

Click Patrol

Click Fraud; **The advertiser's plague.**
Does it exist?



Table of Contents

3

The value of advertising

- 4 Value creation by clicks
 - Valid Click
 - Invalid Clicks

6

Fraudulent Clicks and Click Fraud

8

Types of Click Fraud

- 4 Content channels and Inflationary click fraud
- 4 Competitive click fraud
- 4 The special case of Disgruntled Former Employees

11

Estimating and addressing the threat

- 4 Why are IPs important in detecting Click Fraud?

13

The role of search engines

15

Combating Click Fraud

- 4 The Pay Per Action Model
- 4 Third-Party Tools

17

The ClickPatrol Tool

- 4 Why should you choose the ClickPatrol tool?
- 4 Savings Predictions and Calculations

The value of advertising

The end goal of every advertiser who puts out an advert is the value their business receives from the ad. This could be in form of;

- Brand recognition from impressions in the traditional advertising model (PPM),
- Engagement in form of click in the pay per click model (PPC)
- Action e.g a purchase, a phone call or filling a form in the pay per action model (PPA)

The ability to relatively measure value in the online advertising space has given it its edge over other forms of advertising. The PPM, PPC and PPA models all measure value proxies to the advertiser who seeks to achieve two things; attention and conversion¹.

Attention:

For big brands such as auto manufacturers, their advertising intentions can be purely attention-seeking. Attention is thus measured via impressions and click-through rates.

Conversion:

For a small business that decides to place an ad, the most important metric is any action that directly brings in revenue. A conversion is defined as any action that directly brings in revenue. This is often translated as a sale.

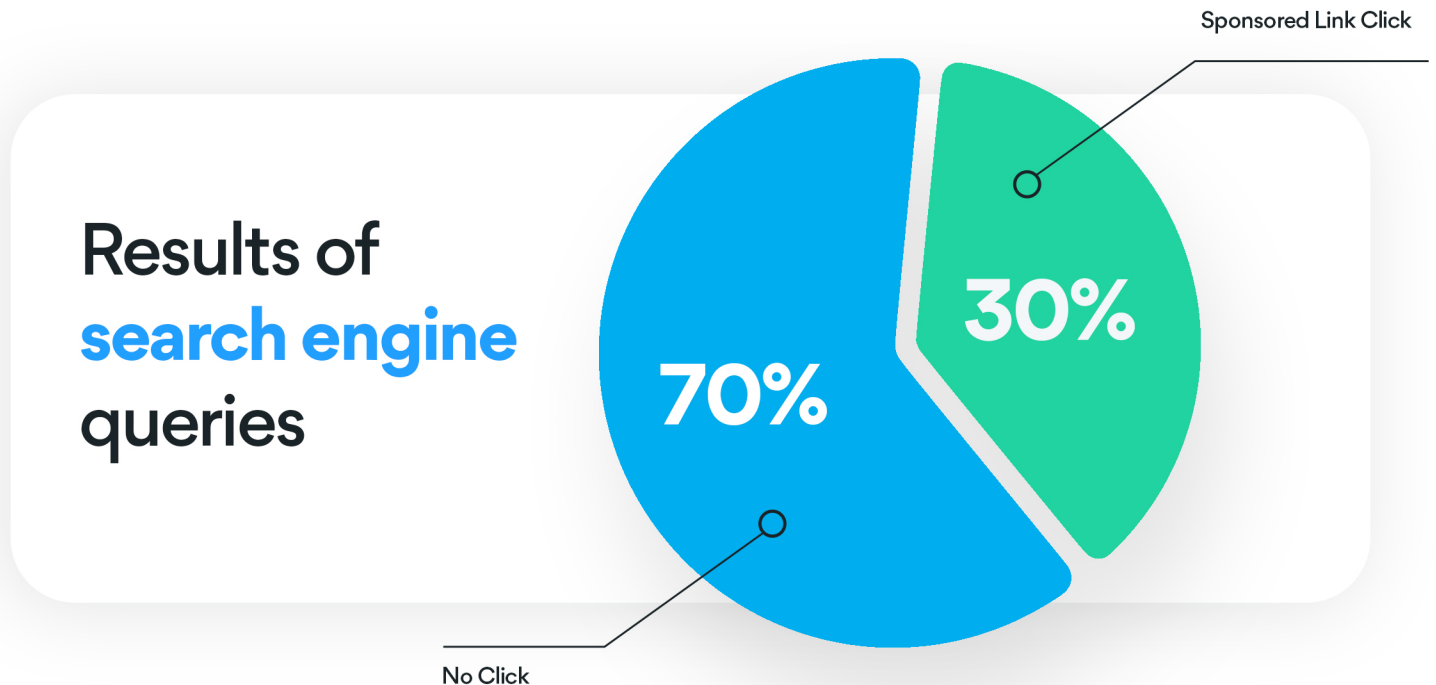
The pay-per-click model was designed in 1998 to attract small advertisers eager to drive traffic to their websites but was afraid of the risk's opacity related to pay-per-impression, the traditional advertising method at the time²

Every time a consumer enters a search query, the search engine produces a list of candidates' ads, together with other results that have been pre-ranked (ranking factors include the bid price) and possibly match the consumer's request.

If the consumer clicks on an ad, this event is logged and charged to the advertiser's account.

Value creation by clicks

Seventy percent of all search engine queries result in a paid link click. Sponsored links on SERPs get one or more clicks 30% of the time. However, not all link clicks generate value

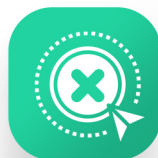


A click signifies the movement from the search engine's domain to the advertisers. This can be either a valid or invalid click



Valid Click

A valid click is an intentional click that provides value to the advertiser or an invalid click that offers no value. This accounts for approximately 24% of sponsored link clicks.



Invalid Clicks

Invalid clicks are made up of;

Void clicks:

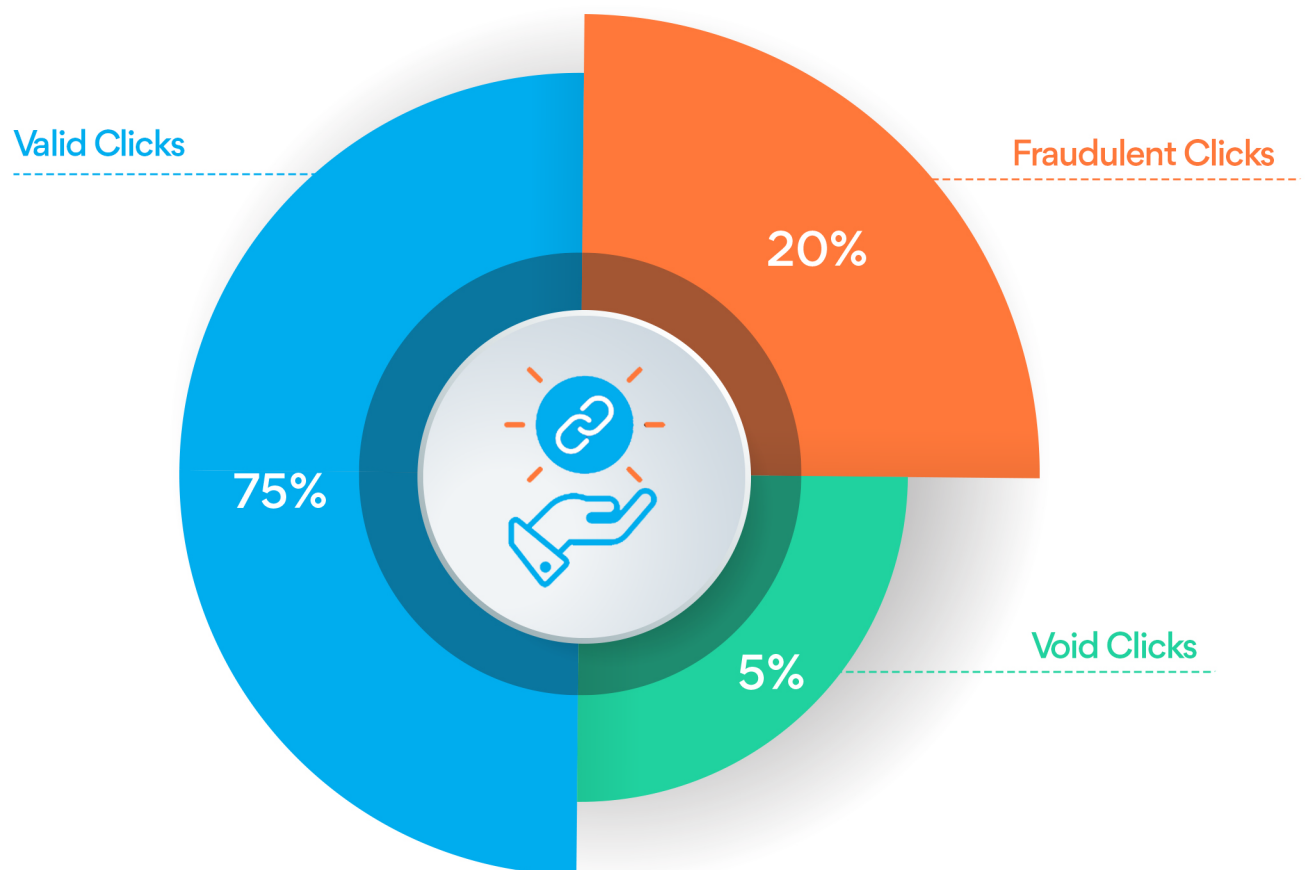
unintentional, with no discernible patterns or red flags. E.g. a user mistakenly double-clicks on a link. The ad network does not charge void clicks. Fraudulent clicks – intentional clicks, marked with one or more red flags. Every valid click indicates a user's interest in the advertiser's goods and services. This allows the advertiser to deliver value.

The **Economy** of Clicks

	Value Generating	No Value Generated
Paid Clicks	Genuine valid Clicks	Fraudulent Clicks
Unpaid	User Generated Clicks	Void Clicks

Free clicks are also valuable to online businesses

Distribution of **Paid Link Clicks**



Fraudulent clicks account for up to 20% of all clicks on paid links. Void and unintentional clicks happen approximately 5% of the time, while 75% of clicks are valid, genuine clicks.

³Xiarong Li, Daniel D. Zeng, and Yong Liu, Yanwu Yang, CBrendan Kitts,

Click Fraud and the Adverse Effects of Competition, IEEE Computer Society, 2011. Search engines often Click fraud as “invalid clicks” or “unwanted clicks.” This takes away any legal implications of the word ‘fraud’ and protects their best interests³.

Fraudulent Clicks and Click Fraud

Fraudulent clicks are intentional clicks with no value-generating intention¹.

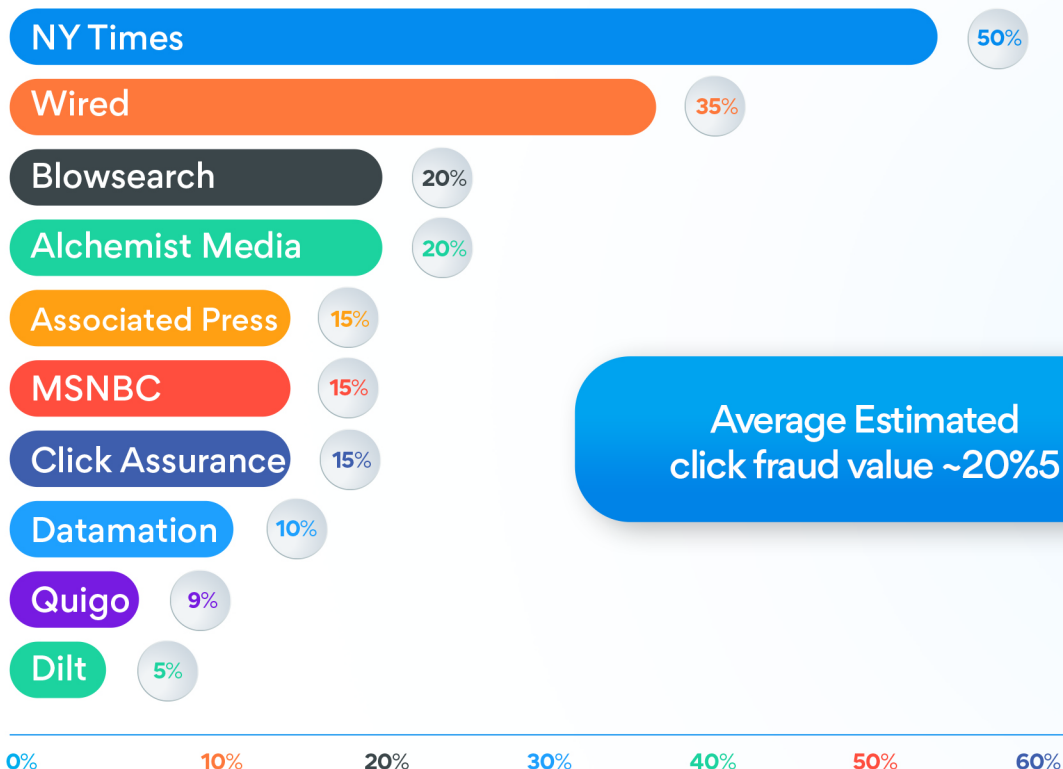
They deplete the advertisers' advertising budget with absolutely no ROI. Often, they are malicious^{4,1}

They often mirror valid clicks. However, in many cases, they follow a pattern and display characteristics that third-party tools and advanced AI can screen.

Click fraud is a complicated socioeconomic and technological phenomenon⁴. Unchecked, click fraud could undermine the sponsored search business model¹

Yahoo sees click fraud as “clicks arising for reasons other than the good-faith intention of an Internet user to visit a Web site to purchase goods or services or to obtain information.”

Google prefers the term “invalid clicks” and explains it as “any method used to artificially and/or maliciously generate clicks or page impressions.”



⁴ Tamara Dinev, Qing Hu, and Ali Yayla, Is There an On-line Advertisers' Dilemma? A Study of Click Fraud in the Pay-Per-Click Model, International Journal of Electronic Commerce / Winter 2008–9.

⁵ Benjamin LeBlanc, Ryan Meech and Parameshvyas Laxminarayan, Click Fraud, Bulletin of the American Society for Information Science and Technology, 2006

Types of Click Fraud

Although click fraud is generally described as malicious, click fraud types are distinguished based on the motive behind the action.



Content channels and Inflationary Click Fraud:

A major revenue source in the digital marketing and advertising space is the affiliate model/content channels. Search advertisements often appear on third-party affiliate websites. These website owners are compensated on a pay-per-click model. These third-party website owners often click on the ads to inflate their revenues.

This is the most common type of click fraud as these third parties are sometimes desperate to earn more ^{4,6}.

There are allegations of ad networks intentionally placing ads in known fraudulent 3rd party sites.

Competitive Click Fraud:

Competitors are notorious for attempting to use up their rival's ad budgets without any intention to purchase. Once a rival's ad budget is depleted, their ads are taken down, leaving the competitors' ads running. This inadeptly increases their ad budgets and reduces their profit ^{4,6}.

In 2004, John Carreras, president of Impact Displays, returned from a trade fair to discover that his ad expenses had been reduced by 50%. He then deduced that his competitors had been too busy with the trade show to click on his ad ⁵

In 2020, Online golf equipment retailer Motogolf.com dragged competitor Top Shelf Golf LLC to court for allegedly clicking repeatedly on Motogolf's PPC campaigns. They presented proof that specific IP addresses clicking on their ads were linked to Top Shelf Golf LLC.

In an interview with a particular company executive who enjoys clicking on his competitor's ads, he describes it as "entertainment" ⁵.

The special case of Disgruntled Former Employees:

A small percentage of click fraud is attributed to disgruntled former employees and customers⁴. This has gained more attention over time and is starting to become a concern for business owners.

In the past, there was news about disgruntled French workers inserting their wooden shoes (sabots) into machines to obstruct or sabotage them. Today, disgruntled employees are powerful enough to sabotage your business operations simply with the click of a button⁷.

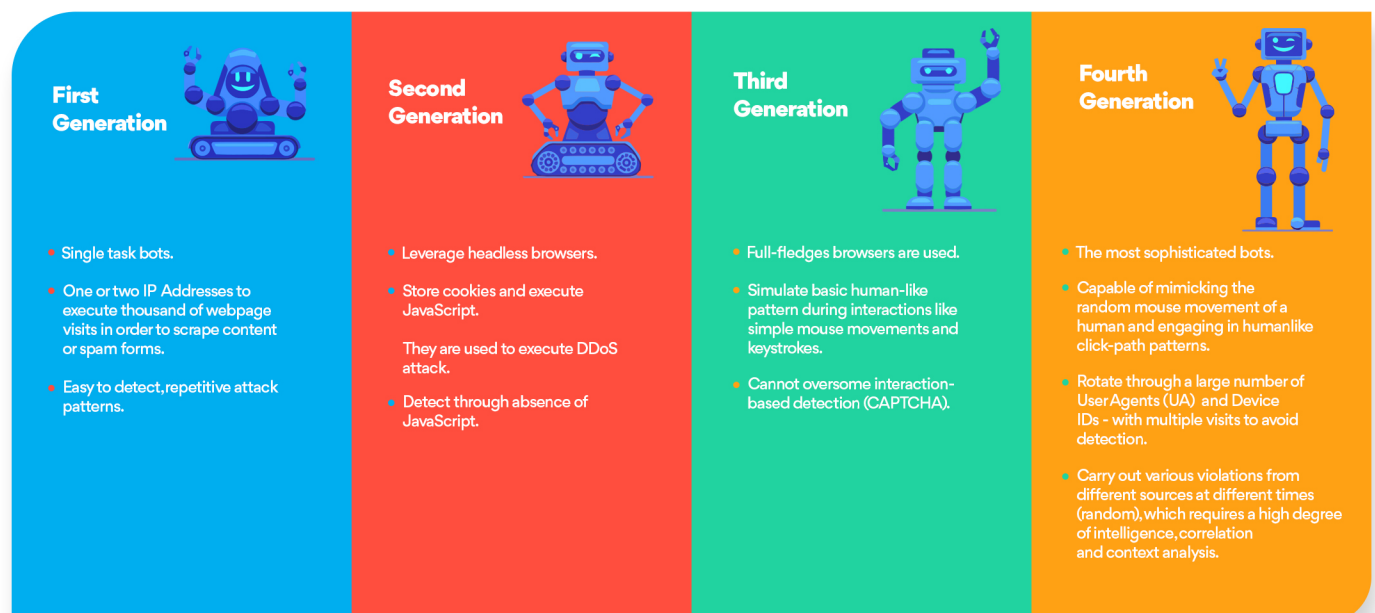
Bots and Click Fraud

Bots are essential tools for perpetrating click fraud. Web bots have rapidly evolved from simple coding tools with control interfaces to modern-day, complex algorithms that mimic human behavior (e.g., maneuvering a website or application, utilizing the mouse, touching and dragging objects, etc.)⁸.

Fig 4: The Evolution of Bots⁸

⁷Sjaak Schouteren, JLT Specialty, from wooden shoe to click of a button: the risk of disgruntled employees, Computer Fraud & Security, 2019.

⁸Shadi Sadeghpour* and Natalija Vljic, Click Fraud in Digital Advertising: A Comprehensive Survey, Computers 2021, <https://www.mdpi.com/journal/computers>



Botnet click campaigns are the most efficient way to target many pay-per-click ads by infecting computers connected to the internet with malware and using them to click on ads without the knowledge of the owners of these computers under the control of a botmaster⁸.

They are used by network owners who wish to inflate traffic, competitors who wish to spy on their rivals and inflate their ad spending and aggrieved and disgruntled employees looking for payback.

Estimating and addressing the threat

Over the years, researchers have used various methods to detect and estimate click fraud. Some of which were developed using high-level research. Ad networks and third-party screening tools often use more than one method to detect click fraud.

The statistical approach assesses past advertising data, including click-through and conversion rates. This information calculates the probability of a click converting using binomial distribution⁹.



$$\text{Fraud \%} = \frac{\sum_{u: p_u < 0.01} c_u}{\sum_{i=1}^N c_i} \quad \text{Where } p_u = \text{bpdf}(A_u, c_u, a) = \binom{c_u}{A_u} a^X (1-a)^{(c_u - A_u)}$$

The anomaly-based approach assesses how much a click deviates from the normal predictable characteristics of valid clicks based on existing data⁹.

The rule-based approach employs optimization algorithms to classify valid and invalid clicks determined by specific conditions⁹.

The Classifier-based approach relies on past data to detect invalid clicks. It assumes past clicking behaviors predict future behaviors⁹.

⁹ Nir Kshetri, The Economics of Click Fraud, IEEE COMPUTER AND RELIABILITY SOCIETIES, 2010.

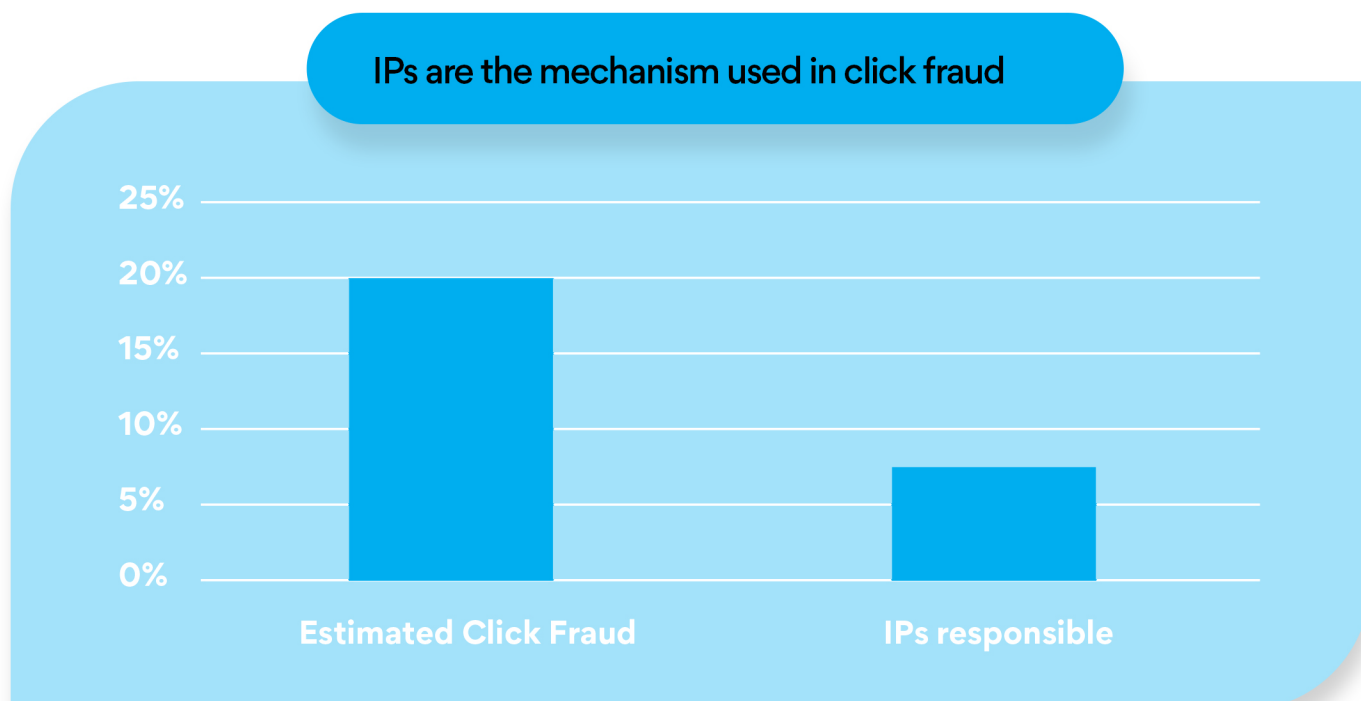
Why are IPs important in detecting Click Fraud?



Every device that accesses the internet has a unique address called the Internet Protocol (IP) address. This means that each click on an ad can be traced via the IP address of its originating device.

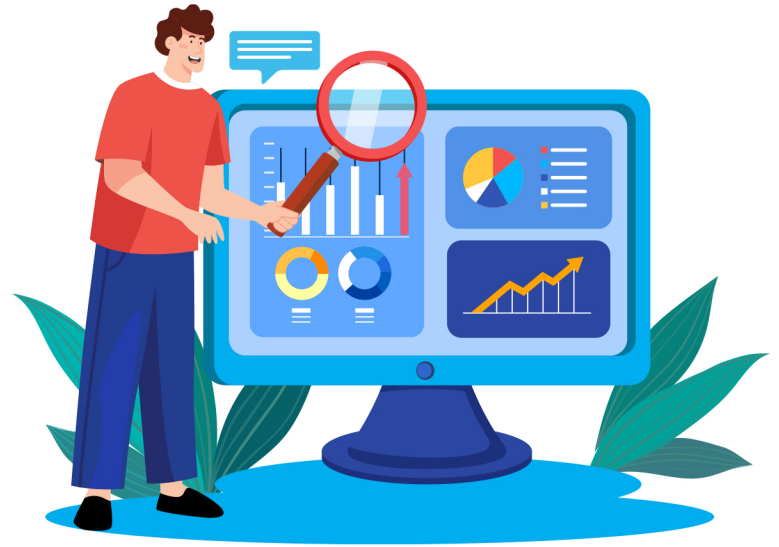
Over the years, certain IPs have been flagged as fraudulent due to recurrent fraudulent activities. An essential function of third-party tools is to screen IPs that click on an ad and block/blacklist fraudulent IPs.

Fig 5: IPs and Click Fraud



Only about 5% of IPs are responsible for the estimated 20% Click Fraud

The Role of Search Engines

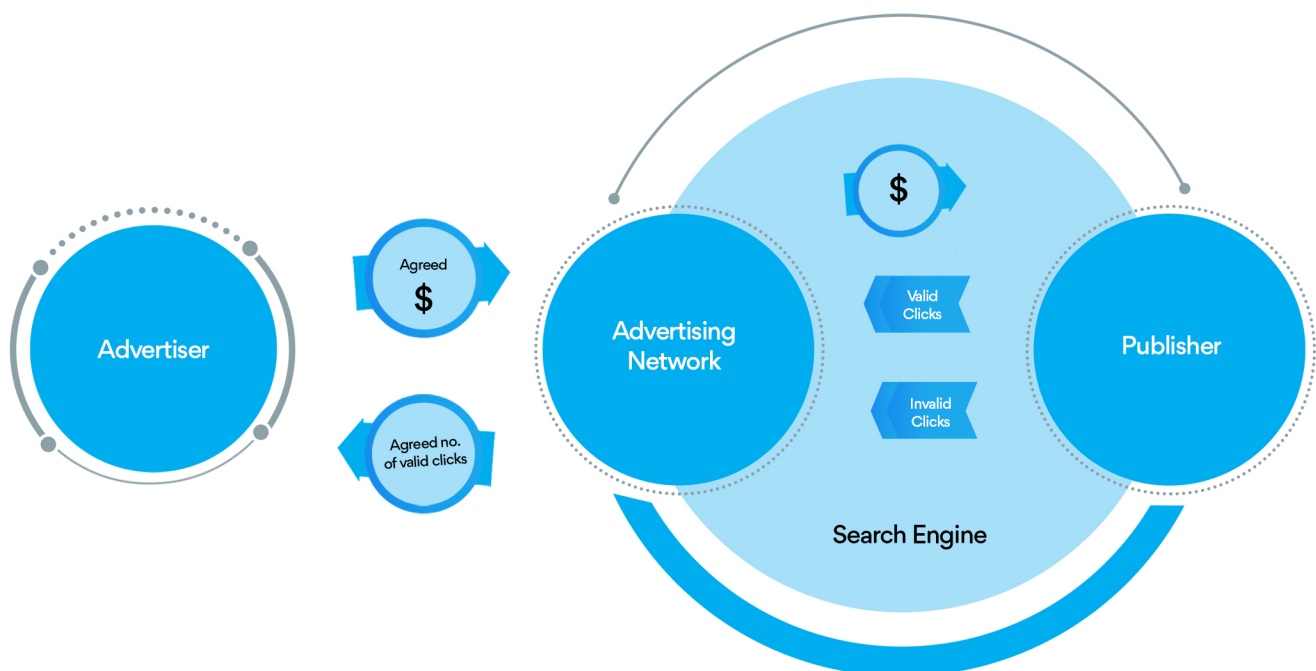


The relationship between advertisers and search engines is somewhat complex.

Advertisers (businesses and organizations) contact advertising networks (e.g., Google Ads) with a need to promote their goods and services. They agree on specific terms, i.e., a price for a few clicks.

These advertising networks then provide delivery services that enable these adverts to run on the publishers' web pages (Google SERPs), where clicks are generated. They are also charged with detecting and removing invalid clicks¹⁰.

In many cases, search engines own both the advertising networks and the publishers belong to the search engine^{3,10}



¹⁰ Bobji Mungamuru, Stephen Weis, Hector Garcia-Molina, Should Ad Networks Bother Fighting Click Fraud? (Yes, They Should), Stafford University Press, 2010

Trust is a critical factor in the relationship between advertisers and search engines. Advertisers trust advertising networks to deliver only valid clicks. This means that advertisers believe in the absolute ability of advertising networks (search engines) to handle the problem of click fraud.

This trusting belief explains the advertiser's expectation that the search engine provider acts in their best interest.

However, many industry experts have begun questioning search engines' commitment to tackling the issue. This perception stems from the lack of transparency and accountability in search engine efforts to combat click fraud⁴.

Visibility = Accountability

Transparency in handling click fraud is seemingly tricky for search engines as complete visibility and transparency from search engines risks further enabling Click Fraudsters.

Advertisers cannot ignore the direct benefits of click fraud to advertising networks and search engines. Search engines directly benefit from the number of valid clicks delivered to advertisers.

This conflict of interest indicates that search engines may not be as aggressive as they should in tackling click fraud because they profit from labeling more clicks as valid^{9,10}

Over time, Google has continued to receive heat for its inability to detect click fraud correctly. In 2006, Google paid a \$90 Million settlement to a group of 70 advertisers who claimed they had been billed for fraudulent clicks.

In 2017, A company called Ad Trader led another lawsuit against Google for failing to provide refunds to selected advertisers who had been previously charged for fraudulent clicks.



Combating Click Fraud

Advertisers want value. Search engines can provide the value; however, fraud tries to come in the way of that. To effectively fight ad fraud, advertisers must put themselves first. Pay for value and receive Value. No more blind trust, no more half-truths.

According to industry experts, ad fraud can be eliminated in two ways; Using the pay per action model and aggressive monitoring using third party tools.

The Pay Per Action Model

The-pay-per-action model puts the advertiser in the driving seat. They only pay for actions that directly translate to value for their business. A call, A firm filled, a new sign-up, or a new sale.

In the PPA model, Ad networks and publishers are forced to trust the advertisers as the timing and frequency of action that is recorded cannot be monitored by the search engine.

Gathering and sharing this data is expensive for advertisers, and they may also choose to misreport details for strategic reasons

Third-Party Tools

Third-party tools act as a screen between the Ad network and the advertiser. They conduct a more thorough investigation of clicks as they move from the ad network to the advertiser's website.

These neutral third parties are obliged to share their screening technologies with both the publisher and the advertisers, thus making them free of moral hazards and possible conflicts of interests.

The Relief Third Party Tools bring to all parties involved in the click fraud fiasco cannot be overstated. They can help restore the trust between Advertisers, Ad networks, and Publishers.

With third-party monitoring tools, advertisers can have a smoother interaction with search engines, knowing that regardless of the actions or inactions of search engines in dealing with click fraud, their investments are well protected and are assured of receiving valid clicks only.

Advertisers describe the effectiveness of third-party tools in PPC as the key to maximizing the benefits of online advertising.

Many third-party tools operate the advertiser-pay-regime, where advertisers pay third parties for each click investigated. This regime is most efficient as it demonstrates the advertisers' interest in receiving the best possible value for money. This also forces search engines to improve their verification technology

With these tools, advertisers can verify each click and fully control who can or cannot click on their ads, using blacklist and whitelist options.

The Clickpatrol Tool

The ClickPatrol software is a 3rd party tool that screens every single click on your PPC campaign. Our Algorithm screens clicks based on a set of well-defined set of criteria.

This criterion is made up of 800 IP and fingerprint characteristics that are checked for every click. These characteristics are based on the peculiarity of your campaign.

They include location, type of device, device software, number of times they have visited your campaign, etc.

These characteristics have a standard for genuine valid clicks. Fraudulent clicks have one or more deviations from the standard (red flag).

A value is assigned for each deviation, a maximum value after which a click is flagged, and a threshold value, after which a click is blocked.

For example, if a campaign which is running in the US and in desktop only, gets a click from a mobile device in India, the click is flagged and may be blocked, depending on how much of a variation it displays.

Our software Algorithm uses traffic data collected over several years from multiple sources to determine what characteristics need to be checked and how much deviation should be recorded as fraudulent.

Clicks are only blocked if we are confident they are Unwanted.

Blocked clicks are determined based on the history of an IP, as well as its fingerprint.

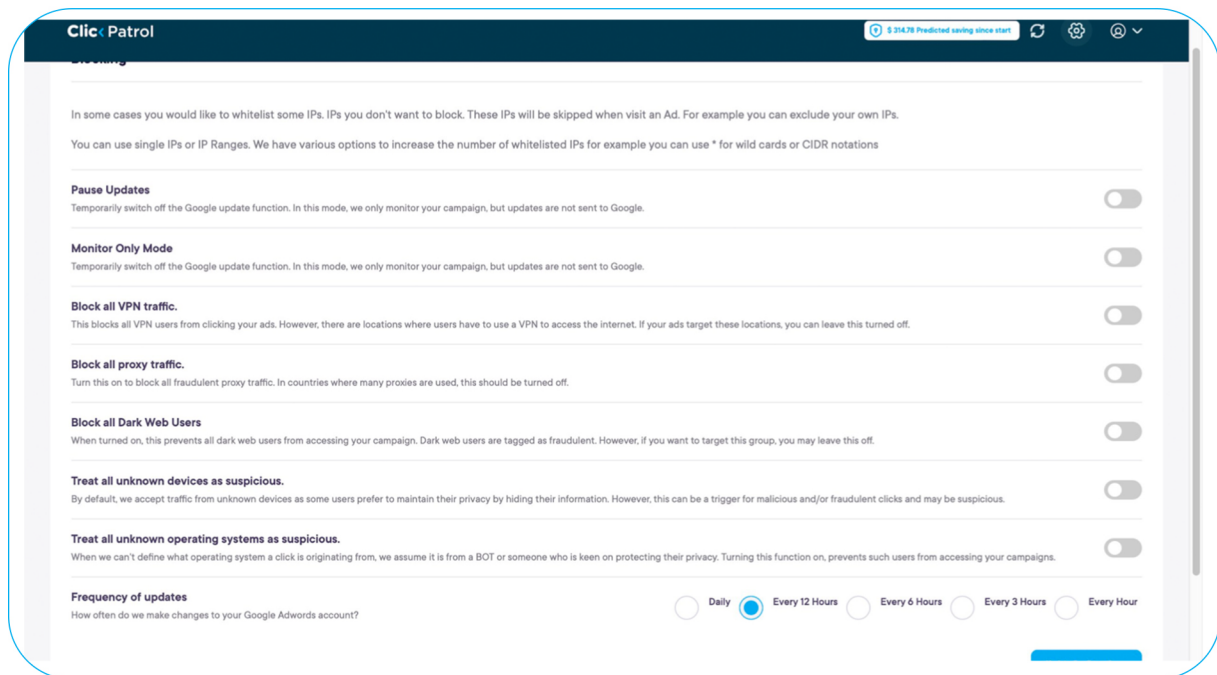


Why should you choose the ClickPatrol tool?

Users have complete control.

Our clients can fully customize the API and maximize their experience.

You can choose to only monitor your campaigns and not make updates to google; you can also decide how aggressively you want to track and block fraudulent or unwanted clicks.



Users can also manually review blocked IPs, whitelist, and blacklist where necessary.

Supports all Google Campaigns

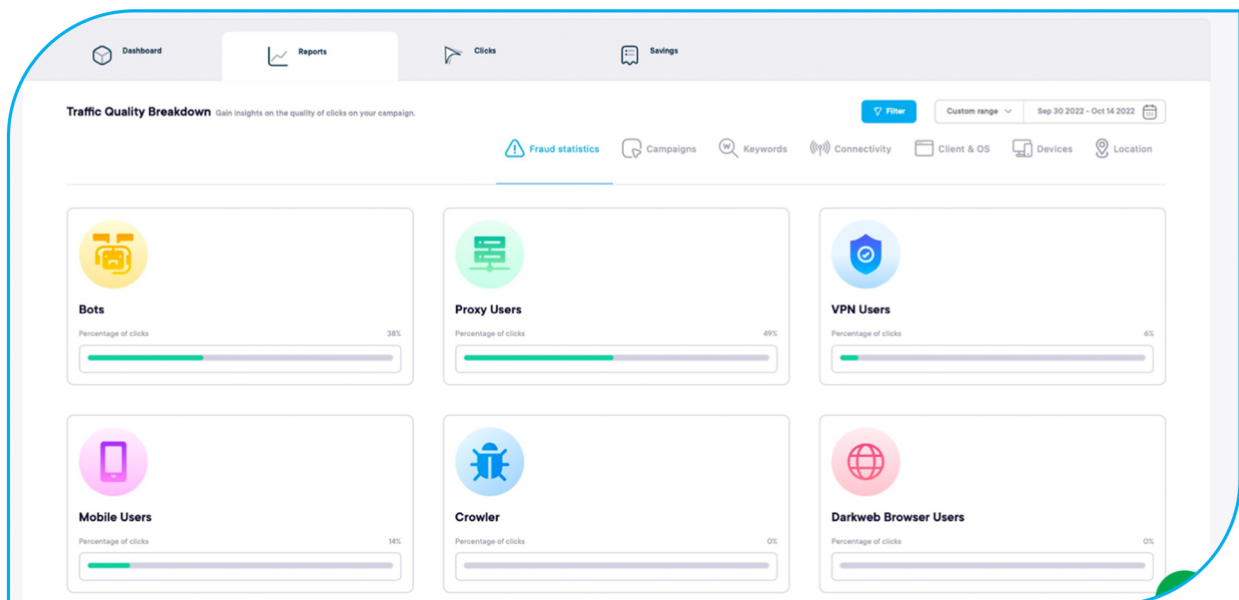
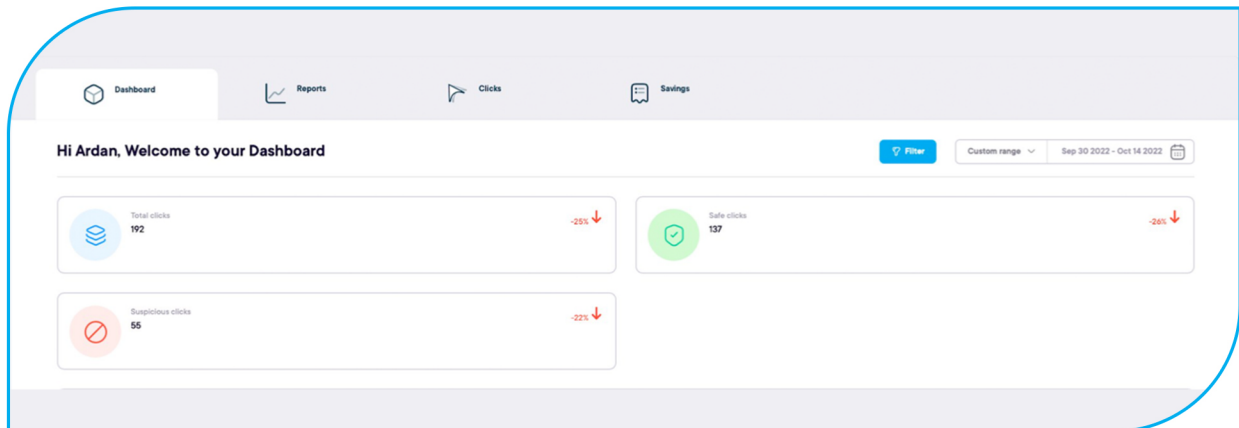
Our tool supports all forms of Google ads campaigns including;

- ✓ Google Pmax,
- ✓ Google Search ads,
- ✓ Google Display ads,
- ✓ Apps (We exclude traffic on account level),
- ✓ Google Shopping Advertising,
- ✓ Gmail Sponsored Promotions

Users can also exclude certain on campaigns on their ad accounts from being monitored.

Monitor traffic quality with In-depth Reporting and Insights.

Our reports tell you exactly what kind of traffic comes to your website. We share unique insights based on our data points unavailable via the ad network. All data can be exported, analyzed, and used to make informed marketing decisions.



Click Patrol \$ 314.96 Predicted saving since start

Click Insights Detailed insights on each individual click on your campaigns

+ Add column CSV Search

DATE	GEO	AI SCORE	INTERNET SERVICE PROVIDER	DEVICE OPERATING SYSTEM	SUSPICIOUS
14-10-2022 03:11:29	Regent	High	Telmex Colombia S.A.	iOS 16.0	☐
14-10-2022 00:27:40	Phnomh	High	Telenor Bulgaria	Android 11	☐
14-10-2022 00:21:25	Tangerang	Low	PT Telkom Indonesia	iOS 16.0	☐
13-10-2022 23:56:19	Istanbul	High	Turk Telekom	iOS 15.6	☐
13-10-2022 22:04:39	Karakik	Low	Turk Telekom	Android 11	☐
13-10-2022 21:39:05	Mesta	Low	GO Malta	Android 11	☐
13-10-2022 21:30:01	Zamboanga City	Low	Philippine Long Distance Telephone	Android 10	☐
13-10-2022 20:21:44	Recoar	High	Philippine Long Distance Telephone	iOS 16.0	☐
13-10-2022 19:57:31	Istanbul	Low	Turk Telekom	iOS 16.0	☐
13-10-2022 19:54:38	Jemena	Low	Telo2 Lithuania	Android 12	☐
13-10-2022 19:45:01	Nairobi	Low	Falba	iOS 15.6	☐
13-10-2022 19:29:56	Colombo	Low	Dialog Axiata	iOS 14.7	☐
13-10-2022 18:38:49	Dallas	High	Zscaler	Windows 10	☐

ClickPatrol

\$ 314.96 Predicted saving since start

Sep 30 2022

Oct 01 2022

Oct 02 2022

Oct 03 2022

Oct 04 2022

Oct 05 2022

Oct 06 2022

Oct 07 2022

Oct 08 2022

Oct 09 2022

Oct 10 2022

Oct 11 2022

Oct 12 2022

Oct 13 2022

Oct 14 2022

Click Insights

Detailed insights on each individual click on your campaigns

+ Add column

CSV

Search

DATE	GEO	AI SCORE	INTERNET SERVICE PROVIDER	DEVICE OPERATING SYSTEM	SUSPICIOUS
14-10-2022 03:11:29	Regent	High	Telecom Colombia S.A.	iOS 14.0	☐
14-10-2022 00:27:40	Plovdiv	High	Telenor Bulgaria	Android 11	☐
14-10-2022 00:21:25	Tangerang	Low	PT Telkom Indonesia	iOS 14.0	☐
13-10-2022 23:56:19	Istanbul	High	Turk Telekom	iOS 15.6	☐
13-10-2022 22:04:39	Karslik	Low	Turk Telekom	Android 11	☐
13-10-2022 21:39:05	Mosta	Low	GO Malta	Android 11	☐
13-10-2022 21:30:01	Zamboanga City	Low	Philippine Long Distance Telephone	Android 10	☐
13-10-2022 20:31:44	Bacoor	High	Philippine Long Distance Telephone	iOS 14.0	☐
13-10-2022 19:57:31	Istanbul	Low	Turk Telekom	iOS 14.0	☐
13-10-2022 19:54:38	Jonava	Low	Tele2 Lithuania	Android 12	☐
13-10-2022 19:48:01	Nafrobi	Low	Falba	iOS 15.6	☐

Dashboard

Reports

Clicks

Savings

Device Operating System

Gain insights on the operating system of devices assessing your ads

Filter

Custom range

Sep 30 2022 - Oct 14 2022

Fraud statistics

Campaigns

Keywords

Connectivity

Client & OS

Devices

Location

Device Operating System

Show 10 entries

Search

OS TYPE	TOTAL CLICKS	SUSPICIOUS CLICKS	% OF SUSPICIOUS CLICKS
iOS	95	45	47%
Android	70	38	54%
Windows	23	10	43%
Mac	4	1	25%

Showing 1 to 4 of 4 entries

Previous

1

Next

Advanced OS Reports

Show 10 entries

Search

OS VERSION	TOTAL CLICKS	SUSPICIOUS CLICKS	% OF SUSPICIOUS CLICKS
iOS 14.0	43	22	51%
iOS 15.4	27	14	52%
Android 12	24	13	54%
Windows 10	23	10	43%
Android 11	20	9	45%
Android 10	14	11	79%
Android 9	6	1	17%
iOS 15.5	6	3	50%
iOS	4	0	0%
iOS 14.7	3	1	33%

ClickPatrol

\$ 314.96 Predicted saving since start

Sep 30 2022

Oct 01 2022

Oct 02 2022

Oct 03 2022

Oct 04 2022

Oct 05 2022

Oct 06 2022

Oct 07 2022

Oct 08 2022

Oct 09 2022

Oct 10 2022

Oct 11 2022

Oct 12 2022

Oct 13 2022

Oct 14 2022

Dashboard

Reports

Clicks

Savings

Devices

Assess device types and models

Filter

Custom range

Sep 30 2022 - Oct 14 2022

Fraud statistics

Campaigns

Keywords

Connectivity

Client & OS

Devices

Location

Device Manufacturer

Show 10 entries

Search

DEVICE MANUFACTURER	TOTAL CLICKS	SUSPICIOUS CLICKS	% OF SUSPICIOUS CLICKS
Apple	95	45	47%
Samsung	37	18	49%
N/A	31	18	58%
Xiaomi	2	2	100%

Showing 1 to 4 of 4 entries

Previous

1

Next

Device Type

Show 10 entries

Search

DEVICE TYPE	TOTAL CLICKS	SUSPICIOUS CLICKS	% OF SUSPICIOUS CLICKS
iPhone Apple	91	45	49%
N/A Samsung	37	18	49%
N/A N/A	31	18	58%
iPad Apple	4	0	0%
N/A Xiaomi	2	2	100%

Showing 1 to 5 of 5 entries

Previous

1

Next

© ClickPatrol

Copyright | Privacy Policy