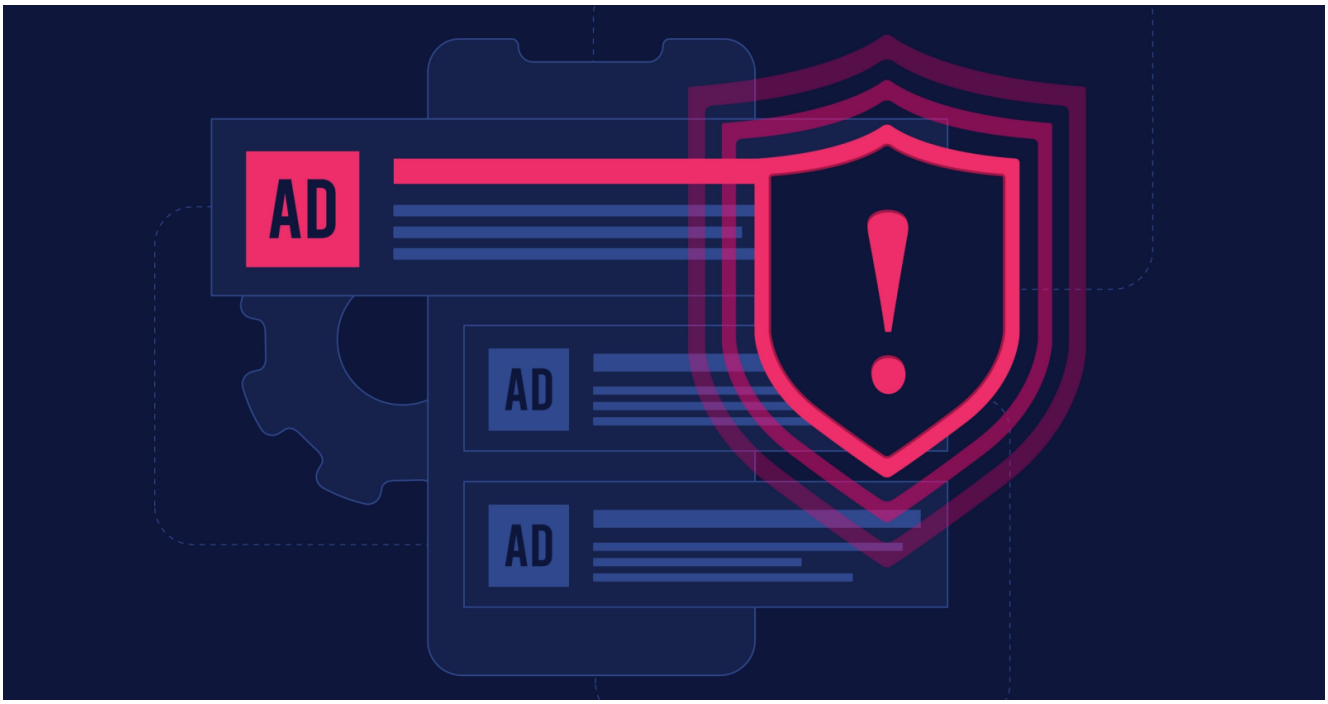
Beyond Tools: A Google Ads Guide To Detecting And Preventing Click Fraud In Lead Generation



Click fraud in lead generation can drain your marketing budget and corrupt your data, leading to misguided strategic decisions.

While automated detection tools serve as a first line of defense, relying solely on them is not enough.

This guide presents practical, hands-on approaches to identify and combat click fraud in your lead generation campaigns in Google Ads.

Understanding Modern Click Fraud Patterns

Click fraud isn’t just about basic bots anymore. The people

running these scams have gotten much smarter, and they're using tricks that your regular fraud tools might miss.

It's a big business, and if you think you are not affected, you are wrong.

Here's what's really happening to your ad budget: Real people in click farms are getting paid to click on ads all day long.

They use VPNs to hide where they're really coming from, making them look just like normal customers. And they're good at it.

The bots have gotten better, too. They now copy exactly how real people use websites: They move the mouse naturally, fill out forms like humans, and even make typing mistakes on purpose.

When these smart bots team up with real people, they become really hard to spot.

The scammers are also messing with your tracking in clever ways. They can trick your website into thinking they're new visitors every time.

They can make their phones seem like they're in your target city when they're actually on the other side of the world.

If you're counting on basic click fraud protection to catch all this, you're in trouble. These aren't the obvious fake clicks from years ago – they're smart attacks that need smart solutions.

That being said, the good old competitor trying to click 50 times on your ad is also still existent and not going away anytime soon.

Luckily, it is safe to say that Google can spot and detect those obvious fraud clicks in many cases.

Google’s Click Fraud Dilemma: Walking The Revenue Tightrope

Google faces a tricky problem with click fraud.

Every fake click puts money in Google’s pocket right now, but too many fake clicks will drive advertisers away. This creates a conflict of interest.

Google needs to show that it’s fighting click fraud to keep advertisers happy and the ad platform and all of its networks healthy, but it can’t afford to catch every single fake click.

If it did, its ad revenue would drop sharply in the short term because it also runs the risk of blocking valid clicks if it goes in too aggressively.

But if it doesn’t catch enough fraud, advertisers will lose trust and move their budgets elsewhere.

Some advertisers say this explains why Google’s fraud detection isn’t as strict as it could be.

They argue Google has found a sweet spot where it catches just enough fraud to keep advertisers from leaving, but not so much that it seriously hurts its revenue.

This balance gets even harder as fraudsters get better at making fake clicks look real.

This is also why many advertisers don’t fully trust Google’s own click fraud detection and prefer to use third-party tools.

These tools tend to flag more clicks as fraudulent than Google does, suggesting Google might be more conservative in what it considers fraud.

The Over-Blocking Problem Of Third-Party Tools

Third-party click fraud tools have their own business problem: They need to prove they're worth paying for every month.

This creates pressure to show lots of "blocked fraud" to justify their subscription costs. The result? Many of these tools are too aggressive and often block real customers by mistake.

Other tactics are to show lots of suspicious traffic or activities.

Think about it. If a click fraud tool shows zero fraud for a few weeks, clients might think they don't need it anymore and cancel.

So, these tools tend to set their detection rules very strict, marking anything slightly suspicious as fraud. This means they might block a real person who:

- Uses a VPN for privacy.
- Shares an IP address with others (like in an office).
- Browses with privacy tools.
- Has unusual but legitimate clicking patterns.

This over-blocking can actually hurt businesses more than the fraud these tools claim to stop.

It's like a store security guard who's so worried about shoplifters that they start turning away honest customers, too.

Why Click Fraud Tools Are Still

Valuable

Despite these issues, click fraud tools are still really useful as a first line of defense.

They're like security cameras for your ad traffic. They might not catch everything perfectly, but they give you a good picture of what's happening.

Here's what makes them worth using:

- They quickly show you patterns in your traffic that humans would take weeks to spot.
- Even if they're sometimes wrong about individual clicks, they're good at finding unusual patterns, like lots of clicks from the same place or at odd hours.
- They give you data you can use to make your own decisions – you don't have to block everything they flag as suspicious.

The key is to use these tools as a starting point, not a final answer. Look at their reports, but think about them carefully.

Are the "suspicious" clicks actually hurting your business? Do blocked users fit your customer profile?

Use the tool's data along with your own knowledge about your customers to make smarter decisions about what's really fraud and what's not.

In terms of functionality, most third-party click fraud detection tools are somewhat similar to each other.

A simple Google search on "click fraud tool" shows the market leaders; the only bigger difference is usually pricing and contract duration.

Tackling Click Fraud With Custom Solutions

After getting a first impression with third-party click fraud tools, it’s best to build a collection of custom solutions to tackle your individual scenario.

Every business has a different situation with different software environments, website systems, and monitoring.

For custom solutions, it’s recommended to work closely with your IT department or developer, as many solutions require some modification on your website.

The Basics: Selecting An Identifier

There are a handful of solutions to cover 80% of the basics.

The first way to do something against click fraud is to find a unique identifier to work with.

In most cases, this will be the IP address since you can exclude certain IP addresses from Google Ads, thus making it a good identifier to work with.

Other identifiers like Fingerprints are also possible options. Once an identifier is found, you need to make sure your server logs or internal tracking can monitor users and their identifiers for further analysis.

The Basics: CAPTCHAs

Another basic tool, which is often forgotten, is CAPTCHAs.

CAPTCHAs can detect bots or fraudulent traffic. Google offers a free and simple-to-implement solution with reCAPTCHA.

CAPTCHAs might seem like an easy answer to bot traffic, but they come with serious downsides.

Every time you add a CAPTCHA, you're basically telling your real users, "Prove you're human before I trust you." This creates friction, and friction kills conversions.

Most websites see a drop in form completions after adding CAPTCHAs if they are set too aggressively.

Smart CAPTCHAs can limit the frequency, but not all CAPTCHA providers allow that option, so choose your provider or solution wisely.

The Basics: Honeypot Fields

Honeypot fields are hidden form fields that act as traps for bots.

The trick is simple but effective: Add extra fields to your form that real people can't see, but bots will try to fill out.

Only bots reading the raw HTML will find these fields; regular users won't even know they're there. The key is to make these fields look real to bots.

Use names that bots love to fill in, like "url," "website," or "email2." If any of these hidden fields get filled out, you know it's probably a bot. Real people won't see them, so they can't fill them out.

Pro tip: Don't just add "honeypot" or "trap" to your field names. Bots are getting smarter and often check for obvious trap names. Instead, use names that look like regular-form fields.

Advanced Validation Methods

Smart Form Validation: Email

Most businesses only check if an email address has an “@” symbol and looks roughly correct.

This basic approach leaves the door wide open for fake leads and spam submissions.

Modern email validation needs to go much deeper. Start by examining the email’s basic structure, but don’t stop there.

Look at the domain itself: Is it real? How long has it existed? Does it have proper mail server records?

These checks can happen in real time while your user fills out the form. It should be noted, however, that smart form validation usually requires some sort of third-party provider to check the details, which means you need to rely on external services.

A common mistake is blocking all free email providers like Gmail or Yahoo. This might seem logical, but it’s a costly error.

Many legitimate business users rely on Gmail for their day-to-day operations, especially small business owners.

Instead of blanket blocks, look for unusual patterns within these email addresses. A Gmail address with a normal name pattern is probably fine; one with a random string of characters should raise red flags.

For enterprise B2B sales, you expect bigger companies to sign up with their company domain email address, so blocking free mail providers might work.

Smart Form Validation: Phone

Phone validation goes far beyond just counting digits. Think about the logic of location first.

When someone enters a phone number with a New York area code but lists their address in California, that’s worth investigating.

But be careful with this approach – people move, they travel, and they keep their old numbers. The key is to use these mismatches as flags for further verification, not as automatic rejections.

The Art Of Smart Data Formatting

Data formatting isn’t just about making your database look neat. It’s about catching mistakes and fraud while making the form easy to complete for legitimate users.

Name fields are a perfect example.

While you want to catch obviously fake names like “asdfgh” or repeated characters, remember that real names come in an incredible variety of formats and styles.

Some cultures use single names, others have very long names, and some include characters that might look unusual to your system.

Modify Your Google Ads Campaign Settings To Tackle Click Fraud

Google offers multiple campaign options to increase reach, on the downside most of those options come along with an increase of click fraud activities.

App Placements

Performance Max campaigns can place your ads across Google’s entire network, including in apps. While this broad reach can be powerful, it also opens the door to potential fraud.

The challenge is that you have limited control over where your ads appear, and some of these automatic placements can lead to wasted ad spend.

Kids' games are often a major source of accidental and fraudulent clicks. These apps frequently have buttons placed near ad spaces, and children playing games can accidentally tap ads while trying to play.

What looks like engagement in your analytics is actually just frustrated kids trying to hit the "play" button.

Another issue comes from apps that use deceptive design to generate clicks. They might place clickable elements right where ads appear, or design their interface so users naturally tap where ads are located.

This isn't always intentional fraud. Sometimes, it's just poor app design, but it costs you money either way.

Unlike traditional campaigns, where you can easily exclude specific placements, Performance Max's automation makes this more challenging.

The system optimizes for conversions, but it might not recognize that clicks from certain apps never lead to quality leads. By the time you spot the pattern, you've already spent money on these low-quality clicks.

Excluding app placements is for almost all advertisers a must have. Very few advertisers benefit from app placements at all.

Partner And Display Network

Lead generation businesses face a unique challenge with Performance Max campaigns that ecommerce stores can largely avoid.

While ecommerce businesses can simply run Shopping-only campaigns and tap into high-intent product searches, lead gen

businesses are stuck dealing with the full Performance Max package, including the often problematic Display Network.

The Display Network opens up your ads to a mass of websites, many of which might not be the quality placements you'd want for your business.

While Google tries to filter out bad actors, the display network still includes sites that exist primarily to generate ad clicks.

These sites might look legitimate at first glance, but they're designed to encourage accidental clicks or attract bot traffic.

Some are specifically designed for server bot farms, as they run on expired domains and have no content besides ads.

Lead generation businesses don't have this luxury. Their Performance Max campaigns typically run on all networks except shopping. This creates several problems:

- **The quality of clicks varies wildly.** Someone might click your medical practice ad while trying to close a pop-up on a gaming site. They'll never become a patient, but you still pay for that click.
- **Display placements can appear on sites that don't match your brand's professional image.** Imagine a law firm's ad showing up on a site full of questionable content – not ideal for building trust with potential clients.
- **Bot traffic and click farms often target display ads** because they're easier to interact with than shopping ads. You might see high click-through rates that look great until you realize none of these clicks are turning into leads.

All those are reasons to question PMax campaigns for lead gen, but that's a decision every marketer has to make.

Advanced Google Ads Settings To Tackle Click Fraud

If the basics are implemented but there is still a higher amount of suspected click fraud, advanced solutions need to be implemented.

Besides excluding suspicious IP addresses, you can also build negative audiences.

The idea is to have a second success page for your lead generation form and only forward potential bots or fake sign-ups to this page.

To achieve that, your website needs to evaluate potential bots live during the sign-up process.

You can then setup a dedicated “bot pixel” on the second success page in order to send data of this audience to Google.

Once enough data is retrieved, you can exclude this audience from your campaigns. This approach is a little trickier to implement but is worth the effort as those audience signals are of high quality if enough data is supplied.

Make sure to only fire the “bot pixel” on the special success page and only there, otherwise you run the risk of mixing your audiences which would render the system useless.

Filtering Fake Leads With Conditional Triggers

Another tracking-based strategy is to set up condition-based conversion tracking. Combined with hidden form fields, you can modify the conversion trigger not to send data if the hidden field was filled.

In that scenario, you would filter out bots from conversion

tracking, sending back only real conversion to your campaign, and therefore, also training the Google algorithm and bidding strategy only on real data.

You eliminate a majority of fake leads and traffic with this setup.

Making Sign-Ups More Challenging To Improve Lead Quality

Another advanced strategy is to make the sign-up process a lot harder.

Tests have shown that much longer forms are not finished by bots because they are usually trained on simpler and shorter forms, which require only mail, name, phone, and address.

Asking specific questions and working with dropdowns can dramatically increase the lead quality. It should be noted, however, that longer forms can also hurt the valid signup rate, which is a risk you want to take if you have to deal with bot and fraud traffic.

A fitting case was a car dealer I worked with. They had a form where people could offer their cars for sale and retrieve a price estimate.

A short form had almost three times the signup rate than before, but it turned out later that a lot of them were spam signups or even very low-qualified leads.

A shorter form leads to more spam because it’s easy to sign up. After switching to a longer form, the signups dropped, but quality increased drastically.

Almost 20 fields long, and potential clients had to upload pictures of their car.

It took a few minutes to finish the signup, but those who did

were committed to doing business and open to discussing the sale, which also made it easier for the salespeople to follow up properly.

A Hard Truth About Lead Fraud

Let’s be honest: You can’t completely stop lead fraud. It’s like shoplifting in retail – you can reduce it, you can catch it faster, but you can’t eliminate it entirely.

The fraudsters are always getting smarter, and for every security measure we create, they’ll eventually find a way around it.

But here’s the good news: You don’t need perfect protection. What you need is a balanced approach that catches most of the bad leads while letting good ones through easily.

Think of it like running a store: You want security, but not so much that it scares away real customers.

The key is to layer your defenses. Use click fraud tools as your first line of defense, add smart form validation as your second, and keep a human eye on patterns as your final check.

Will some fake leads still get through? Yes. But if you can stop 90% of the fraud, you’re winning the battle.

Remember: Perfect is the enemy of good. Focus on making fraud expensive and difficult for the bad actors, while keeping your lead generation process smooth and simple for real prospects. That’s how you win in the long run.

More Resources:

Featured Image: BestForBest/Shutterstock

https://www.searchenginejournal.com/google-ads-guide-preventin

g-click-fraud-in-lead-gen/539317/