spoofing is a widespread technique used by fraudsters to siphon off ad budgets. Inferior websites are created that pretend to be well-known websites. They are often an exact copy of these websites or are simply created by AI.

The approach sounds simple and effective, and it is. Advertisers pay for this supposed premium traffic but never see a conversion or the hoped-for branding effects.

Gambling

The gambling industry is a lucrative market that is constantly under attack by malicious bots. From online casinos to sports betting, the data generated by gambling activities is both profitable and risky. Fraudsters also exploit new customer bonuses and incentives with the help of bots. Bots pose a serious challenge to this industry.

Over one-third of the traffic
in Gambling is invalid

Invalid traffic
39.17%

Top bot attacks

Fake account creation

Bots are becoming more adept at mimicking human actions online. This enables them to create fake accounts with ease. They do this to take advantage of incentives or promotions offered by gambling sites. This results in significant monetary losses for the gambling industry.

In addition, cybercriminals use gambling websites and apps to launder money. These activities naturally also lead to increasing displeasure among genuine customers.

Polluted analytics & audiences

Bots can distort gaming companies' analytics and audiences by generating false or invalid traffic, clicks, or conversions. This can affect the data and insights that gambling companies use to improve their marketing campaigns, products, and services. It can also increase the costs and reduce the profits of their online advertising activities.

Websites where you can easily buy bot traffic within seconds, even advertise that this traffic ends up in analysis tools such as Google Analytics.

Wasted ad spend

Ad fraud is a major problem for gambling companies, especially in the programmatic space. This is when unscrupulous actors use various techniques to trick these companies into believing that a human has seen and clicked on their ad, rather than the bot performing these actions.

AI makes it even easier for fraudsters to create so-called MFA pages, for example. At the same time, the quality of these pages is improving. Using various fraud techniques such as domain spoofing, ad stacking, or pixel stuffing, fraudsters siphon off advertising budgets through fake impressions and clicks.

Credential stuffing / account takeover

Cybercriminals use bots to break into customer accounts by automating login attempts using compromised or predictable passwords. Gambling companies face these problems, as malicious bots attempt to access users' accounts and take the existing balance.

Stealing customer information

Bots can execute an attack to steal customer data from websites, apps, or APIs. This is especially relevant in the gambling industry, as they often hold a lot of confidential customer data and documents. Often, identification documents must also be provided for verification purposes.

Taking this customer information can damage trust and reputation, as well as cause legal and financial problems.

Ad stacking is the process of placing multiple ads on top of each other in a single ad placement.

While only the top ad is visible to the user, a click or impression is registered for each ad in the stack. This results in advertisers having to pay for fake impressions and/or clicks.

Insurance

The insurance sector is an important area increasingly confronted with bot attacks. The data stored in insurance systems - from customer profiles to claims histories - is both personal and profitable. As a result, bots represent a wide-ranging risk for this sector.

Nearly one fifth of the traffic
in the Insurance industry is invalid

Invalid traffic
17.81%

Top bot attacks

Insurance claims fraud

Bots can file fake or exaggerated insurance claims by pretending to be real customers and using false or stolen identities. They can claim for injuries, illnesses, or material damages that they did not suffer, did not take place, or were not insured. This causes monetary and operational complications for the insurance companies.

Form spam & fake leads

Bots can fill out web forms effortlessly, such as contact or lead gen forms. These bogus forms are hard to spot, as bots use genuine information from data leaks, for instance.

This poses major compliance risks for insurance companies. They must therefore immediately recognize whether a human or bot has filled out the form.

Polluted analytics & audiences

Bots can pollute the analytics and audiences of insurance companies by generating fake or irrelevant traffic, clicks, or conversions. This can skew the data and insights that insurance companies rely on to optimize their marketing campaigns, products, and services. It can also inflate the costs and lower the returns of their online advertising efforts.

Wasted ad spend

Ad fraud is a serious problem for insurance companies, especially in the programmatic space. This is when dishonest actors use various methods to trick those companies into believing humans viewed and clicked on their ad instead of the bot that is performing these actions.

AI acts as an accelerator here. It is becoming easier and easier to create so-called MFA pages. The quality of these pages increases at the same time. Using various fraud methods such as domain spoofing, ad stacking, or pixel stuffing, fraudsters siphon off advertising budgets through false impressions and clicks.

DDoS attacks

DDoS attacks in the insurance industry can have serious consequences. By overloading insurers' digital systems with excessive traffic, DDoS attacks can disrupt critical services.

These disruptions can delay the processing of customer concerns and claims settlements and undermine trust in insurance companies.

Pixel stuffing is a way of putting many ads on a single page without the customers realizing it.

Ads are loaded into small frames of one or just a few pixels in size. The visitor cannot see the ads, but the advertiser is charged for the view.

Telecommunications

As telecom companies increasingly depend on digital platforms for customer engagement, service delivery, and network management, understanding the complex role of bots and invalid traffic is critical.

Over a fifth of traffic
in Telecommunications is invalid

Invalid traffic
20.79%

Top bot attacks

Wasted ad spend

In telecommunications, ad spend is wasted through ad fraud. Programmatic advertising is strongly affected by intentional or dishonest actions that trick advertising platforms, advertisers, or metrics systems. The purpose is to make money from false clicks or impressions.

Fraudsters rely on the increasing possibilities of AI. Within seconds they can build a completely new MFA website. In the past, you could recognize them directly by their contents. The AI is now so good that the texts and images are no longer inferior to those of a legitimate website. These websites are then also delivered by advertisers through domain spoofing leading to impression and click fraud.

Fake account creation

Nowadays, bots can imitate human behavior very well. This also makes it easy to create fake accounts. They intend to sign up for free trials, incentives, or promotions, and also get access to the product or service without paying. This leads to potential financial losses for the telecommunication companies.

As the number of bots and inquiries increases, companies face further challenges. Bots can overload telecommunication websites or apps with too much traffic and requests, using up bandwidth, server resources, and cloud costs, making web services slower and less available.

Wasted tool spend

Telecommunications companies usually have several onsite tools for different purposes. These charge according to the number of sessions where they are loaded. This also happens when invalid traffic comes to the website.

Bots therefore lead to direct costs for these onsite tools, if they are not prevented from loading.

Polluted analytics & audiences

Bot creators even advertise that their traffic also appears in tools like Google Analytics. It pollutes their data and is giving you a false impression of relevant onsite KPIs. This can create the perception that some plans or offers are more interesting than they actually are for real people.

Credential stuffing / account takeover

These types of cyberattacks that use stolen or leaked usernames and passwords to access the online accounts of other users. Bots are automated programs that can perform these attacks at a large scale and speed, trying to find valid credentials for various websites or applications. In the telecommunication industry, it exploits the valuable data and services that these accounts provide.

In addition to direct financial costs, companies could also face legal consequences as a result of disregarding data protection.

Tech & SaaS

The tech and SaaS industry, known for its rapid innovation and digital approach, is not immune to the complex challenges posed by invalid traffic associated with bots. These can lead to a variety of security concerns, including unauthorized data access, fraudulent activity, and service disruption. Given the industry's heavy reliance on digital platforms and data-driven services, understanding the operational impact of bots is critical.

Nearly 20% of traffic
in Tech & SaaS is invalid

Invalid traffic
19.35%

Top bot attacks

DDoS attacks

DDoS attacks aim to interfere with the regular operation of a web service by flooding it with a large number of requests from various sources. In the case of the tech and SaaS industry, the attack can prevent customers from accessing the website or SaaS tool, or significantly increase load times so that customers cannot use the service.

This leads to negative customer experiences and can also have financial consequences for customers.

API abuse

Tech and SaaS companies usually work with different API interfaces. Bots can exploit vulnerabilities in APIs to either steal data or disrupt the service, impacting both performance and security.

Consequently, security vulnerabilities from other companies can also pose a threat to you if they are connected via an API.

Review & rating manipulation

Tech and SaaS companies are in direct competition with their competitors' solutions. Online ratings and reviews are often the deciding factor when choosing a solution. Fraudsters can use bots to place false and bad reviews on popular portals and thus directly influence a company's business.

Polluted analytics & audiences

Tech and SaaS companies are very data-driven due to their nature. However, invalid traffic settles in precisely this data. This means decisions are made on polluted data. Therefore, it is extremely important for companies to extract the bot-generated data.

Consequently, this also influences the marketing of tech and SaaS companies. If bots are still in the data that is used for target group creation, then the ads will increasingly be played out to bots again.

Form spam & fake leads

Nowadays, bots can easily fill out web forms, e.g. contact or lead gen forms. These fake forms can no longer be recognized quickly, as bots use real information from data breaches, for example.

These fake leads in the CRM result in headaches for the sales team. It is hard for them to distinguish genuine buyers from the rest. Moreover, the bots can repeatedly exploit free trials to use the service without paying or to spy on the product with its functionalities.

Healthcare

The healthcare sector is a critical area that is becoming increasingly susceptible to bot attacks. From patient records to pharmaceutical research, the data held within healthcare systems is both sensitive and valuable. Bots pose a multi-layered threat to this sector.

Over 15% of traffic
in Healthcare is invalid

Invalid traffic
15.76%

Top bot attacks

DDoS attacks

DDoS attacks in the healthcare sector can have dire consequences. By overwhelming healthcare digital systems with excessive traffic, DDoS attacks can disrupt critical services, including patient records access, medical equipment functionality, and telehealth platforms.

These disruptions can delay patient care, compromise patient safety, and erode trust in healthcare institutions. Given the vital nature of healthcare services, any downtime can lead to life-threatening situations, making it imperative for the sector to prioritize robust cyber defenses.

Data breaches

Criminals can use a cyber attack to infiltrate healthcare systems and steal patient information, medical records, and personal data. This highly sensitive data is of great value to criminals. They can be sold on the black market or used for identity theft.

In addition, the company may face legal consequences and financial fines following a data breach.

Appointment spam

Nowadays, more and more medical offices and other service providers are using online booking systems for appointments. Bots can flood appointment scheduling systems with fake appointments, causing confusion and disruption in patient scheduling.

In addition to unsatisfied patients, this also leads to a loss of revenue, as many appointments remain unused, and therefore no revenue is generated.

Insurance claims fraud

Bots can automate the submission of fraudulent insurance claims. They can impersonate real customers and use stolen or fake identities to file claims for injuries or illnesses that never occurred or were not covered by the policy.

This leads to financial losses and operational complications for the insurance companies.

Phishing

Bots can pose as trustworthy sources or officials and send fake emails or messages to healthcare workers or clients. This can lure them into opening harmful links or files, or sharing sensitive or monetary data.

If fraudsters gain access to the system, they can carry out malicious attacks with severe consequences, as explained in previous sections.

Services & Consulting

In an increasingly digital world, the services and consulting sector has witnessed a rapid transformation in the way it operates and delivers value to its clients. With a growing reliance on online platforms and data-driven insights, this sector has become more efficient, accessible, and dynamic. However, along with these advancements comes the challenge of dealing with malicious bots that can disrupt operations, compromise data security, and erode client trust.

Over a fifth of traffic
in the Service & Consulting industry is invalid

Invalid traffic
22.69%

Top bot attacks

Scraping

Bots target services and consulting firms to scrape and steal sensitive data, proprietary information, and intellectual property from their websites. This can include price information, product and service features, or business strategies. The fraudsters use this information to gain an unfair advantage over their competitors or damage their reputation.

Stealing customer information

Bots can be programmed to perform an attack to steal customer data from websites, apps, or APIs. This is particularly important in the services and consulting industry, as they usually have access to a large amount of sensitive customer data and documents.

Stealing customer information not only leads to a loss of trust and reputation but can also have legal and financial consequences.

Review & rating manipulation

Fraudsters can program bots to post fake or negative reviews and ratings about consulting firms on various platforms. This can harm the services and consulting industry in several ways.

They can mislead customers, investors, or partners, influence demand, supply, and pricing, and create unfair disadvantages for certain services or consultants. To prevent this, a reliable and effective review and rating system is needed.

Form spam & fake leads

Bots flood web forms, such as contact or lead gen forms, with spam content, causing disruptions and data integrity issues. This also applies to your lead gen campaign leading to wasted ad budgets.

A few years ago some of these leads were so obviously fake you could just look at the street address or the name and see which ones were made up. But these days it's not so easy anymore because of some very large data breaches that occurred in the past and bad guys now have data from real people. So they are using entirely accurate information. The result: fake leads in your CRM that cause headaches for your sales team.

Polluted analytics & audiences

Your performance data, analytics, and KPIs are distorted by invalid traffic, which makes you misjudge your campaigns and performance. Bots can now consent, so your CMP data is also contaminated. You need data-based decisions, but polluted data leads to poor decisions.

Media & Marketing

In the rapidly evolving landscape of media and marketing services, the presence of invalid traffic and bots has become a critical concern for both providers and consumers. From infiltrating user accounts to manipulating viewer metrics and even scraping valuable content, bots have the potential to disrupt the media and marketing sector in numerous ways.

Nearly a fifth of traffic
in Media & Marketing is invalid

Invalid traffic
17.58%

Top bot attacks

Scraping

In the media and marketing industry, bots are used to scrape and duplicate copyrighted or proprietary media content. This can involve documents, texts, or videos. The fraudsters then pass the content off as their own and try to make a profit with it. They either use the content to gain attention or reach themselves or pretend to be someone else to defraud other users.

For the original creator, intellectual property theft leads not only to a loss of image but also to possible financial losses.

View fraud

View fraud is a deceptive practice in which bots artificially inflate view counts on media and streaming platforms. This nefarious tactic is often used to mislead advertisers, content creators, and users by making it appear that their content is far more popular or engaging than it actually is. On the other hand, bots are also used to generate more advertising revenue by increasing the number of views on a given video or stream.

Fake engagement

Bots artificially like, share, or comment on media and streaming content to create a false sense of popularity or sentiment. This issue is universal across platforms.

Furthermore, bots flood the comment sections with spam, creating a poor user experience and potentially distributing malicious links. The fraudsters then use these links to try to obtain sensitive data or gain a monetary benefit directly.

Credential stuffing / account takeover

Bots are programmed in such a way that they use real information that has been exposed in a data breach (email addresses, names, passwords, etc.) to log into other people's accounts.

When they gain unauthorized access to user accounts, they use these accounts for further fraudulent activities and to spread malicious links.

Wasted ad spend

The media and marketing industry can be affected by ad fraud in two ways. On the one hand, it can affect publishers who have MFA pages in their offering. On the other hand, advertisers who place their ads on MFA sites or in a non-brand-safe environment.

In the end, the fraudsters' goal is to generate revenue through fake clicks or impressions.

The future of invalid traffic and bots

Chapter 4

4.0

The future of invalid traffic and bots

Advances in artificial intelligence (AI), exemplified by models such as ChatGPT, will lead to an increase in fake internet activity as the barriers to creating bots are lowered and the sophistication and capabilities of malicious bots are improved.

Using modern AI, it is now trivial to spin up hundreds of thousands fake bot accounts with human-like behavior for less than a penny per account. We are coming to the end of this version of the internet, and it will be replaced by something entirely different.

This evolving landscape turns cybersecurity into a constant game of adaptation, where defense mechanisms are continually challenged by advancing opponents. The availability of advanced, free AI models potentially offers those with malicious intentions a tactical advantage.

Imagine this:

AI-driven bots creating compelling content – reviews, comments, user-generated content – with a level of credibility that is unparalleled. Imagine phishing emails brought to life by AI, or fake chatbots that can deceive on an unprecedented scale.

The impact of these expanded capabilities presents a challenge that requires a collaborative, multi-faceted effort to resolve.

In today's world, organizations must employ proactive strategies, monitor inbound activity, and automatically intercept and identify spoofed traffic before it enters their systems. Bot management is challenging, but by implementing effective bot detection and mitigation strategies, you can protect your website from threats.

AI-Powered bot detection to the rescue

Fighting bots is all about identifying visiting bots and minimizing their negative impact on your company, your users, and your customers. Bot detection and mitigation solutions are tailored to enable uninterrupted website access for humans and legitimate bots and act as barriers to prevent unauthorized access by malicious bots. With bot activity on the rise, it is important to detect and deal with traffic generated by bots. Nowadays, software continuously monitors bot activity within your online platforms, meaning it automatically fights threats in real-time as soon as they appear or try to gain access.

5.0

About fraud0

fraud0 is a cybersecurity company, backed by some of Europe's best software investors and serial entrepreneurs. Our mission is to protect businesses from the damaging effects of bot-generated activity such as fraudulent ad impressions, fake clicks, or skewed marketing statistics by providing advanced AI-powered bot detection solutions, optimizing marketing performance, and improving the digital experience for valid human traffic.

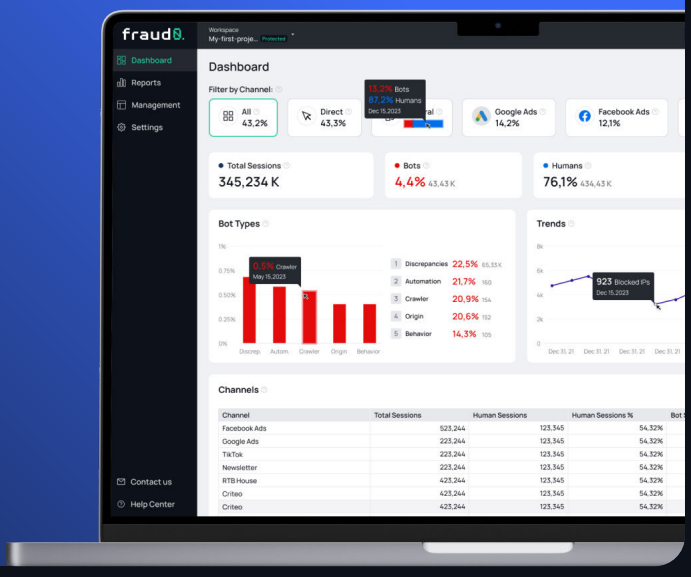
We strive to empower companies to make data-driven decisions based on accurate and reliable information, allowing them to thrive in the digital age. In this context, we can benefit from the knowledge of Dr. Augustine Fou - a leading fraud researcher who graduated from MIT with a PhD at 23. Dr. Fou has authored over 1,500 scientific articles on cybersecurity, developed proprietary technology, and works with leading global brands to protect them from the impact of invalid traffic.

Don't take our word for it, take our data.

Test fraud0 for 7 days without any obligation.

Test now for free

XPOSE360 RUFF CYCLES CHAIN REACTION AVANTGARDE pmc. ltur usercentrics MERZ AESTHETICS LEVIA FORUM Apollo dentsu Ulla Popken ARTDECO karriere.at elements



Disclaimer

The data and information presented herein are derived from internal databases and analyses performed by fraud0 based on our customers. Efforts have been made to ensure the accuracy and reliability of the information provided; however, the authors do not guarantee the absence of errors or omissions. Therefore, the information is provided "as is," and no warranties or representations are made regarding its completeness, accuracy, or currentness. This report contains information and analysis regarding invalid traffic on various marketing platforms. It is important to note that many marketing platforms employ sophisticated measures to identify and filter out invalid traffic, including but not limited to bot traffic. Such invalid traffic is generally excluded from performance metrics and billing calculations. As a result, advertisers are typically not charged for this category of traffic. However, the effectiveness of these filtration mechanisms can vary across different platforms and over time. Advertisers are encouraged to familiarize themselves with the specific policies and protections offered by each platform regarding invalid traffic. The findings and conclusions presented in this report are intended for informational purposes only and should not be considered as professional advice. Decisions based on the content of this report are the sole responsibility of the reader. The authors and publishers of this report disclaim any liability for losses or damages, direct or indirect, that may result from the use of, or reliance upon, any information contained in this report, including, but not limited to, any errors or omissions.

fraud0.

INVALID TRAFFIC 2024