# EVERYTHING YOU NEED TO KNOW ABOUT CLICKFRAUD

PPC Protect

https://ppcprotect.com

# QUICK NAVIGATION

# A LOOK INTO CLICK FRAUD

## THE BIGGEST PROBLEM FACING PPC MARKETERS

The last two decades has brought about a marketing revolution, with online advertising completely changing the way businesses reach out to consumers. TV ads and billboards are giving way to online advertising as the more traditional advertising methods are slowly fading away.

Not only does online advertising allow businesses to reach more consumers for a fraction of the price, it also allows companies to target specific demographics. When combined with real-time analytics, and the ability to closely monitor advertising spend, it's no surprise that online advertising has become so popular. Online advertising has seen a wide variety of advertising models throughout its history; from banners with fixed monthly fees, to ads that run on a cost per impression basis, and with models constantly evolving, businesses of all sizes are able to tap into the potential of online advertising.

However, none of these methods come close to the power and customizability which pay per click marketing offers you. The ability to bring in billions of people every single day means that pay per click marketing is quickly becoming an essential marketing strategy for every business.

With so many businesses all using pay per click advertising, and with money constantly changing hands, it has attracted an increasing number of fraudsters to the industry.

Known as click fraud, this activity can cause businesses to lose billions of dollars a year. Thanks to the simplicity of click fraud and the amount of businesses using pay per click advertising, almost no one is safe.

To give you an idea of how click fraud costs businesses so much money, we first need to take a look at pay per click advertising. In order to do that, we need to travel back to 1994 – the dawn of internet advertising.

# THE HISTORY OF ONLINE ADVERTISING

## HISTORY PART ONE: THE EARLY DAYS

To many people, it often seems like online advertising has been around forever, when in fact it's only just recently celebrated its 23rd birthday. Over the years online advertising has changed immensely with new advertising models and technologies constantly shaping the industry. However, all online advertising models are built on the same foundations and can be traced back to a single website.

On the 27th October 1994 when the website HotWired (now Wired.com) displayed a simple banner ad, it became the first documented case of online advertising.

The ad which was paid for by AT&T simply read: Have you ever clicked your mouse right here? You Will.

Have you ever clicked
your mouse right HERE?
YOU
WILL

The first "online billboard" of its time.

This single banner ad is what changed the marketing industry forever and spawned a new era of online marketing.

For the first time in history, advertisers could analyze exact numbers for how many people had seen and interacted with their ads. This allowed them to understand how well an ad was performing and if it was worth the money. A huge change from traditional billboards where advertisers had no idea if the hundreds of people driving past their giant ads so much as glanced up at them.

The AT&T banner ad had a reported click through rate as high 44%! This was an impressive feat as these days most display ads have a meagre click through rate of around 0.19% and as soon as other advertisers heard about the success of this online banner, they began to find ways to get their own companies advertised on the internet.

Not long after the online banner ad, online advertisers took the concept to the next level with geographical targeting. This ability to target specific web users from certain locations would become the foundation for many future online advertising models. Not only does it help advertisers target the consumers they want to target, but it also helps them save money by avoiding the consumers who are unlikely to fork over the cash.

Advertisers began to pile millions into the online advertising industry, creating an unprecedented wave of ads. Of course, this quickly resulted in people getting fed up of them. Still, webmasters continued placing ad banners on their websites, which resulted in their click through rate dropping dramatically. Advertisers were desperate for a new way to grab users and to reach the click rate they once possessed. The battle for your attention had begun.

This thirst for increased user interaction led to one of the most annoying online advertising methods ever: the pop-up.

After an advertiser complained that an ad had appeared on an inappropriate page, Ethan Zuckerman, a developer for Tripod.com, developed a new method to display adverts. The aim of the pop-up was to associate an ad with a web page without putting the ad directly on the page.

Although his intentions were honest, many other websites quickly copied the idea and by the end of 1997 the internet was swamped with these ads. Pop-ups initially saw a boost in click through rates on ads, but eventually users got fed up with the constant spam and installed pop-up blockers.

# THE BIRTH OF GOOGLE AND ADWORDS

## HISTORY PART TWO: GOOGLE AND BEYOND

It wasn't long until a significant shift started to occur in online advertising. Since the launch of the first banner ad in 1994, many advertisers had to display their ads on hundreds of different websites to capture the most traffic.

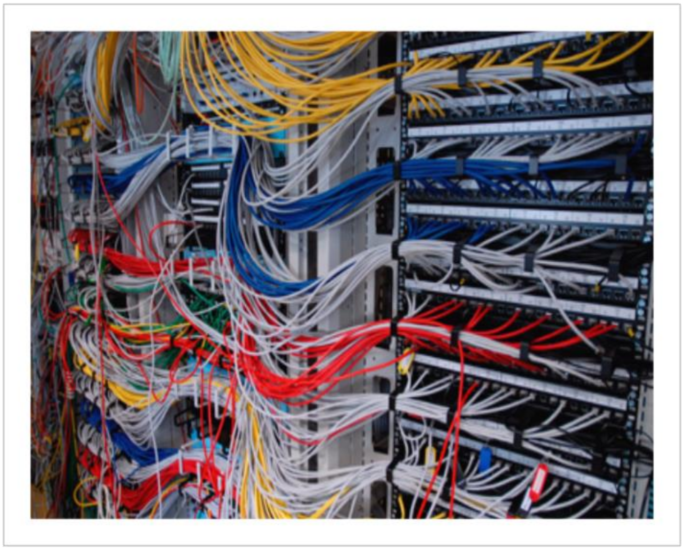
In the late 1990's however, a new central hub which attracted millions of users was born: the search engine.

Back in the 1990's before Google was around, you would have had to rely on the likes of Yahoo and Goto.com to find websites. These search engines attracted millions of users per day and were the perfect place for businesses to advertise their goods and services.

These websites served as the middle man between advertisers and consumers. Users would come to the search engine trying to find a specific product or service, while advertisers would try to ensure that what they were offering was seen by relevant consumers.

The invention of search engines allowed advertisers to do much more than target users based on their search intention though.

Advertisers were now able to determine where customers were visiting their websites from. This gave them the power to focus their ads toward geographical locations where clicks were the highest.



When the first search engine advertising service was launched by Planet Oasis in 1996 it wasn't long before many other search engines began to copy it, including Yahoo.

In the year 2000 a newly formed search engine called Google launched its search engine advertising service "AdWords" despite no one really knowing who they were.

Initially launched as a cost per thousand impressions service, the service quickly changed to a cost per interaction or cost per click model.

Unlike other advertising models in the past that were priced at a fixed monthly cost, search engine advertising was different. Since there were only a limited number of advertising slots per search term, advertisers had to bid against each other to win the right to display their ads.

This type of keyword bidding spawned the birth of the pay per click advertising model and is still the most widely used and popular advertising method today.

# PAY PER CLICK EXPLAINED

## THE SIMPLE WAY AND THE DETAILED WAY

If you are new to pay per click advertising and aren't very technical, then understanding it can be tricky, but think of it like this:

Imagine you own a grocery store and you want to advertise your products to potential customers in the area. With a small advertising budget of a few hundred dollars, expensive advertising methods are certainly a no no. Instead, you decide to invest your budget into producing leaflets. Each leaflet produced costs you a fixed amount of money with higher quality leaflets costing slightly more.

You put these leaflets on a stand outside your store, as well as placing them in other shops around the area. After a few days, you notice the average number of customers to your shop has started to increase.

You go outside and see that almost all the leaflets you left outside are gone. It would be pretty safe to conclude that: the leaflets placed outside your shop and in other shops are attracting more customers to your store.

Of course, the statistician in the group may point out that this could be random chance, but you could ask customers how they heard of your business, or offer a discount for showing the coupon on purchase.

This is essentially how pay per click marketing works.

Online adverts are the leaflet and the cost per click is the cost of the leaflet. Displaying your advert on other websites using the Google display network is the online equivalent of leaving leaflets in other shops, and every time somebody takes your leaflet it costs you the production fee regardless of whether they end up buying from you or not. The same applies to the pay per click model.

Obviously, there are some major differences in pay per click advertising, such as the ability to target specific demographics and an international audience. However, the leaflet analogy is still a good starting point for beginners to understand the core concept of pay per click advertising.

# A MORE DETAILED LOOK

To understand how fraudsters abuse online advertising it's important to understand how the various advertising models work.

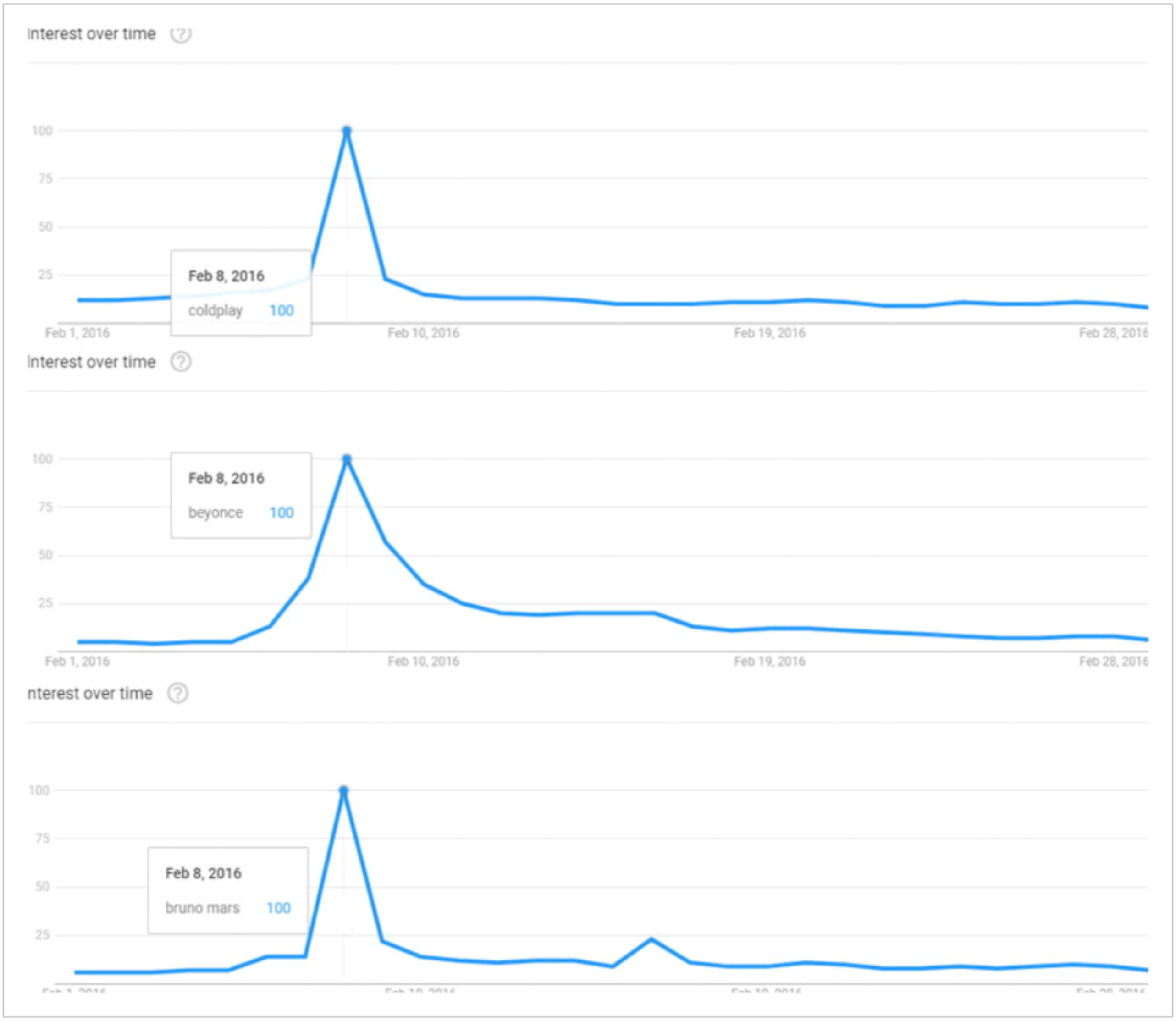
Pay per click marketing is by far the biggest online advertising model out there, and is used by hundreds of websites including Google, Bing and Facebook.

You might be wondering why search engines don't just charge a fixed monthly fee for their adverts, well here's why:

Unlike other online advertising models, pay per click benefits both advertisers and publishers equally. Advertisers can split their budget between hundreds of keywords and have the ability to change them or adjust their spend at any time. Other methods such as fixed banned ads usually require advertisers to commit to at least a full month, or a minimum spend which doesn't offer as much flexibility. This allows advertisers to spend their budget in the places that give them the best return on their investment.

Publishers benefit from the pay per click model by using it to take advantage of the constant change in demand for keywords. For example, you're not likely to find many people searching "Christmas pudding recipe" in the middle of August.

But there are also plenty of keywords that can receive spikes in search volume due to certain events. A great example of this is Superbowl 50 back in 2016, when Coldplay, Beyoncé and Bruno Mars performed at the half time show, they all saw an increase in search volume which led to a lot more album sales.

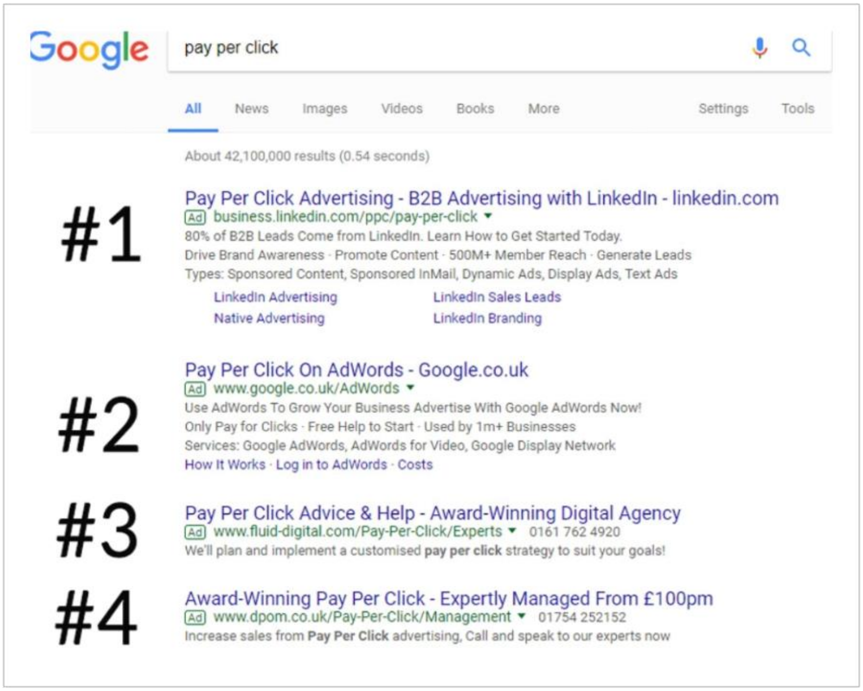


As you can see from the data taken from Google trends, each search term received a spike in traffic around the time of the Super Bowl. During that time, it's common for certain keywords to increase in price due to the increase in demand. If search engines used a fixed model then advertisers would be paying the same price regardless of how much traffic they received. Obviously, search engines are in the business to maximize their profits, which is exactly what pay per click advertising helps them do.

So how does the pay per click advertising model work?

Well, it's fairly simple.

Advertisers bid against each other to display their ads on a given search engine or network. Since Google and their pay per click service AdWords is the biggest and most popular network, we'll be focusing on how their service works. Don't worry if you aren't a Googler though, almost every pay per click network is identical.



About 42,100,000 results (0.54 seconds)

Pay Per Click Advertising - B2B Advertising with LinkedIn - linkedin.com
Ad business.linkedin.com/ppc/pay-per-click
80% of B2B Leads Come from LinkedIn. Learn How to Get Started Today.
Drive Brand Awareness · Promote Content · 500M+ Member Reach · Generate Leads
Types: Sponsored Content, Sponsored InMail, Dynamic Ads, Display Ads, Text Ads
LinkedIn Advertising · LinkedIn Sales Leads
Native Advertising · LinkedIn Branding

Pay Per Click On AdWords - Google.co.uk
Ad www.google.co.uk/AdWords
Use AdWords To Grow Your Business Advertise With Google AdWords Now!
Only Pay for Clicks · Free Help to Start · Used by 1m+ Businesses
Services: Google AdWords, AdWords for Video, Google Display Network
How It Works · Log in to AdWords · Costs

Pay Per Click Advice & Help - Award-Winning Digital Agency
Ad www.fluid-digital.com/Pay-Per-Click/Experts 0161 762 4920
We'll plan and implement a customised **pay per click** strategy to suit your goals!

Award-Winning Pay Per Click - Expertly Managed From £100pm
Ad www.dpom.co.uk/Pay-Per-Click/Management 01754 252152
Increase sales from **Pay Per Click** advertising, Call and speak to our experts now

If you've been using Google regularly over the last few years then you'll notice that the top links are increasingly becoming sponsored results. Look at the screenshot on the left.

As you can see, there are 4 adverts displayed for the keyword "pay per click" at the top and 3 at the bottom, not shown in this image. The number of ads regularly changes with the popularity of a keyword, the maximum being 7. It is fairly common for less popular keywords to only have a handful of ads at the top.

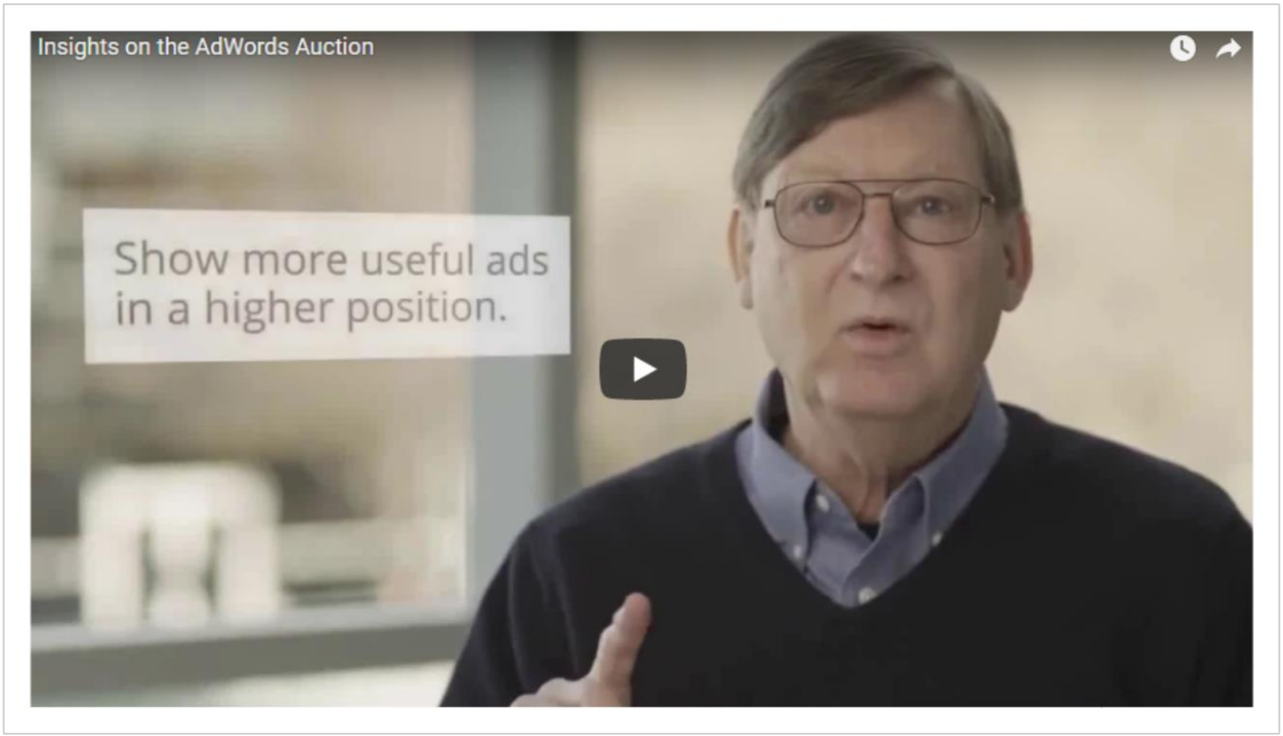
In this example, advertisers bid against each other to decide who takes the number 1 spot.

As most people click the first link they come across when using a search engine, the top advert will get a great deal more clicks and the highest amount of traffic.

The bidding system allows advertisers to decide how much they are willing to pay per click with the results being updated in real time. Going for the number 1 spot is not always profitable though, as you can usually pay less money and still receive a nice number of clicks.

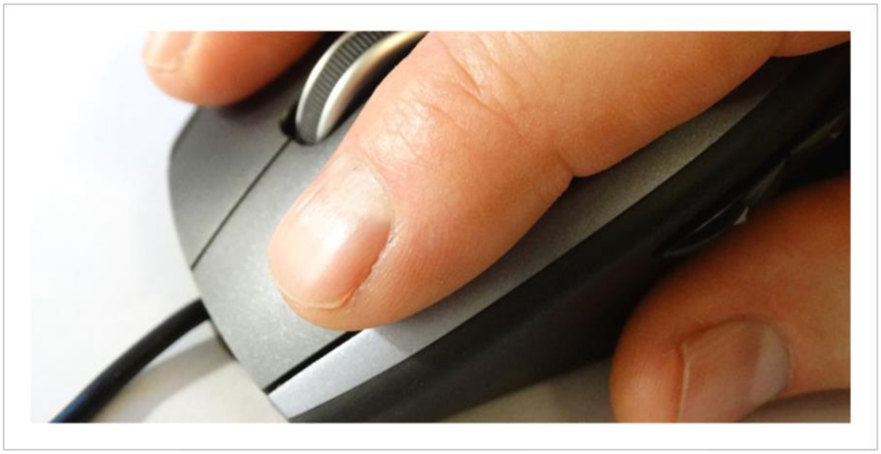
Having this bidding mechanism in place allows the market to decide how adverts are placed.

It's important to note that in the Google bidding system it's not always as simple as paying more to get the top spot. There are other factors at play, which this video explains:


Insights on the AdWords Auction
Show more useful ads in a higher position.

# WHAT IS CLICK FRAUD?

## WHAT'S ALL THE FUSS ABOUT?



Now that you understand how pay per click advertising works, it is much easier to understand what click fraud is.

Click fraud is due to advertisers being charged for every click on their ad, hence the model's name. In 2017 alone, about 1 in 5 clicks on adverts were fraudulent, with the number slowly increasing every month.

To put it simply, click fraud can be defined as:

**The fraudulent clicking of pay per click adverts to generate fraudulent charges for advertisers.**

Notice how the definition specifically mentions pay per click adverts. If the same fraudulent clicks took place on a different model, say a cost per impression model, then it would be completely different as advertisers are charged every per 1,000 views, regardless of how many clicks they get.

So how does click fraud work?

If we go back to the leaflet analogy, then it's the same as someone tearing down all your leaflets.

Since they've ran off with your leaflets, how is anybody else going to hear about your store? They're probably not unless you buy more leaflets which will cost you more money. If you do decide to buy more leaflets then what are the chances that the same person will come and take them all again?

As you can see, click fraud is a frustrating and demotivating problem.

Not only does click fraud drive up advertising costs for businesses, but it also skews analytical data which many companies rely on to make effective marketing decisions. Maybe you have a pay per click campaign with a really high converting and profitable keyword that delivers 80% of your sales. If that keyword suffers from regular click fraud without you being able to detect it, then from a marketing perspective you might decide to get rid of it. From looking at your data the click through rate would be extremely high, while the conversion rate would be extremely low. Since you get charged for every click, eventually the cost of the ad will outweigh the profit and you'll have to give up on it.

However, if you have sufficient data and monitor the keyword closely, then there is a good chance you would notice a change in performance, alerting you to the fact that something shady might be going on with that keyword.

Dig a little deeper, and you would notice multiple clicks from the same IP addresses or an influx of clicks from a high-risk country you don't even offer services in.

But who's doing this? Who exactly is responsible for these clicks, and what do they get out of sabotaging you?

# WHO’S RESPONSIBLE FOR CLICK FRAUD?

## A LOOK AT WHO’S CLICKING WHAT

Click fraud can take many forms. From accidental clicks by genuine customers, to serious underground fraud groups. Every industry and business is affected differently by click fraud, and there is never just 1 party responsible. To understand who might be fraudulently clicking your ads, we need to take a look at the 4 most common offenders.

### WHO’S RESPONSIBLE

1. Competitors
2. Webmasters
3. Disgruntled Customers
4. Fraud Rings

# 1. COMPETITORS

**Threat Level: 8/10**

**What they gain: A competitive advantage by wasting your PPC budget**

Responsible for the vast majority of click fraud

One of the most common culprits for click fraud is most certainly other businesses that compete on your terms. When it comes to pay per click advertising, everyone wants to be number 1.

No matter what keyword you're bidding on, there's a high chance you won't be the only person doing so. When other businesses compete for the same keyword, it can often turn into a ferocious battle.

Many businesses will run pay per click campaigns with a daily budget in place. Once this budget has been reached, the advert will turn itself off to stop anyone from clicking it. Since a lot of businesses do this with their campaigns, other businesses can take advantage.

By clicking competitor's ads, businesses can waste their advertising budget and turn the advert off for the day. If a business is currently in position 2 and can't afford to outbid position 1, then by repeatedly clicking the top advert they can waste their budget. Eventually, whoever was in position number 2 will take the top spot. This means extra clicks and extra traffic, all for free!

Although a daily budget spend is common for smaller businesses, some larger businesses won't use them. This means their adverts can often be subjected to a large amount of click fraud and financial loss. Most businesses who don't use daily budgets will usually be huge multinational companies worth billions, so it won't exactly affect them that much. However, it is still possible for them to lose thousands a day on click fraud.

As you can see, competitors have a strong motive to click on your ads. Not only does it waste your money and skew your data, but it also allows them to get more clicks with very little effort.

# 2. WEBMASTERS

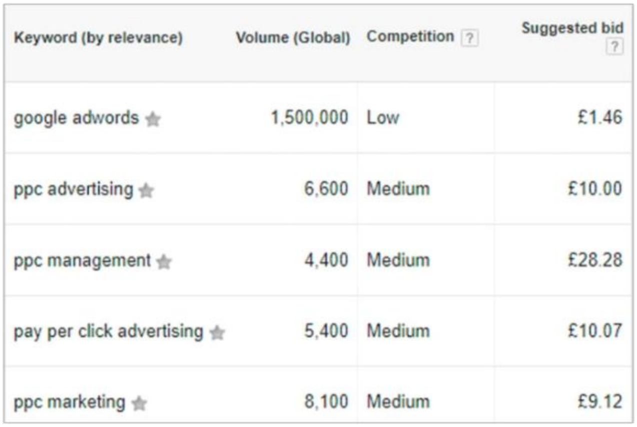
**Threat Level: 6/10**

**What they gain: More income from displaying ads on their website**

Only applicable to those that use Google's network display option.

If none of your competitors are trying to take advantage of your pay per click campaigns, then there is a high chance that certain webmasters will be.

Almost any webmaster is allowed to display Google ads on their website. They simply create an AdSense account and can start displaying ads immediately. For every person who clicks on their ad they get 68% of the amount paid to Google. As you can imagine, if a keyword costs £10 a click then that can be a lot of money for a webmaster, even if it's a just a few clicks a week. Take a look at these suggested bid prices for pay per click keywords.



| Keyword (by relevance) | Volume (Global) | Competition ? | Suggested bid ? |
|---|---|---|---|
| google adwords | 1,500,000 | Low | £1.46 |
| ppc advertising | 6,600 | Medium | £10.00 |
| ppc management | 4,400 | Medium | £28.28 |
| pay per click advertising | 5,400 | Medium | £10.07 |
| ppc marketing | 8,100 | Medium | £9.12 |

In order to make more money, a webmaster will require more clicks. Sadly, instead of spending time developing and growing their website, many webmasters can be tempted to click their own ads. These fraudulent clicks will still generate the same profit as the genuine clicks, but are much easier to obtain. This means many webmasters will purposely click their ads to give themselves a little bit more profit. This can often be identified by a huge increase in the click through rate of your display network ads.

Although this is a violation of Google's terms of service, there's no denying that it still happens.

However, webmasters only have an incentive to click ads on their own website. In order to make your advert appear on 3rd party websites, you need to enable the display network option. If you don't enable this, then your advert will only appear on Google's search engine and won't be subject to this kind of click fraud. It's basically a tradeoff, you get less traffic to your ads but also reduce the number of fraudulent clicks.

After reading this you might be tempted to stop using the Google display network. However, it's important to understand that this doesn't happen to everyone. Many webmasters will only target the expensive keywords, so if you're not bidding on any expensive keywords then you're likely to be safe.

# 3. DISGRUNTLED CUSTOMERS

**Threat Level: 4/10**

**What they gain: Revenge on the company through financial loss**

Can cause many problems, especially if you are bidding on expensive keywords

One of the least common causes of click fraud is often down to repeat customers who will click the same ad for a variety of different reasons. Sometimes a user will click an advert and then a few days later click the same advert again.

This might be down to the fact that they forgot the website or because it just happened to grab their attention again. Although this type of click fraud is rarely as malicious compared to some of the other reasons we've listed, it still costs businesses money. Ideally, you only want a customer to click your advert once and then convert, but this is often not the case. Sometimes it takes more than 1 click to convert a customer which will naturally increase your average conversion cost.

This type of click fraud is rare and not really worth worrying about, especially when there are other forms of click fraud which are more likely to harm a company's profits.

Let's face it, you can't please every customer. Some of them can hold petty grudges against companies for a long time, and If you run into a dissatisfied customer who knows a bit about pay per click, then they may purposely click the same advert to try and get back at you. This can seem like a strange and childish way to behave, but anyone who's worked in retail will tell you of the bitterness some people can possess.

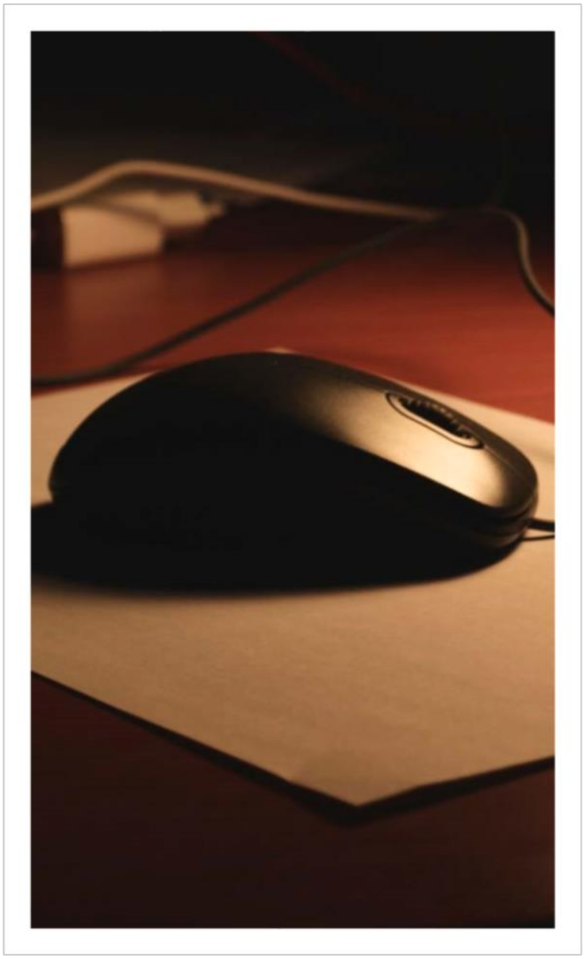
As stated above, this type of click fraud doesn't occur regularly. In order for a customer to do this they would need to understand how pay per click works, which instantly rules out a lot of people. The chances of this ever happening to you is miniscule.

# 4. FRAUD RINGS

**Threat Level: 5/10**

**What they gain: Huge amounts of revenue**

Only target expensive keywords backed by big companies



The final and most serious offender of click fraud is fraud rings. These large groups of people specifically target certain ad networks in order to extract the most amount of money in the shortest time possible. Using a huge array of automated programs, the group can generate millions of fraudulent clicks and views per day.

In December 2016, the company White Ops, released a report exposing a huge fraud ring they dubbed “The Methbot Operation.” This Russian criminal fraud group are reportedly making $3 – $5 million per day from fraudulent clicks and fake views.

The Methbot operation works in a similar way to how webmasters click ads on their own website, but with the Methbot Operation it’s takes taken to an entirely new level. Using thousands of unique IP addresses and domain names, the group can simulate thousands of clicks and views every day on their ads.

According to the report, the average cost per mile (per 1,000 impressions) for these ads ranged from $3.27 to $36.72. Considering the group is faking up to 400 million views a day, that is a lot of dirty money.

The group was initially discovered in 2015 when White Ops noticed suspicious traffic affecting their clients ads. After investigating the source of the traffic, they quickly discovered over 852,992 unique IP addresses responsible for the operation. This led to constant monitoring of the network until they managed to piece together the entire fraud group.

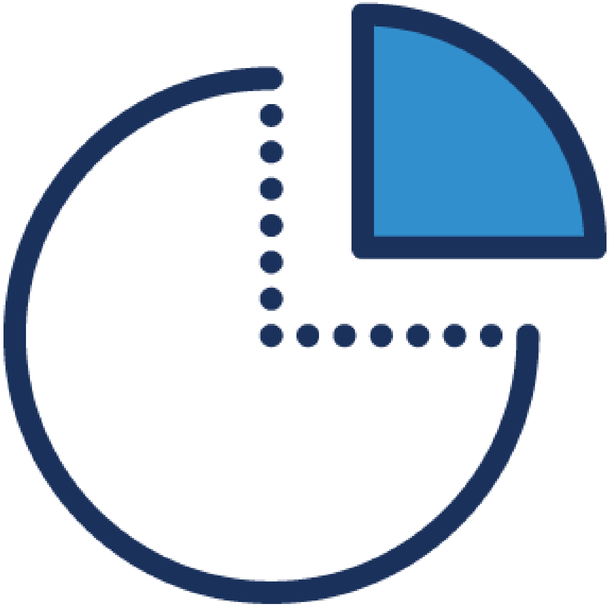
This was unlike any fraud groups which have been discovered in the past.  Not only was it much larger in scale, but it operated entirely differently.

Instead of relying solely on botnets to do the work, the network was built from scratch using unique IP addresses rented from other companies. The estimated cost of the vast amount of unique IP addresses alone is around $4 million. That is money most of us can only dream of, but when you're making that amount in a day it's pocket change.

Although the Method Bot Operation focuses primarily on video CPM ads, there is no doubt that there are other groups doing the same thing on pay per click ads.

Should this be a concern to you and your business? Not at all.

Currently, this is the biggest ad fraud group out there and they're focusing solely on impressions on video ads. This means if you're using pay per click ads then you won't be affected. Combine this with the fact that most fraudsters only target exceptionally expensive keywords and the chances are they'll never see your ads. You're much more likely to be the victim of click fraud from competitors and webmasters than from a fraud group.



# THE MOST AFFECTED INDUSTRIES

## WHO'S HIT THE HARDEST?

Now you know the parties responsible for click fraud, it's also important to understand which industries are affected the most.

From advertising to technology, every industry has its own unique differences, and when it comes to click fraud, there are clearly some industries that are more fraudulent than others.

This can be narrowed down to 2 main factors: the average cost per click and the amount of traffic.

If fraudsters want to click your ad undetected, then they want to make sure they are causing the most damage (or making the most money) while keeping under the radar. If you're in a competitive industry that receives millions of clicks per day then finding a few fraudulent clicks seem like a fruitless task.

Compare this to a much quieter industry with a lower cost per click, and the chance of click fraud is greatly reduced. Why would a fraud group target low cost per click ads when they can target much more expensive keywords with a higher payout?

## THE TOP 3 MOST AFFECTED INDUSTRIES

According to a click fraud report in 2015 by Bloomberg, the 3 most affected industries are:

| FINANCE | FAMILY | FOOD |
|---|---|---|
| 22% | 18% | 16% |
| of traffic is bot related | of traffic is bot related | of traffic is bot related |

What do all of these industries have in common?

Well for starters, they all have a relatively high cost per click. Finance is obviously a very competitive industry full of big mortgage advisors and financial companies. These companies have lots of money to throw around and aren't afraid to spend plenty of cash bidding on keywords. After all, everyone needs insurance, mortgages and personal loans, so there is always high demand for them.

Combine this with the fact that the search volume is relatively high for these industries, and they check all of the boxes for an easy click fraud target. By having expensive keywords and a huge amount of traffic to hide themselves in, it's no wonder these industries experience the most click fraud.

## THE 3 LEAST AFFECTED INDUSTRIES

Compare these categories to the 3 least affected industries and you'll notice some major differences:

| SPORT | SCIENCE | INFO |
|---|---|---|
| 3% | 3% | 2% |
| of traffic is bot related | of traffic is bot related | of traffic is bot related |

You'll notice these industries don't have expensive keywords. Out of the 3 industries above, sport is likely to have the most expensive keywords while info most certainly has the lowest.

After all, are website like Wikipedia going to pump millions into pay per click ads? The same applies to science websites. Since there are billion-dollar companies backing them the chances are they won't be paying much for click per click.

In addition to the keywords being relatively cheap, the search volume is also low compared to other industries. Both of these factors make these industries unsuitable for click fraud.

Not only are they unlikely to run ads, but when they do the cost per click is extremely low. Some click fraud might happen from certain webmasters with ads on their site, but if you were a fraud group then it's likely you'd pick a more profitable industry.

# WHAT ARE PPC NETWORKS DOING TO STOP IT?

## THE ANSWER IS CONCERNING

In order to combat the rise of click fraud, many pay per click networks have developed their own systems to detect fraudulent clicks. The biggest pay per click network of them all, Google AdWords, has its own traffic quality center that helps reimburse users who suffer from fraudulent clicks.

The center, known as the ad quality center, tracks all the clicks for every ad in Google's large network. If for whatever reason the system detects suspicious behavior, then it will automatically refund the cost of the click back to the advertiser. From an advertiser's perspective, this is a great feature. Not only are your ads being constantly monitored for click fraud, but if the system detects fraud, then it will automatically refund you. This leaves the advertiser happy and gives Google a better reputation, letting people know they only allow high quality traffic in their network.

> "THIS SYSTEM SOUNDS GREAT DOESN'T IT? WELL IN REALITY, IT'S NOWHERE NEAR AS GOOD."

This system sounds great doesn't it? Well in reality, it's nowhere near as good.

The main problem is the automated detection system doesn't catch all of the fraudulent clicks, which means click fraud still occurs. Considering the amount of time and effort fraudsters put into their click fraud campaigns it can be exceptionally hard to identify every fraudulent click.

The automated programs and robots used by fraudsters are getting more and more advanced every with every day that passes. In fact, some software is so advanced that it can perfectly simulate a user's click while avoiding detection. This means after going through the entire detection process; some users will still be charged for fraudulent clicks.

With this in mind, some advertisers invest a lot of money into investigating their pay per click traffic and checking if it is genuine or not. If they do discover a user spam clicking on their ads and it's not being picked up by Google's system, then they can always report them to Google.

Google then receives the report and will check all the evidence to determine if it was deemed an invalid click. If there is enough evidence to suggest it is, then the amount taken for that click will be refunded back to the advertiser's account.

This means that although Google's system might not be able to detect every fraudulent click, if you can gather enough evidence then you can get your money back.

With that covered, let's get into how  you manually check your traffic for suspected fraudsters.

# IS CLICK FRAUD LEGAL?

## LET’S EXPLORE THE LEGAL ASPECT

One of the first things that often springs to mind when you think about click fraud is the legality of it. Other forms of fraud such as credit card and identity fraud are most certainly illegal and are punishable by up to 25 years in jail. But what about click fraud? Has anyone ever gone to jail over it?

Just like any crime, click fraud requires a lot of investigation to determine who the culprit is. Sometimes small amounts of click fraud often go unnoticed and are not picked up on. Other times the amount lost by the fraud itself is not worth the costs of extensive legal action. This means that the authorities often only target the biggest fraudsters that affect multiples businesses and industries. These groups have been around for so long that monitoring them and gathering evidence is fairly easy. This is essential information authorities need to collect in order to press charges. Although not everyone who commits click fraud will get discovered or charged, the repeat offenders who do it on a large scale are much more likely to end up in trouble with the law.

The Estonian gang leader Vladimir Tsastin was jailed in the US for running an international fraud group which amassed over $14 million in fraudulent activities. After the FBI discovered his scheme in 2009, Tsastin was arrested in in 2011. Upon being found guilty of money-laundering charges, Tsastin was extradited to the US in 2014 to face charges of wire fraud and computer intrusion.

The scheme Tsastin ran was an online fraud ring that used millions of computers to click on advertiser's ads fraudulently. The gang disguised themselves as publishing companies that had agreements with advertising brokers. They would publish advertiser's content on their website, promising that they would receive lots of clicks.

And in fairness they did receive a lot of clicks, but little did the advertisers know that they were completely fake and came from computers infected by malware that the gang created.

By hijacking these unsuspecting users, large amounts of traffic could be directed to web pages that had the adverts on. This allowed the gang to carry out hard to detect fraudulent clicks which made them rich.

To date, Vladimir Tsastin is the only person to have been jailed on click fraud related charges. However, this doesn't mean that jail time is the only way to punish fraudsters.

When a company is responsible for click fraud, then it is usually the entire company that faces the charges and not a specific individual. This means that most click fraud cases are often settled by lawsuits between advertisers and suspected companies who are behind the fraud.

> "NEARLY 20% OF TOTAL DIGITAL AD SPEND WAS WASTED IN 2016 DUE TO AD FRAUD"

In one case, Google sued the Texas company Auction Experts on suspicion of paying people to click on ads that appeared on their website. Overall Google estimated they had cost advertisers around $50,000 due to their click fraud scheme and eventually won $75,000 from the company in 2005. Although, this was a long time ago and today click fraud happens on a much larger scale. Not only are there more cases of fraud, but the offenders are also harder to track.

Google have received some criticism for click fraud, and an interesting case arose in March 2006, when Lane’s Gifts and Collectibles sued Google themselves for not doing enough to stop click fraud. After a long trial, Google agreed to pay a $90 million settlement fund to the company for their financial loss. Despite this large payout, Google still maintained that they had a great reimbursement system, and that any advertiser could request an investigation into suspicious clicks.

Since the lawsuit, Google has put more effort and money into ensuring clicks and traffic are of the highest quality. This is obviously a welcomed improvement, but with fraudsters coming up with new ways to avoid detection every day, it’s a constant uphill battle.

# HOW TO IDENTIFY CLICK FRAUD YOURSELF

## THIS MAY GET COMPLICATED

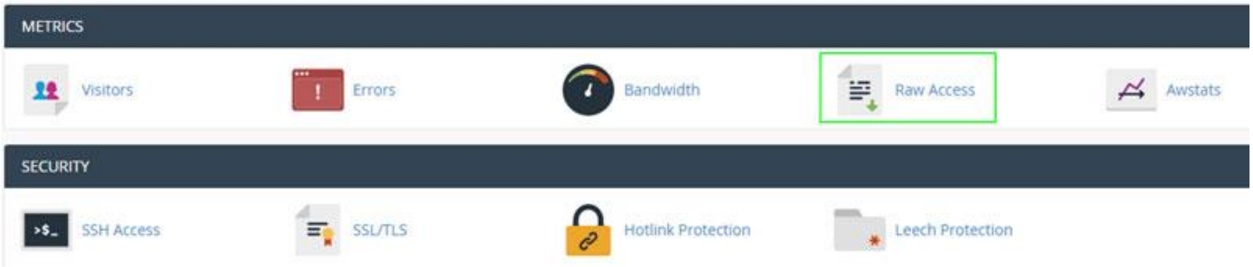
Now you understand the foundations of click fraud and what it is, how can you check your own campaign to see if you've been the victim of it?

Before you can analyze your traffic to see where it is coming from, you first need to collect enough data from your pay per click campaigns. This step can be fairly tricky. As part of Google's privacy policy, there is no way to identify users through AdWords using their IP address. Instead, you'll need to work backwards from the people who have visited your website.

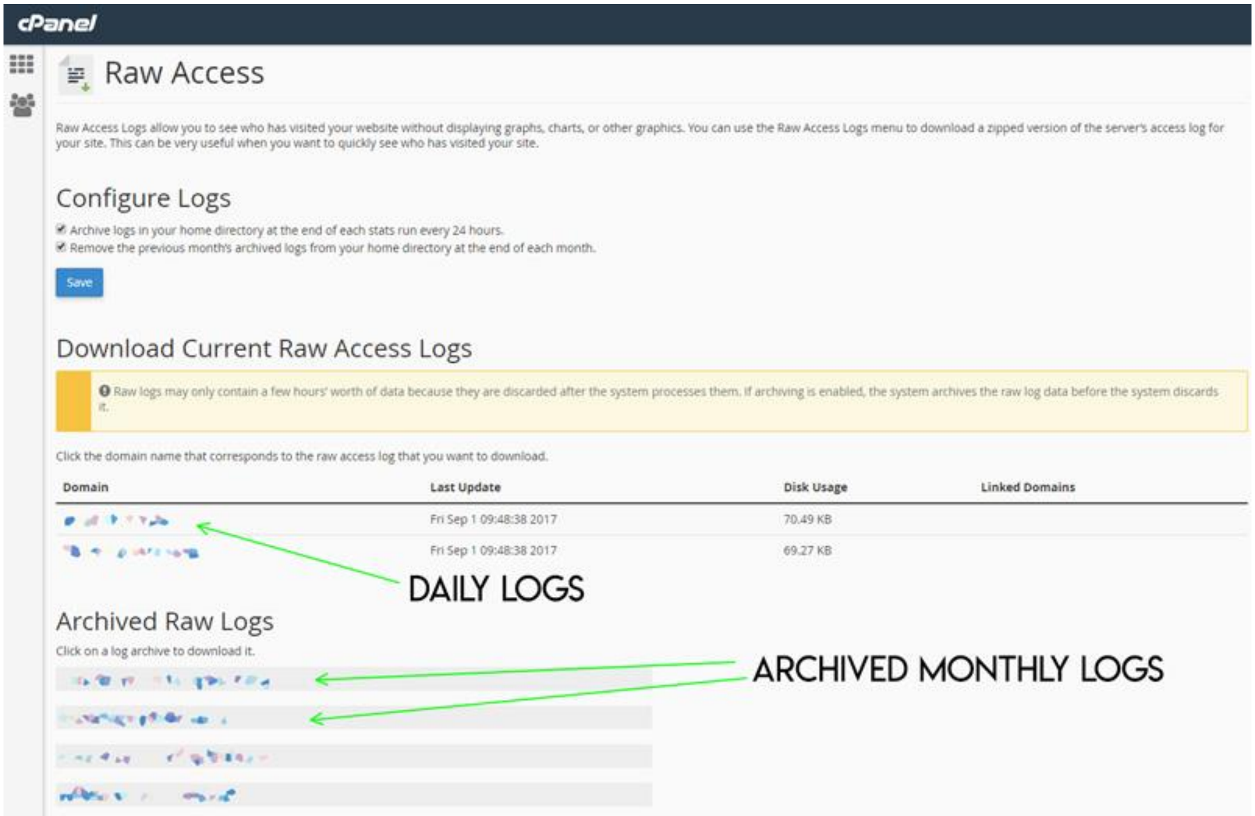
To find out who has visited your website you need to pull up your server logs. Depending on what web host and setup you have, this can be found in a few ways.

If you're using the popular cPanel platform on your server, then getting the list of IP addresses is relatively easy. If you're not using cPanel, then you'll have to Google around to find out how to obtain them.

Head on over to the main cPanel homepage and scroll down to the metrics tab. You'll notice a Raw Access section like in the picture below.



After clicking the Raw Access button you'll be direct to a new page where you can download the data.



Raw Access

Raw Access Logs allow you to see who has visited your website without displaying graphs, charts, or other graphics. You can use the Raw Access Logs menu to download a zipped version of the server's access log for your site. This can be very useful when you want to quickly see who has visited your site.

Configure Logs

☑ Archive logs in your home directory at the end of each stats run every 24 hours.
☑ Remove the previous month's archived logs from your home directory at the end of each month.

Save

Download Current Raw Access Logs

Raw logs may only contain a few hours' worth of data because they are discarded after the system processes them. If archiving is enabled, the system archives the raw log data before the system discards it.

Click the domain name that corresponds to the raw access log that you want to download.

| Domain | Last Update | Disk Usage | Linked Domains |
|---|---|---|---|
| [redacted] | Fri Sep 1 09:48:38 2017 | 70.49 KB | |
| [redacted] | Fri Sep 1 09:48:38 2017 | 69.27 KB | |

DAILY LOGS

Archived Raw Logs

Click on a log archive to download it.

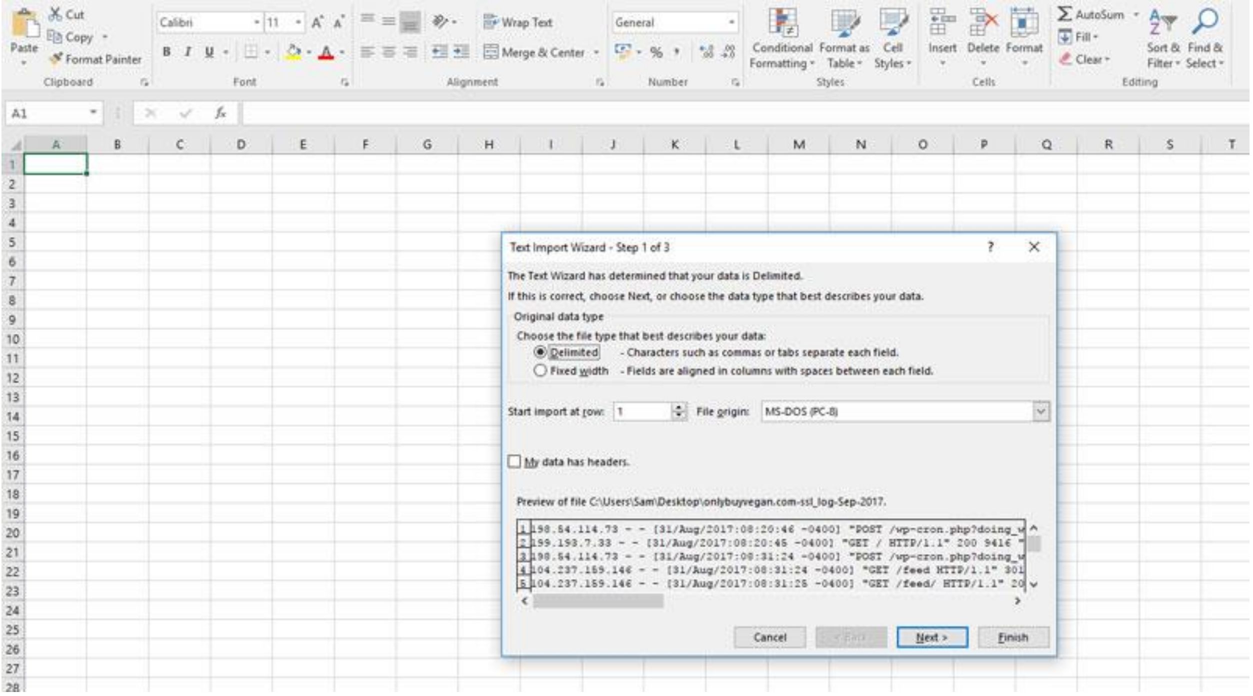
[redacted]

ARCHIVED MONTHLY LOGS

As you can see from the screenshot above there are 2 sections; daily logs, and monthly logs. You'll most likely want to be downloading the monthly logs as it will give you plenty of data to work with.

Upon downloading the logs, you'll need to extract the file to your desktop or somewhere you plan on keeping them. You might need to download several months of data logs in the future so make sure it's somewhere you'll remember. The file itself won't open on its own due to the extension, so to open it you'll have to import it to Microsoft Excel.

If you open the file in Excel, you'll be greeted with the import screen below.



Text Import Wizard - Step 1 of 3

The Text Wizard has determined that your data is Delimited.

If this is correct, choose Next, or choose the data type that best describes your data.

Original data type

Choose the file type that best describes your data:

● Delimited - Characters such as commas or tabs separate each field.

○ Fixed width - Fields are aligned in columns with spaces between each field.

Start import at row: 1 File origin: MS-DOS (PC-8)

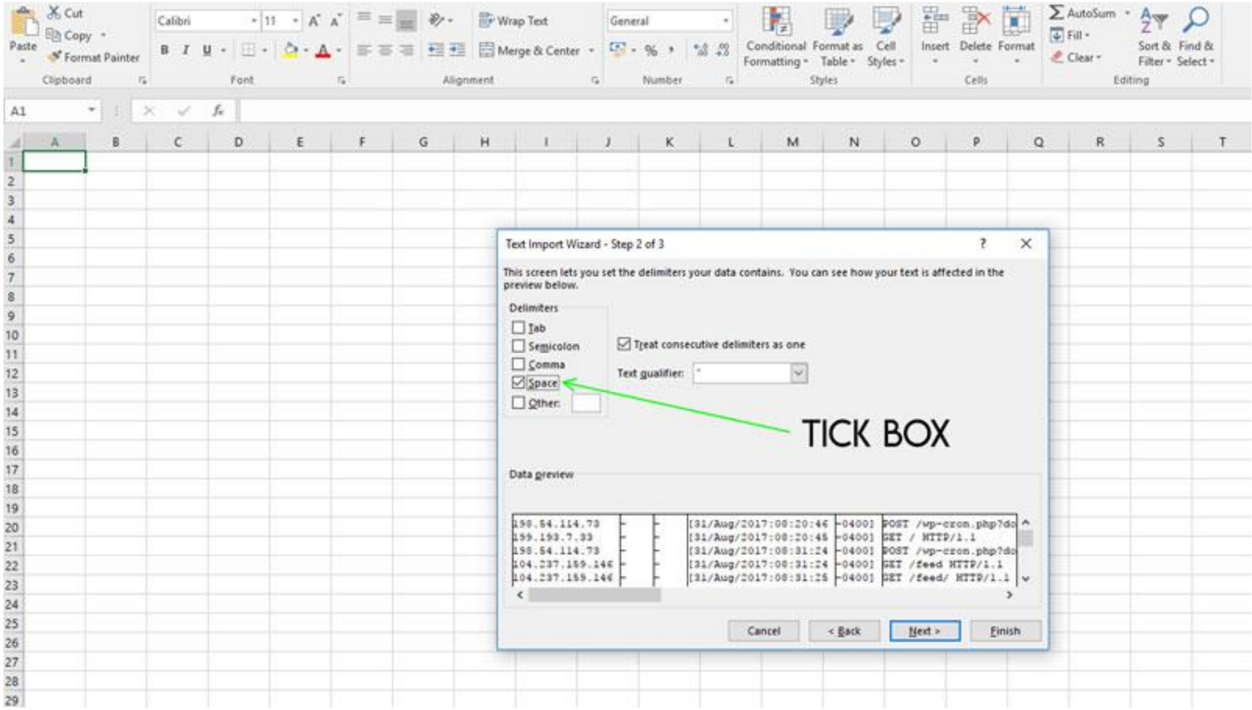
□ My data has headers.

Preview of file C:\Users\Sam\Desktop\onlybuyvegan.com-ssl_log-Sep-2017.

```
1 198.54.114.73 - - [31/Aug/2017:08:20:46 -0400] "POST /wp-cron.php?doing_w
2 199.193.7.33 - - [31/Aug/2017:08:20:45 -0400] "GET / HTTP/1.1" 200 9416 "
3 198.54.114.73 - - [31/Aug/2017:08:31:24 -0400] "POST /wp-cron.php?doing_w
4 104.237.159.146 - - [31/Aug/2017:08:31:24 -0400] "GET /feed HTTP/1.1" 301
5 104.237.159.146 - - [31/Aug/2017:08:31:26 -0400] "GET /feed/ HTTP/1.1" 20
```

You'll get a preview of the data below so you know it's the right file you've selected. The first column on the left should have all the IP addresses from the file.

Press the next button at the bottom to move to the next screen.



Text Import Wizard - Step 2 of 3

This screen lets you set the delimiters your data contains. You can see how your text is affected in the preview below.

Delimiters

- □ Tab
- □ Semicolon
- □ Comma
- ☑ Space
- □ Other:

☑ Treat consecutive delimiters as one

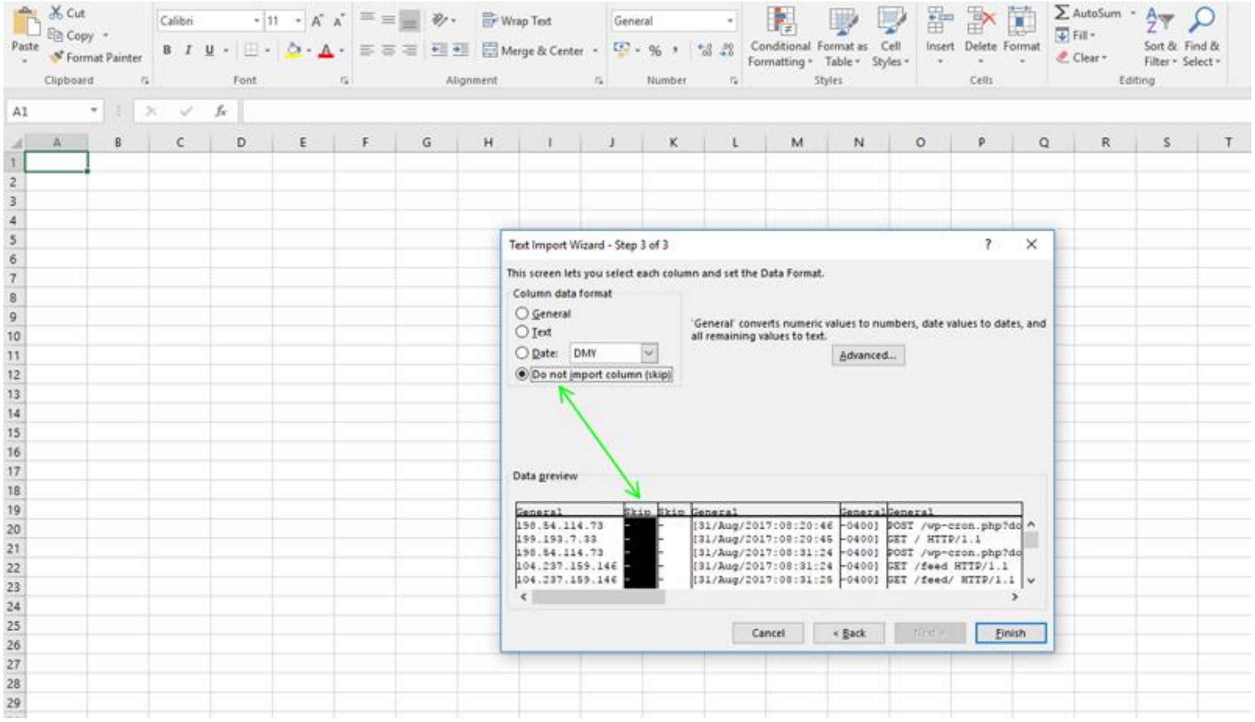
Text qualifier: "

TICK BOX

Data preview

```
198.54.114.73   -  -  [31/Aug/2017:08:20:46  -0400]  POST /wp-cron.php?do
199.193.7.33    -  -  [31/Aug/2017:08:20:45  -0400]  GET / HTTP/1.1
198.54.114.73   -  -  [31/Aug/2017:08:31:24  -0400]  POST /wp-cron.php?do
104.237.159.146 -  -  [31/Aug/2017:08:31:24  -0400]  GET /feed HTTP/1.1
104.237.159.146 -  -  [31/Aug/2017:08:31:25  -0400]  GET /feed/ HTTP/1.1
```

This screen lets you choose how Excel will import the data. You'll want to make sure you select the space delimiter as that's how the standard log file is formatted. Excel will give you a preview of the data below on how it's going to be imported. The data should be split into separate columns as shown in the picture above.



Text Import Wizard - Step 3 of 3

This screen lets you select each column and set the Data Format.

Column data format

- ○ General
- ○ Text
- ○ Date: DMY
- ● Do not import column (skip)

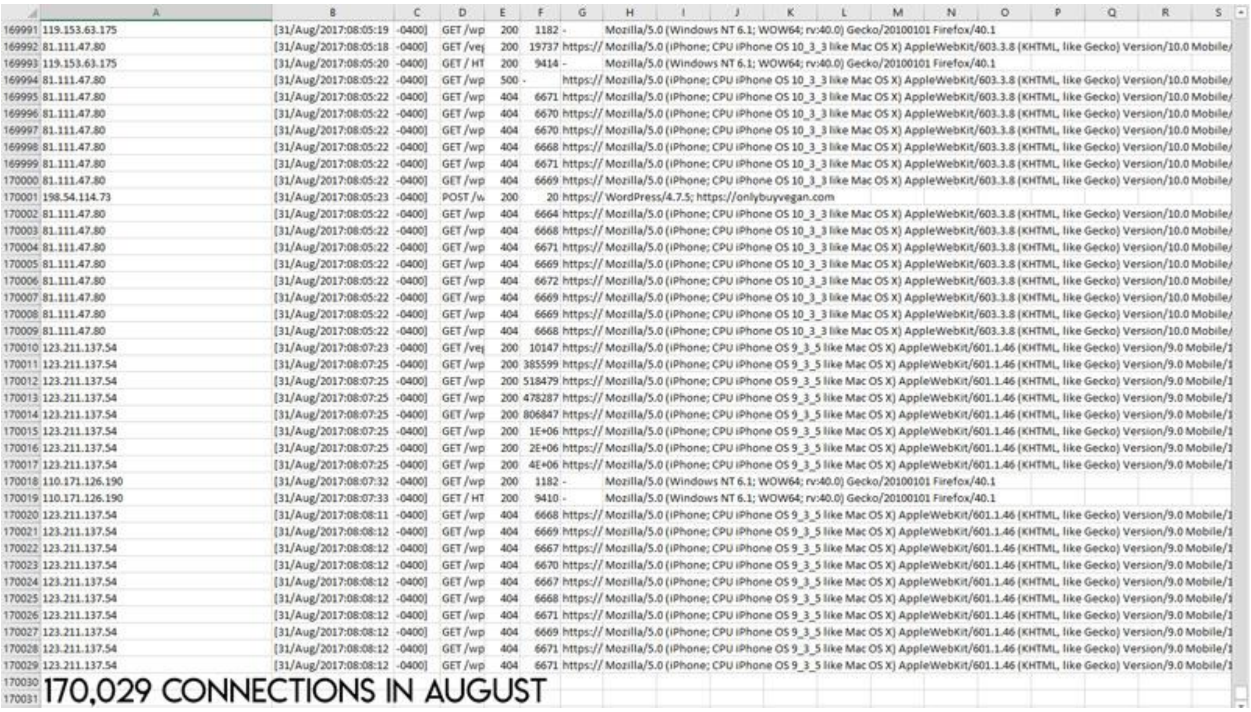
'General' converts numeric values to numbers, date values to dates, and all remaining values to text.

Data preview

```
General         Skip Skip General               General General
198.54.114.73   -    -    [31/Aug/2017:08:20:46 -0400]  POST /wp-cron.php?do
199.193.7.33    -    -    [31/Aug/2017:08:20:45 -0400]  GET / HTTP/1.1
198.54.114.73   -    -    [31/Aug/2017:08:31:24 -0400]  POST /wp-cron.php?do
104.237.159.146 -    -    [31/Aug/2017:08:31:24 -0400]  GET /feed HTTP/1.1
104.237.159.146 -    -    [31/Aug/2017:08:31:25 -0400]  GET /feed/ HTTP/1.1
```

On step 3 of the import wizard, you'll want to get rid of the columns that don't have any information. In this case, it will mainly be columns 2 and 3 as they don't contain any useful data at all. To do this, select the column in the preview window and select the Do not import column (skip) radio button, as shown in the image above.

After pressing finish, Excel will load all the data into their own columns and you'll be left with something that resembles this:



| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 169991 | 119.153.63.175 | [31/Aug/2017:08:05:19 | -0400] | GET /wp | 200 | 1182 | - | Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1 |
| 169992 | 81.111.47.80 | [31/Aug/2017:08:05:18 | -0400] | GET /ve| | 200 | 19737 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 169993 | 119.153.63.175 | [31/Aug/2017:08:05:20 | -0400] | GET / HT | 200 | 9414 | - | Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1 |
| 169994 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 500 | - | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 169995 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6671 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 169996 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6670 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 169997 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6670 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 169998 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6668 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 169999 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6671 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 170000 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6669 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 170001 | 198.54.114.73 | [31/Aug/2017:08:05:23 | -0400] | POST /w. | 200 | 20 | https:// | WordPress/4.7.5; https://onlybuyvegan.com |
| 170002 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6664 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 170003 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6668 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 170004 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6671 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 170005 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6669 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 170006 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6672 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 170007 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6669 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 170008 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6669 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 170009 | 81.111.47.80 | [31/Aug/2017:08:05:22 | -0400] | GET /wp | 404 | 6668 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 10_3_3 like Mac OS X) AppleWebKit/603.3.8 (KHTML, like Gecko) Version/10.0 Mobile/ |
| 170010 | 123.211.137.54 | [31/Aug/2017:08:07:23 | -0400] | GET /ve| | 200 | 10147 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170011 | 123.211.137.54 | [31/Aug/2017:08:07:25 | -0400] | GET /wp | 200 | 385599 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170012 | 123.211.137.54 | [31/Aug/2017:08:07:25 | -0400] | GET /wp | 200 | 518479 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170013 | 123.211.137.54 | [31/Aug/2017:08:07:25 | -0400] | GET /wp | 200 | 478287 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170014 | 123.211.137.54 | [31/Aug/2017:08:07:25 | -0400] | GET /wp | 200 | 806847 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170015 | 123.211.137.54 | [31/Aug/2017:08:07:25 | -0400] | GET /wp | 200 | 1E+06 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170016 | 123.211.137.54 | [31/Aug/2017:08:07:25 | -0400] | GET /wp | 200 | 2E+06 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170017 | 123.211.137.54 | [31/Aug/2017:08:07:25 | -0400] | GET /wp | 200 | 4E+06 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170018 | 110.171.126.190 | [31/Aug/2017:08:07:32 | -0400] | GET /wp | 200 | 1182 | - | Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1 |
| 170019 | 110.171.126.190 | [31/Aug/2017:08:07:33 | -0400] | GET / HT | 200 | 9410 | - | Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1 |
| 170020 | 123.211.137.54 | [31/Aug/2017:08:08:11 | -0400] | GET /wp | 404 | 6668 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170021 | 123.211.137.54 | [31/Aug/2017:08:08:12 | -0400] | GET /wp | 404 | 6669 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170022 | 123.211.137.54 | [31/Aug/2017:08:08:12 | -0400] | GET /wp | 404 | 6667 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170023 | 123.211.137.54 | [31/Aug/2017:08:08:12 | -0400] | GET /wp | 404 | 6670 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170024 | 123.211.137.54 | [31/Aug/2017:08:08:12 | -0400] | GET /wp | 404 | 6667 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170025 | 123.211.137.54 | [31/Aug/2017:08:08:12 | -0400] | GET /wp | 404 | 6668 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170026 | 123.211.137.54 | [31/Aug/2017:08:08:12 | -0400] | GET /wp | 404 | 6671 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170027 | 123.211.137.54 | [31/Aug/2017:08:08:12 | -0400] | GET /wp | 404 | 6669 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170028 | 123.211.137.54 | [31/Aug/2017:08:08:12 | -0400] | GET /wp | 404 | 6671 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170029 | 123.211.137.54 | [31/Aug/2017:08:08:12 | -0400] | GET /wp | 404 | 6671 | https:// | Mozilla/5.0 (iPhone; CPU iPhone OS 9_3_5 like Mac OS X) AppleWebKit/601.1.46 (KHTML, like Gecko) Version/9.0 Mobile/1 |
| 170030 | | | | | | | | |
| 170031 | | | | | | | | |

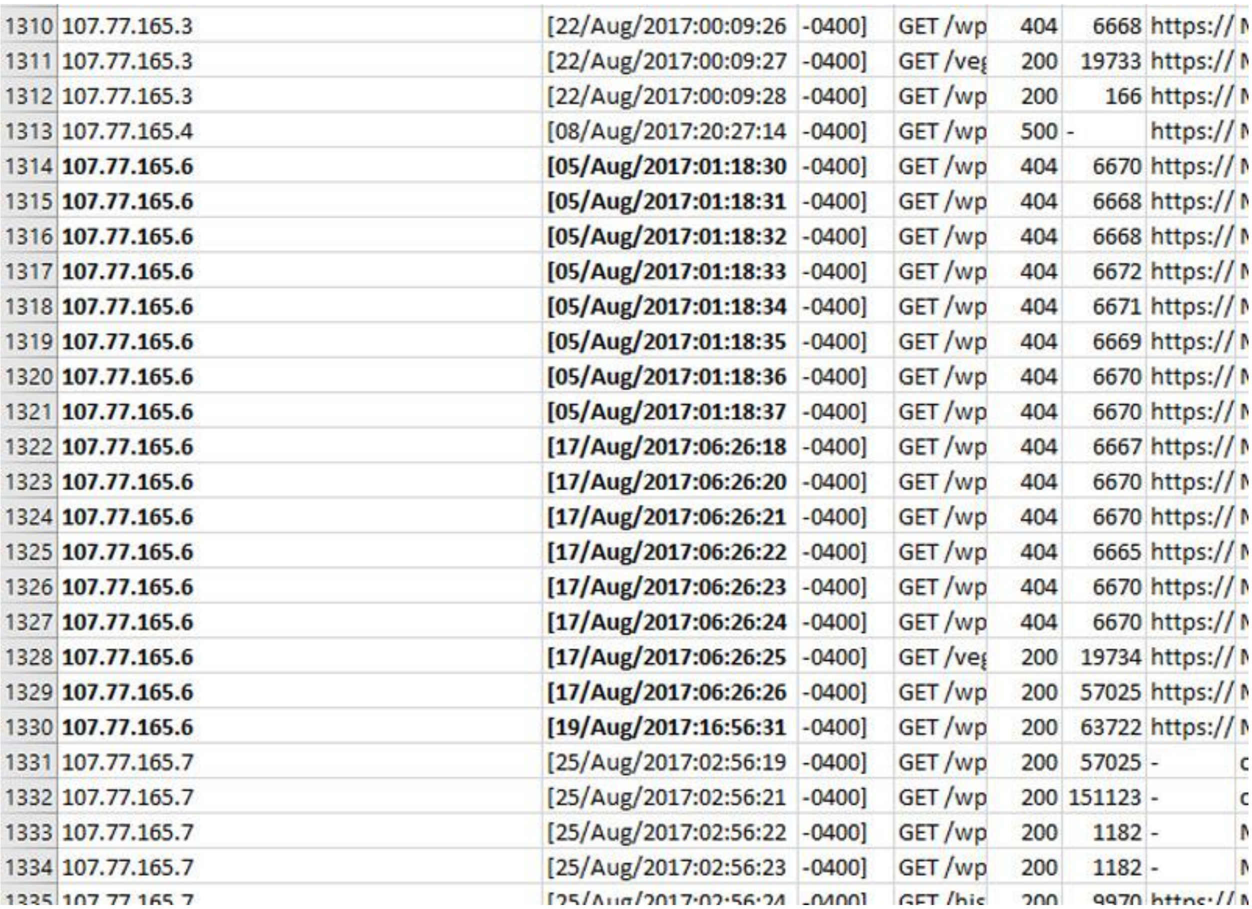
170,029 CONNECTIONS IN AUGUST

As you can see, in this example our log file has over 170,000 connections in August alone. If you have a big website, then this could easily be in the millions or more.

Now you've got the data imported into Excel; it's time to try and identify some offenders. Start off by selecting the first column A and sorting it from A to Z, if a new window pops up be sure to tick expand selection. This arranges the IP addresses in numerical order which makes it much easier to work with.

Now comes the hard part.

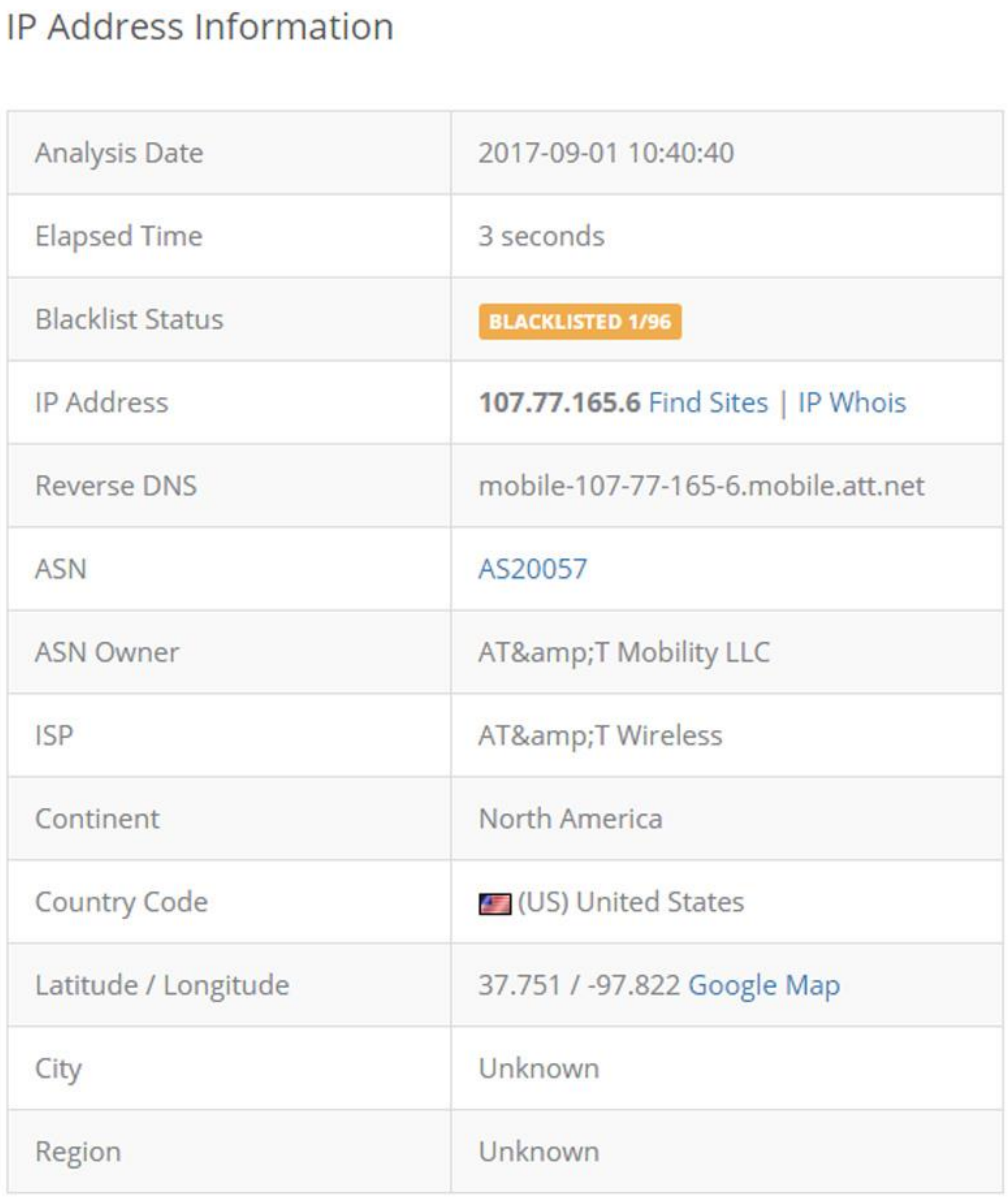
You need to look for IP addresses that visit your website on a regular basis, preferably at least 3 or more times within a month. Now these may be regular users, but for now we are just finding suspected fraudsters, the next stage is to see if there is enough evidence to back up the claim.



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 1310 | 107.77.165.3 | [22/Aug/2017:00:09:26 | -0400] | GET /wp | 404 | 6668 | https:// | N |
| 1311 | 107.77.165.3 | [22/Aug/2017:00:09:27 | -0400] | GET /veg | 200 | 19733 | https:// | N |
| 1312 | 107.77.165.3 | [22/Aug/2017:00:09:28 | -0400] | GET /wp | 200 | 166 | https:// | N |
| 1313 | 107.77.165.4 | [08/Aug/2017:20:27:14 | -0400] | GET /wp | 500 | - | https:// | N |
| 1314 | **107.77.165.6** | **[05/Aug/2017:01:18:30** | -0400] | GET /wp | 404 | 6670 | https:// | N |
| 1315 | **107.77.165.6** | **[05/Aug/2017:01:18:31** | -0400] | GET /wp | 404 | 6668 | https:// | N |
| 1316 | **107.77.165.6** | **[05/Aug/2017:01:18:32** | -0400] | GET /wp | 404 | 6668 | https:// | N |
| 1317 | **107.77.165.6** | **[05/Aug/2017:01:18:33** | -0400] | GET /wp | 404 | 6672 | https:// | N |
| 1318 | **107.77.165.6** | **[05/Aug/2017:01:18:34** | -0400] | GET /wp | 404 | 6671 | https:// | N |
| 1319 | **107.77.165.6** | **[05/Aug/2017:01:18:35** | -0400] | GET /wp | 404 | 6669 | https:// | N |
| 1320 | **107.77.165.6** | **[05/Aug/2017:01:18:36** | -0400] | GET /wp | 404 | 6670 | https:// | N |
| 1321 | **107.77.165.6** | **[05/Aug/2017:01:18:37** | -0400] | GET /wp | 404 | 6670 | https:// | N |
| 1322 | **107.77.165.6** | **[17/Aug/2017:06:26:18** | -0400] | GET /wp | 404 | 6667 | https:// | N |
| 1323 | **107.77.165.6** | **[17/Aug/2017:06:26:20** | -0400] | GET /wp | 404 | 6670 | https:// | N |
| 1324 | **107.77.165.6** | **[17/Aug/2017:06:26:21** | -0400] | GET /wp | 404 | 6670 | https:// | N |
| 1325 | **107.77.165.6** | **[17/Aug/2017:06:26:22** | -0400] | GET /wp | 404 | 6665 | https:// | N |
| 1326 | **107.77.165.6** | **[17/Aug/2017:06:26:23** | -0400] | GET /wp | 404 | 6670 | https:// | N |
| 1327 | **107.77.165.6** | **[17/Aug/2017:06:26:24** | -0400] | GET /wp | 404 | 6670 | https:// | N |
| 1328 | **107.77.165.6** | **[17/Aug/2017:06:26:25** | -0400] | GET /veg | 200 | 19734 | https:// | N |
| 1329 | **107.77.165.6** | **[17/Aug/2017:06:26:26** | -0400] | GET /wp | 200 | 57025 | https:// | N |
| 1330 | **107.77.165.6** | **[19/Aug/2017:16:56:31** | -0400] | GET /wp | 200 | 63722 | https:// | N |
| 1331 | 107.77.165.7 | [25/Aug/2017:02:56:19 | -0400] | GET /wp | 200 | 57025 | - | c |
| 1332 | 107.77.165.7 | [25/Aug/2017:02:56:21 | -0400] | GET /wp | 200 | 151123 | - | c |
| 1333 | 107.77.165.7 | [25/Aug/2017:02:56:22 | -0400] | GET /wp | 200 | 1182 | - | N |
| 1334 | 107.77.165.7 | [25/Aug/2017:02:56:23 | -0400] | GET /wp | 200 | 1182 | - | N |
| 1335 | 107.77.165.7 | [25/Aug/2017:02:56:24 | -0400] | GET /his | 200 | 9970 | https:// | N |

From looking at the screenshot above, you can see that we have identified a repeat visitor. This user has connected to our website on 3 different days through the same month. Either they really love our website and its content, or they are up to something suspicious. You might be thinking: How do I know if this user came directly to my website or through of paid advert? Unfortunately, as Google does not reveal users IP addresses it is pretty much impossible to tell. However, if an IP address does come back as being suspicious and blacklisted, then the chances are you'll want them blocked from seeing your ads anyway.

Now we've you a suspected fraudsters IP address, it's time to head on over to IPAvoid.com and do some research on the address. This tool is great for giving information about a user from their country to ISP and if they're blacklisted. All important information when it comes down to gathering evidence.



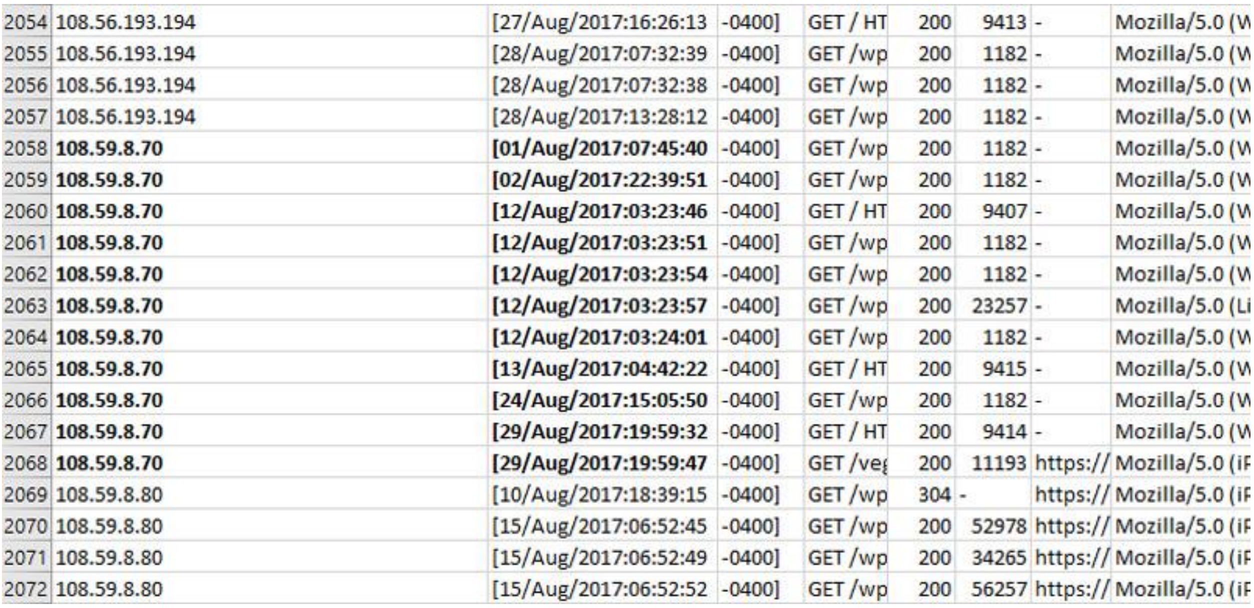
## IP Address Information

| | |
|---|---|
| Analysis Date | 2017-09-01 10:40:40 |
| Elapsed Time | 3 seconds |
| Blacklist Status | BLACKLISTED 1/96 |
| IP Address | **107.77.165.6** Find Sites \| IP Whois |
| Reverse DNS | mobile-107-77-165-6.mobile.att.net |
| ASN | AS20057 |
| ASN Owner | AT&amp;T Mobility LLC |
| ISP | AT&amp;T Wireless |
| Continent | North America |
| Country Code | (US) United States |
| Latitude / Longitude | 37.751 / -97.822 Google Map |
| City | Unknown |
| Region | Unknown |

After entering the IP address into the blacklist checker, the results bring back some interesting information. As you can see, the IP address is actually blacklisted by 1 checker out of 96. Not a huge amount, but usually users need to have a reputation as spammers or do something fraudulent to get on one of those lists. The more important detail from the results is that the mobile company AT&T actually uses this IP address. This means that it's not just 1 user using this address, in fact it could be thousands or millions.

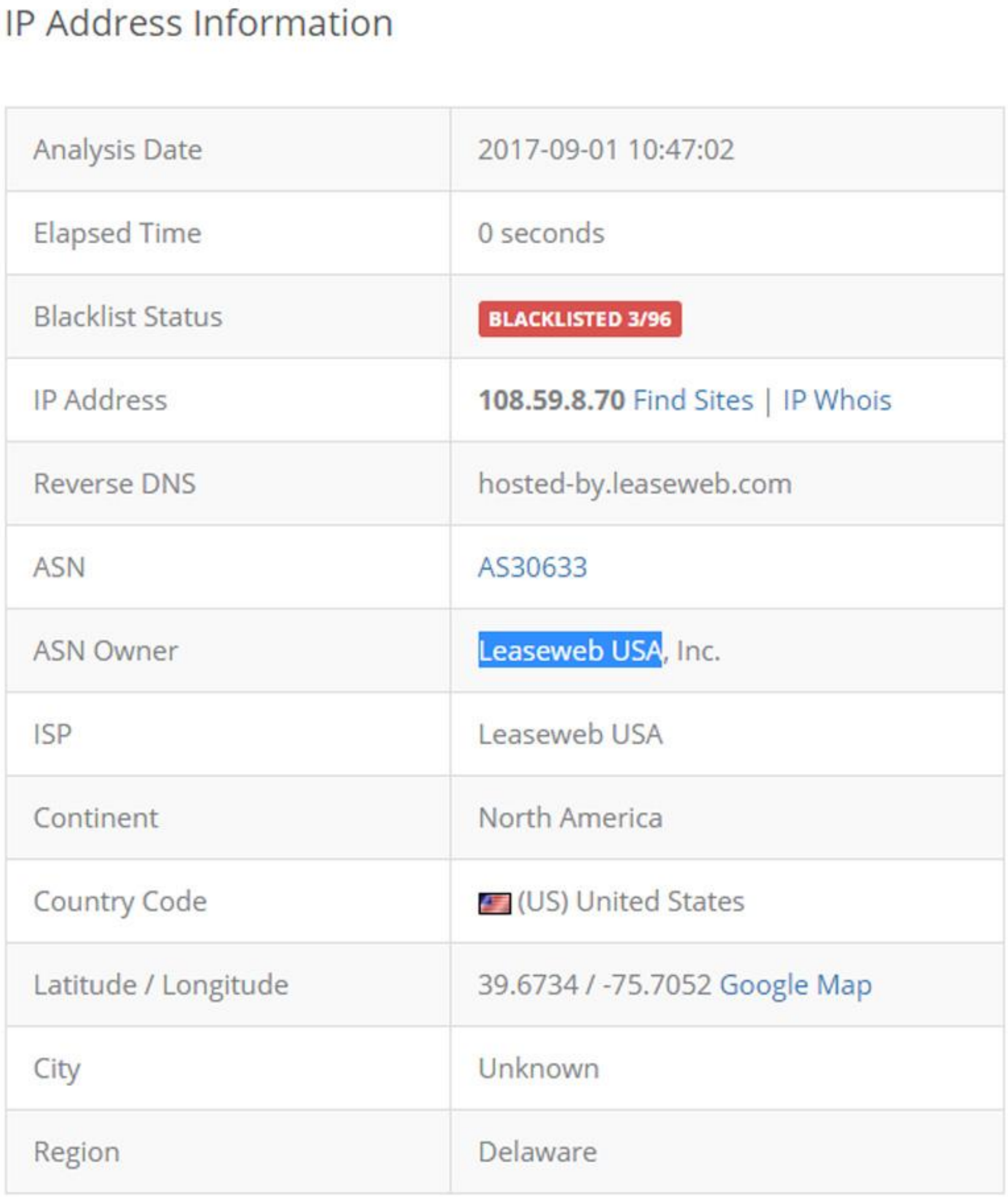
This brings up an important question: Should you block this IP address from seeing your ads if you could potentially block thousands of people?

In this example, it's probably best to leave it unblocked. Sure, the IP address is blacklisted but it's only 1 out of 96. If it was say, 50 out of 96 then it might be worthwhile doing so. However, the amount of potential users you could stop from seeing your ad by blocking this IP is not worth it.



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 2054 | 108.56.193.194 | [27/Aug/2017:16:26:13 | -0400] | GET / HT | 200 | 9413 | - | Mozilla/5.0 (W |
| 2055 | 108.56.193.194 | [28/Aug/2017:07:32:39 | -0400] | GET /wp | 200 | 1182 | - | Mozilla/5.0 (W |
| 2056 | 108.56.193.194 | [28/Aug/2017:07:32:38 | -0400] | GET /wp | 200 | 1182 | - | Mozilla/5.0 (W |
| 2057 | 108.56.193.194 | [28/Aug/2017:13:28:12 | -0400] | GET /wp | 200 | 1182 | - | Mozilla/5.0 (W |
| 2058 | **108.59.8.70** | **[01/Aug/2017:07:45:40** | -0400] | GET /wp | 200 | 1182 | - | Mozilla/5.0 (W |
| 2059 | **108.59.8.70** | **[02/Aug/2017:22:39:51** | -0400] | GET /wp | 200 | 1182 | - | Mozilla/5.0 (W |
| 2060 | **108.59.8.70** | **[12/Aug/2017:03:23:46** | -0400] | GET / HT | 200 | 9407 | - | Mozilla/5.0 (W |
| 2061 | **108.59.8.70** | **[12/Aug/2017:03:23:51** | -0400] | GET /wp | 200 | 1182 | - | Mozilla/5.0 (W |
| 2062 | **108.59.8.70** | **[12/Aug/2017:03:23:54** | -0400] | GET /wp | 200 | 1182 | - | Mozilla/5.0 (W |
| 2063 | **108.59.8.70** | **[12/Aug/2017:03:23:57** | -0400] | GET /wp | 200 | 23257 | - | Mozilla/5.0 (Li |
| 2064 | **108.59.8.70** | **[12/Aug/2017:03:24:01** | -0400] | GET /wp | 200 | 1182 | - | Mozilla/5.0 (W |
| 2065 | **108.59.8.70** | **[13/Aug/2017:04:42:22** | -0400] | GET / HT | 200 | 9415 | - | Mozilla/5.0 (W |
| 2066 | **108.59.8.70** | **[24/Aug/2017:15:05:50** | -0400] | GET /wp | 200 | 1182 | - | Mozilla/5.0 (W |
| 2067 | **108.59.8.70** | **[29/Aug/2017:19:59:32** | -0400] | GET / HT | 200 | 9414 | - | Mozilla/5.0 (W |
| 2068 | **108.59.8.70** | **[29/Aug/2017:19:59:47** | -0400] | GET /veg | 200 | 11193 | https:// | Mozilla/5.0 (iP |
| 2069 | 108.59.8.80 | [10/Aug/2017:18:39:15 | -0400] | GET /wp | 304 | - | https:// | Mozilla/5.0 (iP |
| 2070 | 108.59.8.80 | [15/Aug/2017:06:52:45 | -0400] | GET /wp | 200 | 52978 | https:// | Mozilla/5.0 (iP |
| 2071 | 108.59.8.80 | [15/Aug/2017:06:52:49 | -0400] | GET /wp | 200 | 34265 | https:// | Mozilla/5.0 (iP |
| 2072 | 108.59.8.80 | [15/Aug/2017:06:52:52 | -0400] | GET /wp | 200 | 56257 | https:// | Mozilla/5.0 (iP |

After checking our logs again, we notice another unusual IP address. This address has visited the website 6 times in the space of a month. Again, either they love your website, or they're repeatedly clicking your ads.



IP Address Information

| | |
|---|---|
| Analysis Date | 2017-09-01 10:47:02 |
| Elapsed Time | 0 seconds |
| Blacklist Status | BLACKLISTED 3/96 |
| IP Address | **108.59.8.70** Find Sites \| IP Whois |
| Reverse DNS | hosted-by.leaseweb.com |
| ASN | AS30633 |
| ASN Owner | Leaseweb USA, Inc. |
| ISP | Leaseweb USA |
| Continent | North America |
| Country Code | (US) United States |
| Latitude / Longitude | 39.6734 / -75.7052 Google Map |
| City | Unknown |
| Region | Delaware |

After putting the IP address into the blacklist checker, we get some interesting results. The first thing to notice is that the IP address is on 3 blacklists which means whoever has been using this address is probably up to no good.

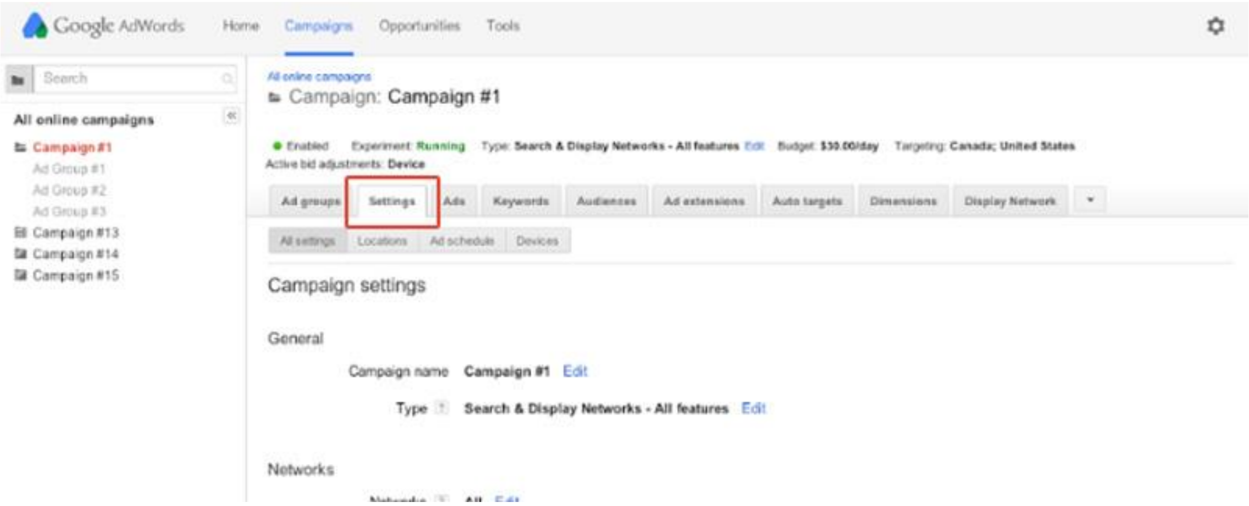
The second thing to notice is that the IP address comes from a company called Leaseweb USA. After checking their site, it seems that they provide servers to many clients across the world.

This could mean a few things. Either someone is using the rented server as a crawler to browse websites, or they could potentially be using it for fraudulent activities. Whatever the case, it's clear to see that this IP address is not coming from a real human and is most likely a bot. As a precaution, it's probably best to stop this IP address from seeing your ads.

## Excluding IP Addresses From AdWords Campaigns

Now you've got a list of suspicious IPs and have got enough evidence to suggest they are up to no good, it's time to block them.

To exclude IP addresses from seeing your campaigns you first need to sign in to your account and go to the main dashboard. At the top click the Campaigns tab and go to the settings after you've select the campaign from the left-hand sidebar.



Campaign: Campaign #1

Enabled  Experiment: Running  Type: Search & Display Networks - All features Edit  Budget: $30.00/day  Targeting: Canada; United States
Active bid adjustments: Device

Campaign settings

General

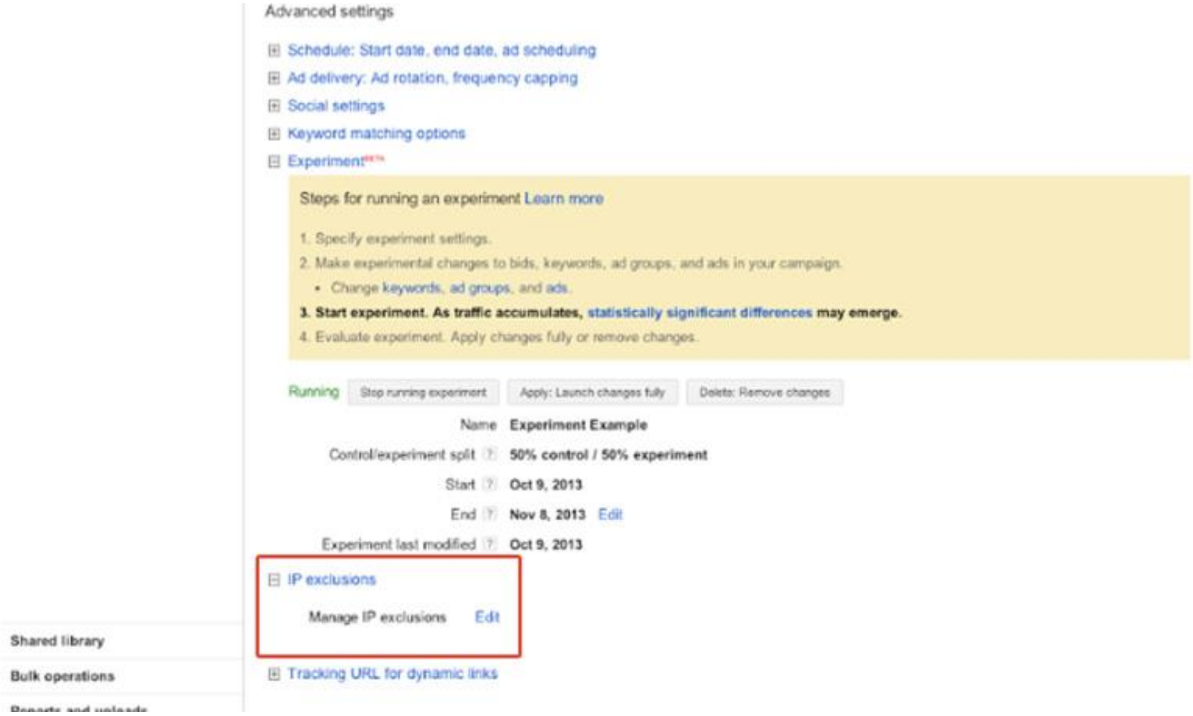
Campaign name  Campaign #1  Edit

Type  Search & Display Networks - All features  Edit

Networks

Networks  All  Edit

Once in the campaign settings, scroll down to the advanced settings and click the IP exclusions drop down button. Then click edit to begin entering the IP addresses.



Advanced settings

⊞ Schedule: Start date, end date, ad scheduling
⊞ Ad delivery: Ad rotation, frequency capping
⊞ Social settings
⊞ Keyword matching options
⊟ Experiment BETA

Steps for running an experiment Learn more

1. Specify experiment settings.
2. Make experimental changes to bids, keywords, ad groups, and ads in your campaign.
   - Change keywords, ad groups, and ads.
3. **Start experiment. As traffic accumulates, statistically significant differences may emerge.**
4. Evaluate experiment. Apply changes fully or remove changes.

Running | Stop running experiment | Apply: Launch changes fully | Delete: Remove changes

| | |
|---|---|
| Name | **Experiment Example** |
| Control/experiment split | **50% control / 50% experiment** |
| Start | **Oct 9, 2013** |
| End | **Nov 8, 2013** Edit |
| Experiment last modified | **Oct 9, 2013** |

⊟ IP exclusions

Manage IP exclusions Edit

⊞ Tracking URL for dynamic links

A new box will pop-up where you can enter the IP addresses you don't want to see your ads. Close the box by clicking save, and that's it. The IP addresses you've entered won't be able to see your adverts from now on.

Although this method does stop repeat offenders from constantly clicking your ads, the whole process can be very time consuming and boring. Another problem is that with the limited amount of data it can also be hard knowing when fraudsters start using different IP addresses. This requires even more effort as you constantly need to check your logs and comparethem to your ban list.

We're not sure about you, but we'd rather be working on improving our pay per click campaigns than worry about click fraud. Thankfully there is a way to completely automate this process with even better results!

# FINAL THOUGHTS

## A FANCY WAY TO SAY CONCLUSION

As you can see, click fraud is a growing problem that affects millions of businesses worldwide, regardless of their size. Although the battle against click fraud has been ongoing for several years, fraudster are always coming up with new ideas and methods to evade detection. Even Google's own anti-fraud system can be evaded with the right programming and knowledge. With click fraud continually on the rise, it's only a matter of time before you become a victim of it.

If you think you've been a victim of click fraud on your pay per click campaigns, then don't panic. If you can gather enough evidence to prove the clicks were fraudulent, then there's a good chance the network will refund your money. However, doing this manually can be extremely tedious and time-consuming. Obviously, this is not something you want to be doing every single day when monitoring your campaign, especially when you could be spending your time doing things that are more productive.

To help you win the fight against online fraudsters, we've created specialist click fraud prevention software which completely automates the process for you.

Having previously worked in the pay per click management industry for several years, we have experienced the terrifying effects of click fraud first hand. One day your campaign is making an impressive return and overnight it suddenly becomes unprofitable.

Having manually reviewed our server logs, we started to notice a pattern of IP addresses and users that would regularly connect to our website. After tracking their location and details, it becomes easy to see that most of these IPs were the same people clicking on our ads over and over again.

Blocking those suspicious IP addresses was easy, and for a time it worked. However, that didn't stop the fraudsters from thinking up new ideas. All they had to do was simply get another IP address that wasn't banned and they could click our ads again!

This meant that in order to stop the constant barrage of new clicks from new IP addresses every day; we had to constantly update our AdWords ban list. This took hours of intensive hard labor, but it had to be done otherwise we would lose a lot of our budget. We knew there had to be a simpler and easier way to fight these fraudsters.

Then came the genius idea: **fight automation with automation!**

If the fraudsters were using robots to automate all their clicks and fraud, then surely we could use something similar to fight back.

After months of designing and development, we have finally come up with something that would help protect our ads from the constant threat of click fraud.

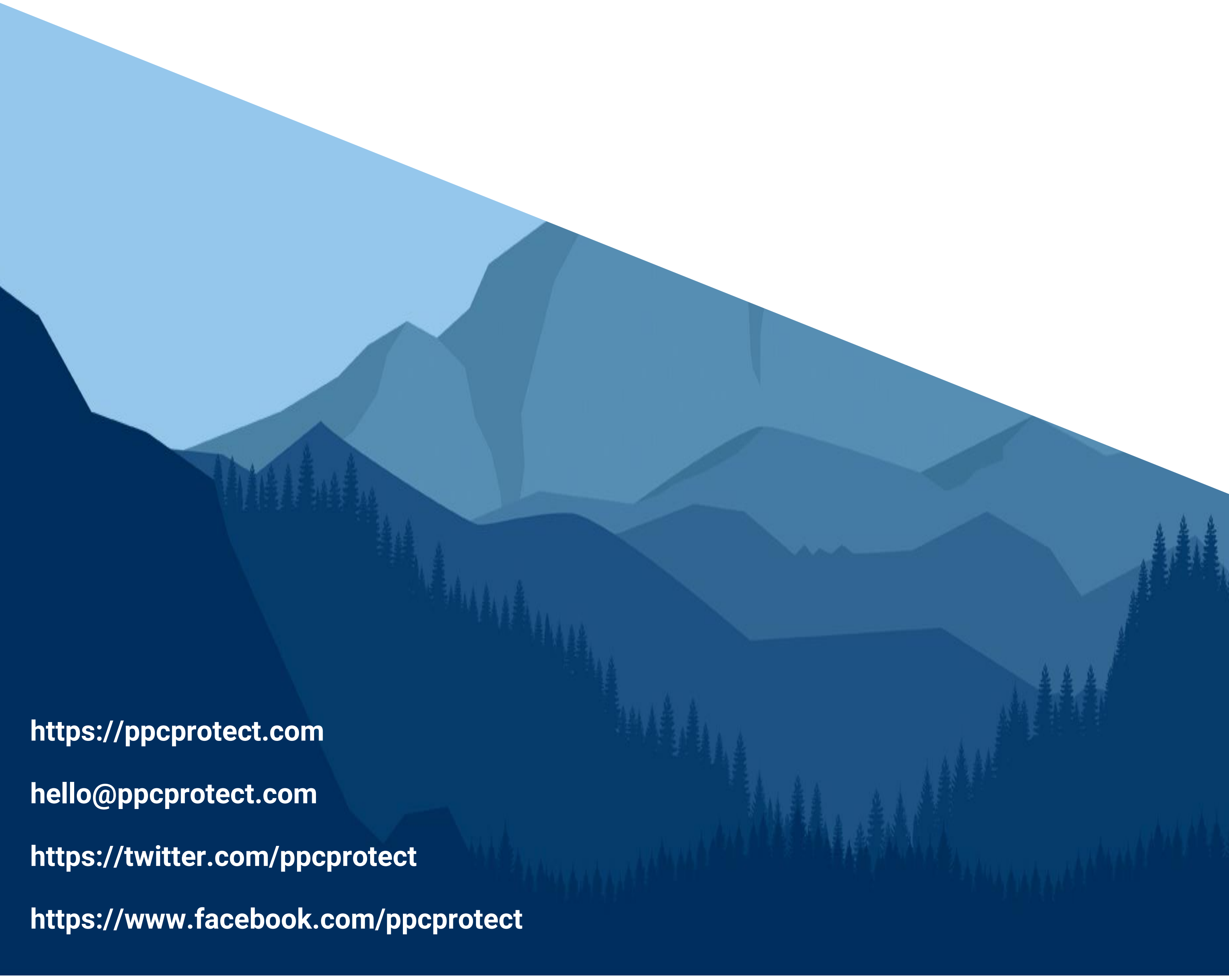
PPC Protect is software we designed specifically to work with Google's AdWords network, the software combines a proprietary click fraud detection algorithm with our blacklist of known fraudulent IP addresses. Having monitored hundreds of clients pay per click campaigns over the years, we've built an extensive list of IP addresses that fraudsters use. By having this at the core of the software, we can automatically stop your adverts from appearing for these users. If they can't see your adverts, then they can't click them and cost you money!

Since there's nothing stopping fraudsters from getting a new IP address, we've also put a lot of effort into our detection algorithm. By analyzing the incoming traffic from a pay per click campaign, we can monitor the frequency of clicks from a certain IP address across hundreds of different campaigns.

By combining data from hundreds of campaigns across various industries, we can easily identify which new IP addresses fraudsters are using. Once we've got evidence to prove the IP address is malicious, the software will automatically add it to the blacklist and request a refund for any previous clicks you may have received. This helps keeps your ads protected without you having to spend hours a day sifting through server IP logs.

Save time and money today with our sophisticated click fraud prevention software. To discover how much money you can save with PPC Protect, sign up to our free 30-day trial below.

## Prevent Click Fraud with PPC Protect



**https://ppcprotect.com**

**hello@ppcprotect.com**

**https://twitter.com/ppcprotect**

**https://www.facebook.com/ppcprotect**