



THERE'S A NEW  
THREAT OUT THERE:  
DON'T BE A VICTIM

# BEHIND THE CLICKS

UNDERSTANDING INVALID TRAFFIC AND

AD FRAUD FOR BEGINNERS

UNDERSTANDING INVALID TRAFFIC AND

AD FRAUD FOR BEGINNERS

# BEHIND THE CLICKS



WHERE THE MONEY GOES, THE FRAUD FOLLOWS!!!

Online advertising is a key strategy for businesses looking to connect with their target audiences. As digital channels, ad networks and advertising grow, so does the threat of ad fraud. We have a saying at TrafficGuard: 'where the money goes, the fraud follows', such is the reality of today's digital world.

## BEHIND THE CLICKS

Aimed at the digital marketers and procurement teams who may be dimly aware that ad fraud is something they should understand but have never got round to doing so. If that's you, we hope you'll find this guide eye-opening, alarming, and reassuring in equal measure.

Whether you need to educate yourself, or you need to educate your wider business: forewarned is forearmed, and it's only when you fully understand the growing complexities of ad fraud that you can begin to fight back against it.

## KEY HIGHLIGHTS

Ad fraud and invalid traffic is a major issue in online advertising. According to Statista it cost \$100bn globally in 2024, expected to rise to \$172bn by 2028

SMEs and Enterprises are both vulnerable to ad fraud in different ways. SMEs usually have fewer resources and skills to notice ad fraud, and their lower overall budgets are more susceptible to being damaged by competitor clicks.

Enterprises struggle to balance returning users draining their ad budgets (we'll explain more later) vs the need to to notice ad fraud, and their lower overall budgets are more susceptible to being damaged by competitor clicks.

To fight invalid traffic and ad fraud, strong detection tools should be considered a vital part of a business' cyber-security and digital marketing stack.

\$172BN BY 2028

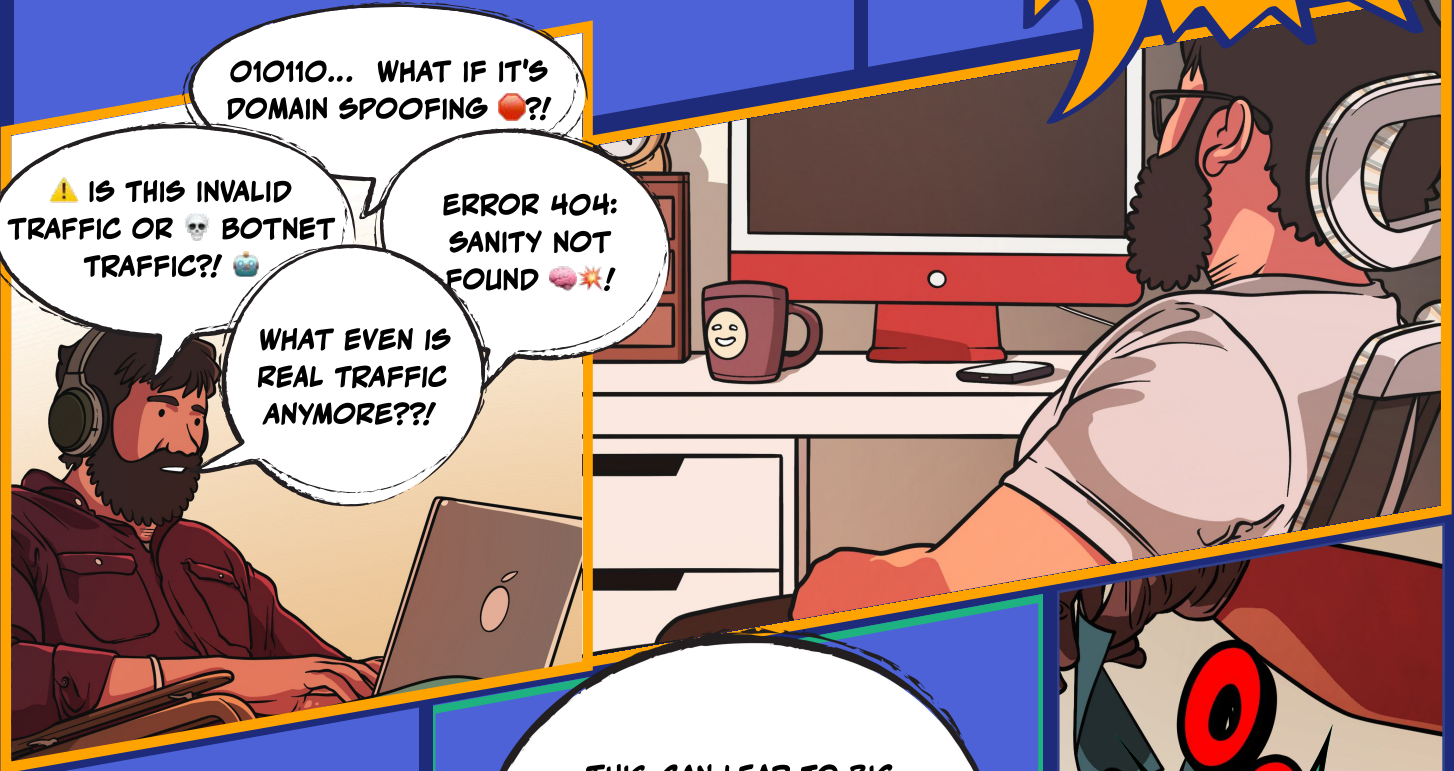
WOW!



**THE BASICS**

When we talk about ad fraud, we mean invalid traffic: any advertising engagement that doesn't represent genuine interest in the advertised offering. Intentional invalid traffic covers everything from bot traffic to more vertical specific problems such as bonus abuse in online sports betting, or price scraping in eCommerce.

**UNINTENTIONAL INVALID TRAFFIC IS EITHER ACCIDENTAL OR NON-MALICIOUS; MORE ON THESE DISTINCTIONS LATER.**



**THE BASICS**

Ad fraud means actions that create fake profit by wrongfully increasing ad impressions, clicks, or other important metrics such as app installs.

**THIS CAN LEAD TO BIG LOSSES FOR ADVERTISERS AND HURT THEIR CAMPAIGN SUCCESS. IN 2023, A SOBERING 22% OF GLOBAL AD SPEND WAS LOST TO INVALID TRAFFIC.**

**22%**

**OF GLOBAL AD SPEND**



THE ALARMING REALITY OF AD FRAUD

AD FRAUD COULD BECOME THE WORLD'S SECOND LARGEST GLOBAL CRIME MARKET AFTER DRUGS



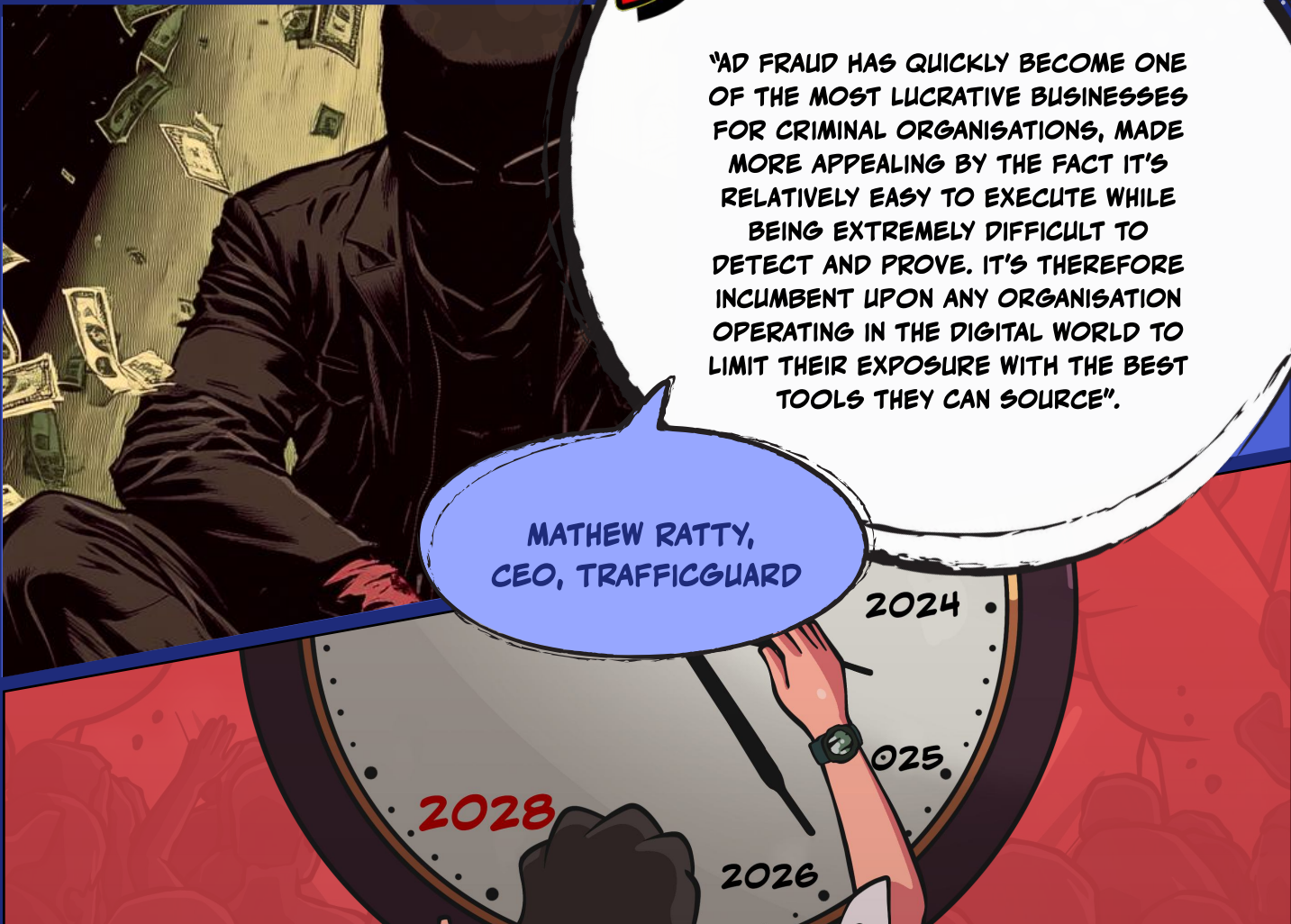
EXPECTED TO COST DIGITAL ADVERTISING \$172BN GLOBALLY BY 2028

AN ANNUAL INCREASE OF APPROXIMATELY 14%.

**BANNING!!**

"AD FRAUD HAS QUICKLY BECOME ONE OF THE MOST LUCRATIVE BUSINESSES FOR CRIMINAL ORGANISATIONS, MADE MORE APPEALING BY THE FACT IT'S RELATIVELY EASY TO EXECUTE WHILE BEING EXTREMELY DIFFICULT TO DETECT AND PROVE. IT'S THEREFORE INCUMBENT UPON ANY ORGANISATION OPERATING IN THE DIGITAL WORLD TO LIMIT THEIR EXPOSURE WITH THE BEST TOOLS THEY CAN SOURCE".

MATHEW RATTY,  
CEO, TRAFFICGUARD



FINANCIAL IMPACT

UP TO 20% OF CLICKS ON PAID SEARCH ARE ESTIMATED TO BE FRAUDULENT OR INVALID - THE IMPACT ON A BUSINESS'S BOTTOM LINE NEEDS NO EXPLANATION

ACCURATE CAMPAIGN DATA IS VITAL FOR STRATEGIC DECISION MAKING. AD FRAUD CAN LEAD TO POOR DECISIONS

SKEWED DATA

REPUTATIONAL DAMAGE

Erosion of trust in digital advertising platforms can impact the entire digital marketing ecosystem. From a marketer's point of view, scaling back on digital campaigns could see them missing opportunities to engage with real customers and reach new markets.

WE'RE MISSING OPPORTUNITIES TO ENGAGE WITH REAL CUSTOMERS AND REACH NEW MARKETS.



UNDERSTANDING THE IMPACT ON BUSINESSES

DIGITAL MARKETERS OFTEN FIND IT HARD TO TELL REAL USERS APART FROM FAKE TRAFFIC, ESPECIALLY WHEN IT COMES TO ONLINE ADVERTISING. FRAUDULENT TRAFFIC CAN HARM AD SPEND AND SKEW CONVERSION DATA WHICH, IN TURN, IMPACTS HOW WELL THE OVERALL CAMPAIGN PERFORMS.

INACCURATE CAMPAIGN DATA CAN LEAD A BUSINESS TO ALL KINDS OF FURTHER ISSUES - KPIS BECOME IRRELEVANT, STRATEGIC INVESTMENT DECISIONS BECOME MISGUIDED AND CHANNEL PERFORMANCE BECOMES DIMINISHED AND DIFFICULT TO ACCURATELY ASSESS.



THIS IS A BIG PROBLEM IN THE DIGITAL ADVERTISING INDUSTRY, BUT MANY DIGITAL MARKETERS AND CYBER SECURITY FUNCTIONS WITHIN BUSINESSES ARE EITHER UNAWARE OF THE PROBLEM OR UNAWARE OF THE SCALE AND POTENTIAL IMPACT OF IT.

One leading [European bookmaker](#) found that a staggering 43% of its PPC budget was being lost to IVT - totalling thousands of Euros per week.

43%

PPC BUDGET WAS BEING LOST TO IVT

Let's take a step back though, because before you can prevent ad fraud from eating up your campaign budgets first you need to understand it; and that starts with understanding IVT.





Real, legitimate users sometimes click on ads by accident or interact with them in surprising ways. Despite their non-malicious intent, this is a form of IVT and it can have a disproportionate impact on your ad campaigns

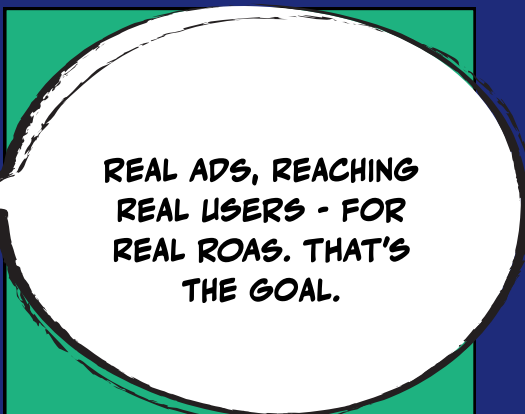
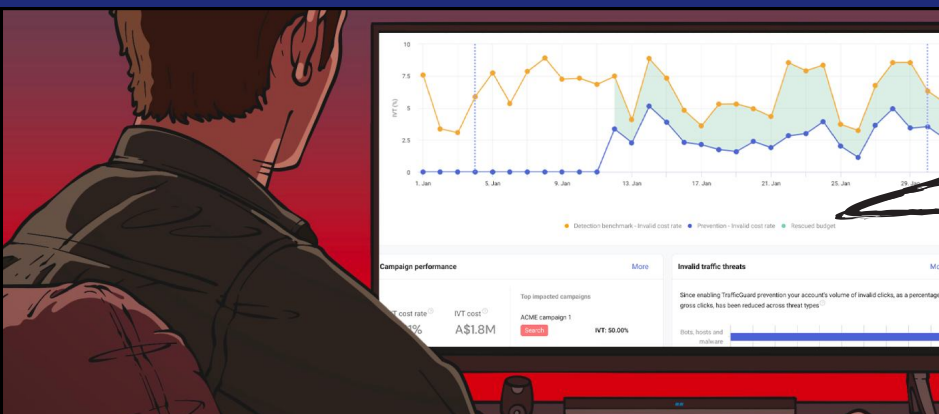


**INTENTIONAL AD FRAUD IS A DIFFERENT STORY, AND TAKES PLACE WHEN BAD ACTORS DELIBERATELY CREATE FAKE TRAFFIC AS A MEANS TO MAKE MONEY**

Fraudsters' ultimate goal is to take advertising money by faking clicks, impressions, or conversions. The concerning part for digital marketers is that the tools at their disposal to do this are becoming ever more sophisticated and hard to mitigate.

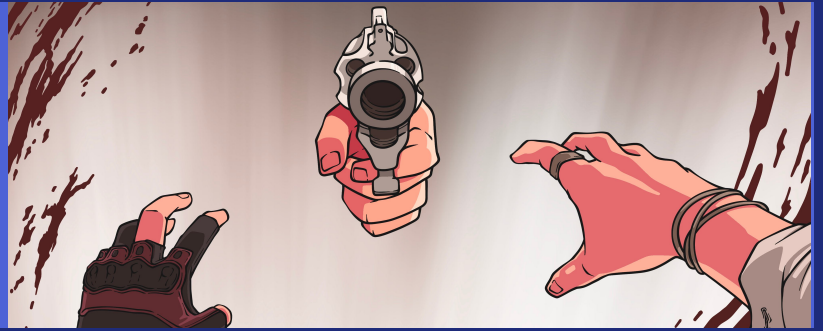
They may use botnets, click farms, or malware to pretend to be real users. Their goal is to take advertising money by faking clicks, impressions, or conversions and they'll stop at nothing to do so.

Being ad fraud-aware and understanding the difference between accidental IVT and intentional ad fraud is key to being able to prevent it.



**REAL ADS, REACHING REAL USERS - FOR REAL ROAS. THAT'S THE GOAL.**

Enterprises with sky-high ad budgets are appealing targets for fraudsters, however, it's the smaller businesses who may actually be at greater risk from ad fraud.



FOR EXAMPLE

PAID SOCIAL ADVERTISING THROUGH META AND X.

The relentless growth of online advertising platforms means that many SMEs rely on them to drive revenue – indeed many SMEs have built their entire businesses off the back of Google paid search campaigns and paid social advertising through Meta and X.

Competitor click fraud – when a competitor company or automated bot intentionally clicks on a rival business's online ads, usually to deplete their ad budget – is a big threat to SMEs who often won't have the capacity in their ad budget to absorb it.



AD FRAUD CAN BE HUGELY DAMAGING TO A FLEDGLING BUSINESS

When you consider the key role that SMEs play in supply chains – and how this can facilitate cybercriminals and fraudsters gaining access to larger enterprises – it brings into sharp focus the importance of being alert to the risks.

KEY ROLE THAT SMES

PLAY IN SUPPLY CHAINS

IN SPITE OF THE ABOVE, COMPARED TO THE BIG ENTERPRISE PLAYERS, SMES OFTEN HAVE LIMITED RESOURCES TO RECOGNISE, ADDRESS, AND ULTIMATELY PREVENT AD FRAUD FROM IMPACTING THEIR BOTTOM LINE.



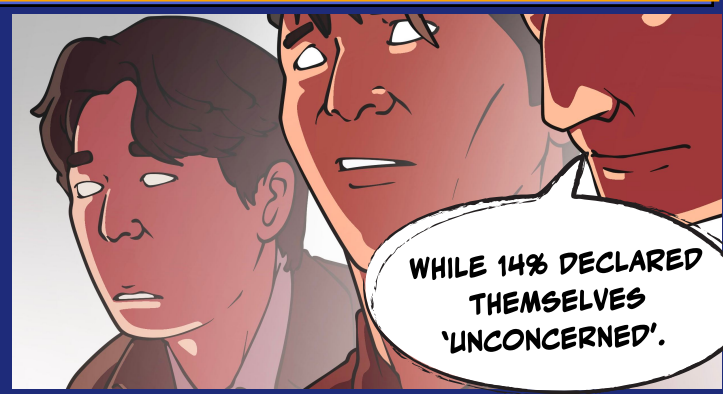


## THE IMPACT OF AD FRAUD ON ENTERPRISE BUSINESS

A study by Outward Media and Ascend2 in late 2023 revealed a concerning lack of awareness of ad fraud among enterprise marketers...



> 23% WERE VERY CONCERNED ABOUT AD FRAUD



WHILE 14% DECLARED THEMSELVES 'UNCONCERNED'.



> 18% CITED AD FRAUD AND INVALID TRAFFIC AS THE MOST SIGNIFICANT CHALLENGE IN DIGITAL DISPLAY ADVERTISING

**33%**

EXTREMELY EFFECTIVE

This is despite one-third – 33% – of them saying that digital display advertising is 'extremely effective' in driving conversions and sales, and 61% saying that it is 'somewhat effective'

**61%**

SOMEWHAT EFFECTIVE



THERE'S NO CLEARER ILLUSTRATION OF THE NEED FOR COMPREHENSIVE EDUCATION ON AD FRAUD FOR DIGITAL MARKETERS AND SUPPORT IN THE IMPLEMENTATION OF EFFECTIVE STRATEGIES TO MITIGATE IT.

THE ROLE OF DIGITAL MARKETERS IN COMBATING AD FRAUD

SO CLEARLY, DIGITAL MARKETERS HAVE A VITAL - ARGUABLY THE MOST VITAL - ROLE TO PLAY IN TACKLING AD FRAUD WITHIN THEIR ORGANISATION.

UNDERSTANDING THE DIFFERENT TYPES OF AD FRAUD HELPS THEM REDUCE RISKS AND KEEP THEIR AD SPENDING SAFE. IT'S ALSO VITAL TO KEEP LEARNING ABOUT NEW WAYS AD FRAUD CAN HAPPEN.

30%

A great example of the difference this can make is the example of Rappi, a high-growth eCommerce app based in Latin America. Ad fraud was impacting it to such an extent that the growth team was spending up to 30% of its time analysing traffic, reacting to fraud and cleaning data for campaign optimisation.

PARTNERING WITH TRAFFICGUARD TO TAKE ACTION ON AD FRAUD:

SAW AN AVERAGE OF 25% OF CLICKS INVALIDATED BEFORE ATTRIBUTION

LED TO A 25% IMPROVEMENT IN ADVERTISING ROI

REMOVED MANUAL ANALYSIS FROM THE GROWTH TEAM, SAVING 30% OF THEIR TIME



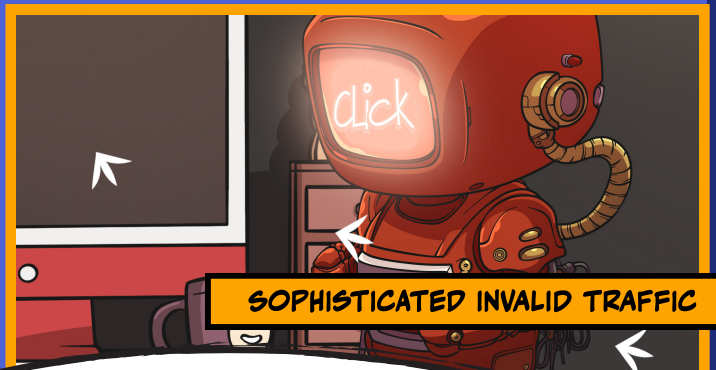
To state the obvious: an understanding of the different types of ad fraud is the first step to stopping it. Invalid traffic refers to any clicks or impressions that may artificially inflate an advertiser's costs, and a significant component of this is non-human traffic such as bots, automated scripts, and malware - more on that shortly.

**INVALID TRAFFIC CAN BE BROKEN DOWN INTO TWO TYPES:**

GIVT is the form of invalid traffic most easiest to detect. It's usually caused by web crawlers as they index web pages and is not done with malicious intent - it can come from accidental clicks and internal traffic.

Despite being benign in intent, it can still damage your ad budgets, as bot traffic inflates your ad costs without yielding genuine conversions.

SIVT is actively fraudulent traffic created to drain ad spend and create inaccurate data. SIVT is generally more difficult to detect than GIVT. This can take a number of forms, for example, automated browsing by bots, emulators and custom automation tools, and manipulated activity designed to appear as valid traffic.



IF YOU THINK IT'S COMPLICATED TO UNDERSTAND, TAKE OUR WORD FOR IT - IT'S EVEN MORE COMPLICATED TO TACKLE

FOR A CLEAR, REAL-WORLD EXAMPLE CHECK OUT THIS INFOGRAPHIC, WHICH USES ONE OF TRAFFICGUARD'S GLOBAL SPORTS BETTING CLIENTS TO ILLUSTRATE THE DIFFERENT TYPES OF NEFARIOUS TACTICS THAT FRAUDSTERS COULD BE USING TO INFILTRATE YOUR AD CAMPAIGNS:

[READ NOW](#)

The budget in traffic and ma over two wee

guard analysed week period, and t

From the \$750,000 ca bots, malicious traffic e



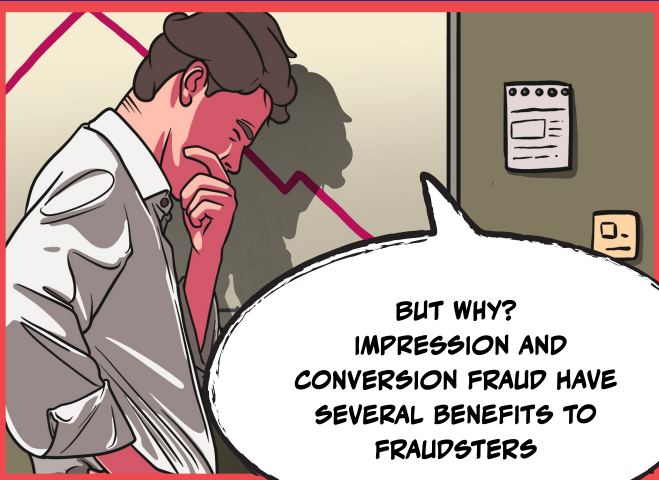
**IMPRESSION FRAUD**

Hate to break it to you, but click fraud is just one of the many types of ad fraud in digital advertising. Impression fraud happens when many ad impressions are recorded, but real users don't actually see the ads. It can be done by placing ads in very small, hidden areas called invisible pixels. Sometimes, fake apps are used to increase impressions without real user engagement. Fraudsters make money by selling fake traffic to advertisers, earning revenue from ad impressions and clicks.



**CONVERSION FRAUD**

Conversion fraud is when bad actors use bots to fool campaigns into thinking they're real users. They might fill out forms, sign up, or install apps to show false success for a campaign. This fake conversion data can mislead businesses, leading them to think their campaigns are performing better than they actually are.



**BUT WHY?  
IMPRESSION AND  
CONVERSION FRAUD HAVE  
SEVERAL BENEFITS TO  
FRAUDSTERS**



**HARMING COMPETITORS**

Fraudsters can drain a competitor's budget and reduce the effectiveness of their campaigns by generating fake clicks and impressions on their ads.



**INFLATING METRICS**

Publishers can make their websites appear more popular by generating fake impressions, which can attract higher-paying advertisers.

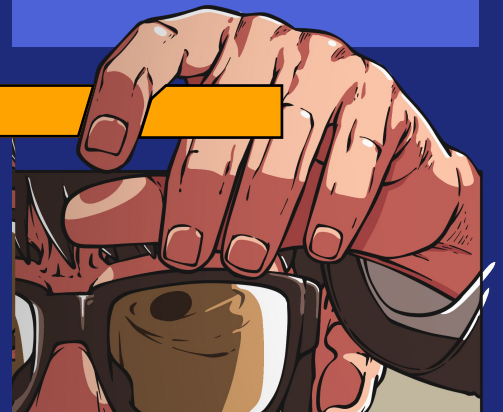


**DATA COLLECTION**

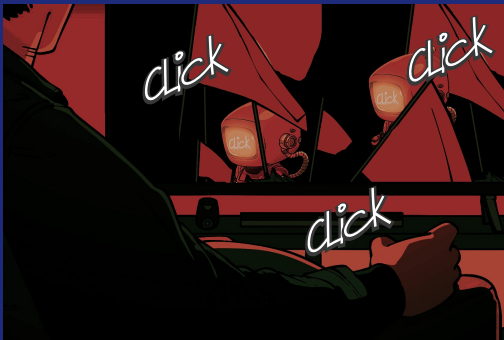
Fraudsters can collect valuable user data, such as IP addresses, browsing habits, and banking details, which can then be sold or used for other malicious purposes.

**ATTRIBUTION FRAUD AND ITS HIDDEN DANGERS**

Attribution fraud is a type of ad fraud. It tricks the system that gives credit for sales made through digital marketing. This system checks different points in a customer's journey. In short, attribution fraud happens when a person claims credit for sales that really should go to other channels or campaigns.



## SIGNS YOU MIGHT BE A VICTIM OF AD FRAUD - AS SIMPLE AS 1,2,3 (4,5)



### SUSPICIOUS TRAFFIC SOURCES

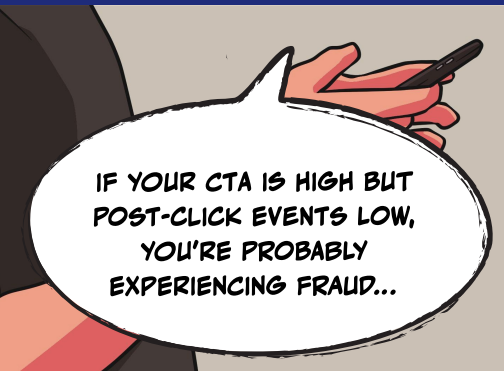
Large amounts of traffic coming from suspicious sources, such as low-quality websites or IP addresses, is a red flag to be aware of. It is crucial to vet an ad network thoroughly to avoid these suspicious traffic sources. This traffic is likely to be generated by bots or click farms rather than genuine human users.

### UNUSUAL CLICK PATTERNS

Ad fraudsters often use bots to generate fake clicks. If you notice unusual click patterns, such as an unusually high number of clicks at specific times or on specific days, this could be a sign of ad fraud.



**MOBILE AD FRAUD CAN ALSO RESULT IN UNUSUAL CLICK PATTERNS, INCLUDING TYPES SUCH AS CLICK INJECTION.**



**IF YOUR CTA IS HIGH BUT POST-CLICK EVENTS LOW, YOU'RE PROBABLY EXPERIENCING FRAUD...**

### HIGH CLICK-THROUGH RATES

While a high click-through rate (CTR) is usually good news to marketers, it can also be a warning sign of ad fraud. Fraudsters often use bots to generate fake ad impressions and inflate CTRs. So if your CTR is high but post-click events low, you're probably experiencing fraud...

### HIGH BOUNCE RATES

High bounce rates are often a consequence of the above. Fraudulent ads can lead to high bounce rates due to a lack of genuine engagement.

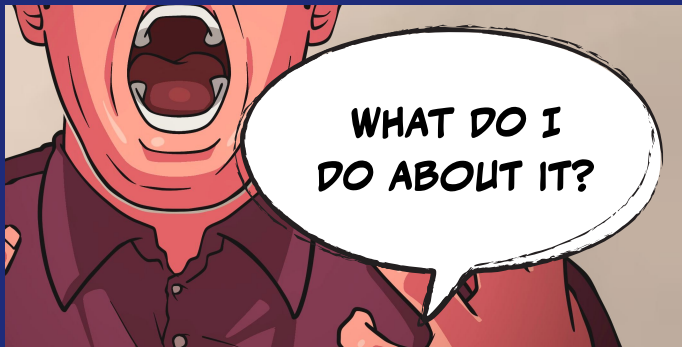


**FRAUDSTERS OFTEN USE BOTS TO GENERATE CLICKS THAT DO NOT RESULT IN GENUINE ENGAGEMENT OR CONVERSIONS.**

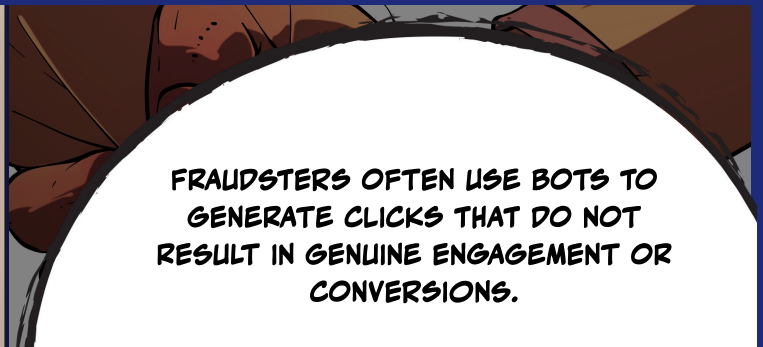
### ABNORMALLY HIGH IMPRESSIONS

Another metric which doesn't necessarily seem negative at first glance, until you see no subsequent engagement from a large number of impressions. Fraudsters can use tactics such as ad stacking to generate multiple impressions for a single ad, inflating the impression count.

They manipulate ad placements to create these false impressions, misleading advertisers into believing they are purchasing legitimate ad placements.



**WHAT DO I DO ABOUT IT?**



**FRAUDSTERS OFTEN USE BOTS TO GENERATE CLICKS THAT DO NOT RESULT IN GENUINE ENGAGEMENT OR CONVERSIONS.**

**YOUR FIRST LINE OF DEFENCE**

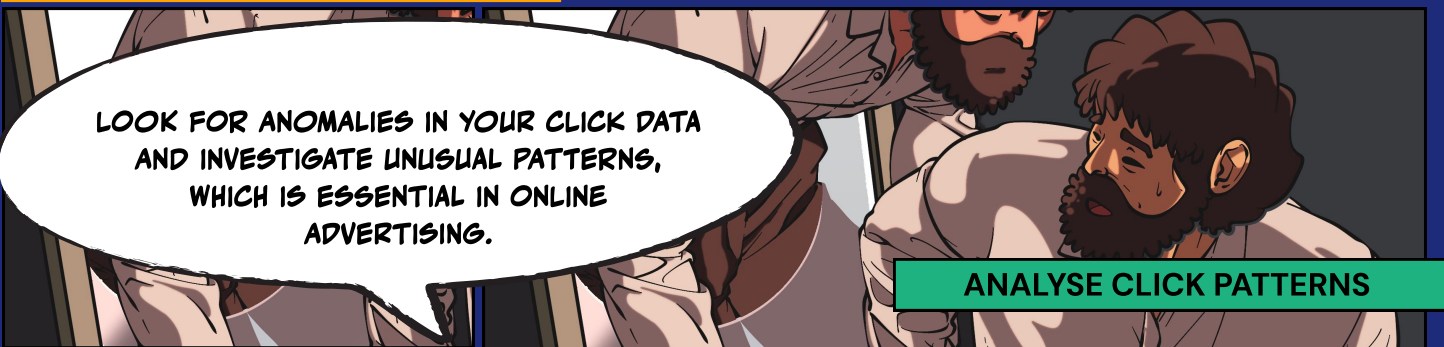
**CHECKING FOR AD FRAUD MANUALLY IS A LABORIOUS PROCESS. AUTOMATED DETECTION TOOLS LIKE TRAFFICGUARD USE AI-POWERED MACHINE LEARNING TO IDENTIFY AND BLOCK FRAUDULENT ACTIVITY, STREAMLINING THE ENTIRE PROCESS.**

**WE USE A TRIPLE LAYER OF FRAUD PREVENTION - PRE-BID EXCLUSIONS, IN-STREAM PREVENTION, AND ATTRIBUTION VERIFICATION - TO KNOCK THE FRAUDSTERS DOWN (AND THEN DOWN AND DOWN AGAIN).**



**MONITOR YOUR TRAFFIC SOURCES**

You should regularly review the sources of your traffic and block suspicious IP addresses to control where your online ads appear. TrafficGuard monitors every click-through to your ads, flagging up any anomalies before they can become a problem.



**LOOK FOR ANOMALIES IN YOUR CLICK DATA AND INVESTIGATE UNUSUAL PATTERNS, WHICH IS ESSENTIAL IN ONLINE ADVERTISING.**

**ANALYSE CLICK PATTERNS**



**KEEP AN EYE ON YOUR CLICK-THROUGH RATES, BOUNCE RATES, AND IMPRESSION COUNTS FOR ANY IRREGULARITIES.**

**REVIEW METRICS FREQUENTLY**

## INDUSTRY-SPECIFIC CONSIDERATIONS

DIFFERENT INDUSTRIES HAVE THEIR OWN UNIQUE CHALLENGES WHEN IT COMES TO AD FRAUD.

## ECOMMERCE

Bounce rate and cart abandonment are a big headache for eCommerce businesses; implementing a solution like TrafficGuard will ensure you only receive engagement from interested users, massively reducing the issue

## SPORTS BETTING

MONITOR SUSPICIOUS BETTING PATTERNS: WATCH OUT FOR IRREGULAR BETTING ACTIVITIES FROM FRAUDSTERS AND AUTOMATED BOTS, WHICH CAN WREAK HAVOC ON YOUR ADVERTISING BUDGETS.

Sports betting is highly competitive, and customer acquisition costs are high

By implementing TrafficGuard's shadow campaign technology, sportsbooks can minimise CAC and maximise new customer engagement.

## TRAVEL

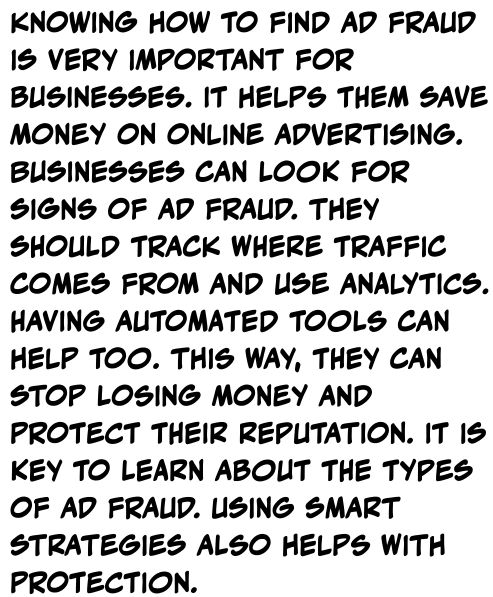
BOTS MAKE UP 80% OF THE IVT EXPERIENCED BY OPERATORS IN THE TRAVEL SECTOR: A CLEAR INDICATION OF A DIRECT THREAT, AS THIS NUMBER USUALLY SITS BETWEEN 15-30% FOR MOST OTHER SECTORS.

ADDING TRAFFICGUARD PROTECTION TO YOUR CAMPAIGNS WILL ENSURE ONLY GENUINE USERS CAN CLICK ON YOUR ADS, GIVING YOU PEACE OF MIND THAT YOUR DATA IS CLEAN AND YOUR BUDGET OPTIMISED

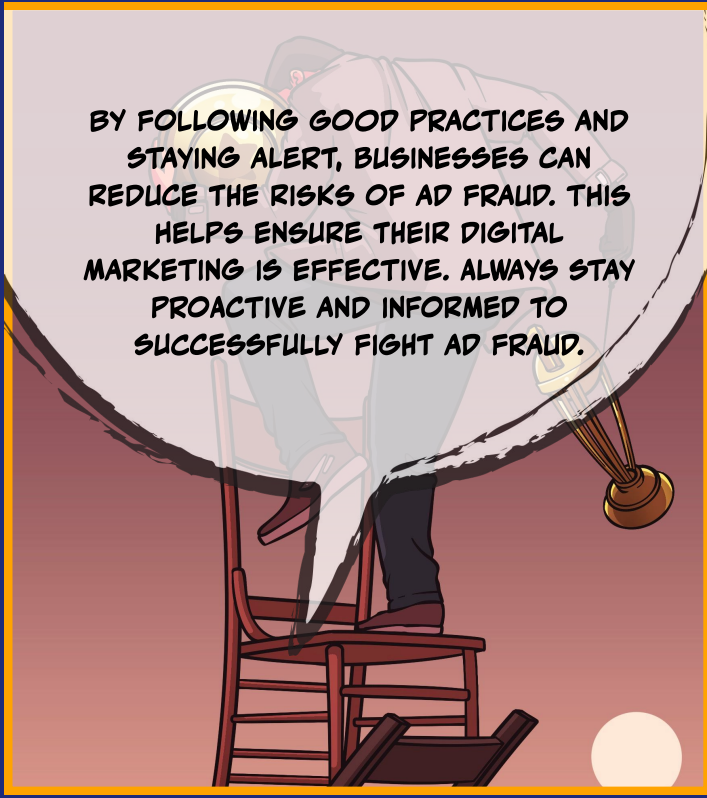
## AGENCIES

MANAGE MULTIPLE CLIENTS EFFICIENTLY: IF YOU HAVE MULTIPLE CLIENTS TO MANAGE, YOU WANT TO ENSURE YOU'VE IMPLEMENTED THE BEST PRACTICES IN TRACKING AND REPORTING. THIS ENSURES YOUR CLIENTS RECEIVE RELIABLE DATA ON THEIR RETURN ON INVESTMENT, ENABLING INFORMED DECISION-MAKING AND STRATEGIC ADJUSTMENTS.

ADOPT ADVANCED FRAUD PREVENTION TOOLS: TOOLS LIKE TRAFFICGUARD ARE YOUR SECRET WEAPON TO SECURING MULTIPLE CLIENT CAMPAIGNS, INCREASING CLIENT SATISFACTION, AND IMPROVING THE QUALITY OF YOUR SERVICE.



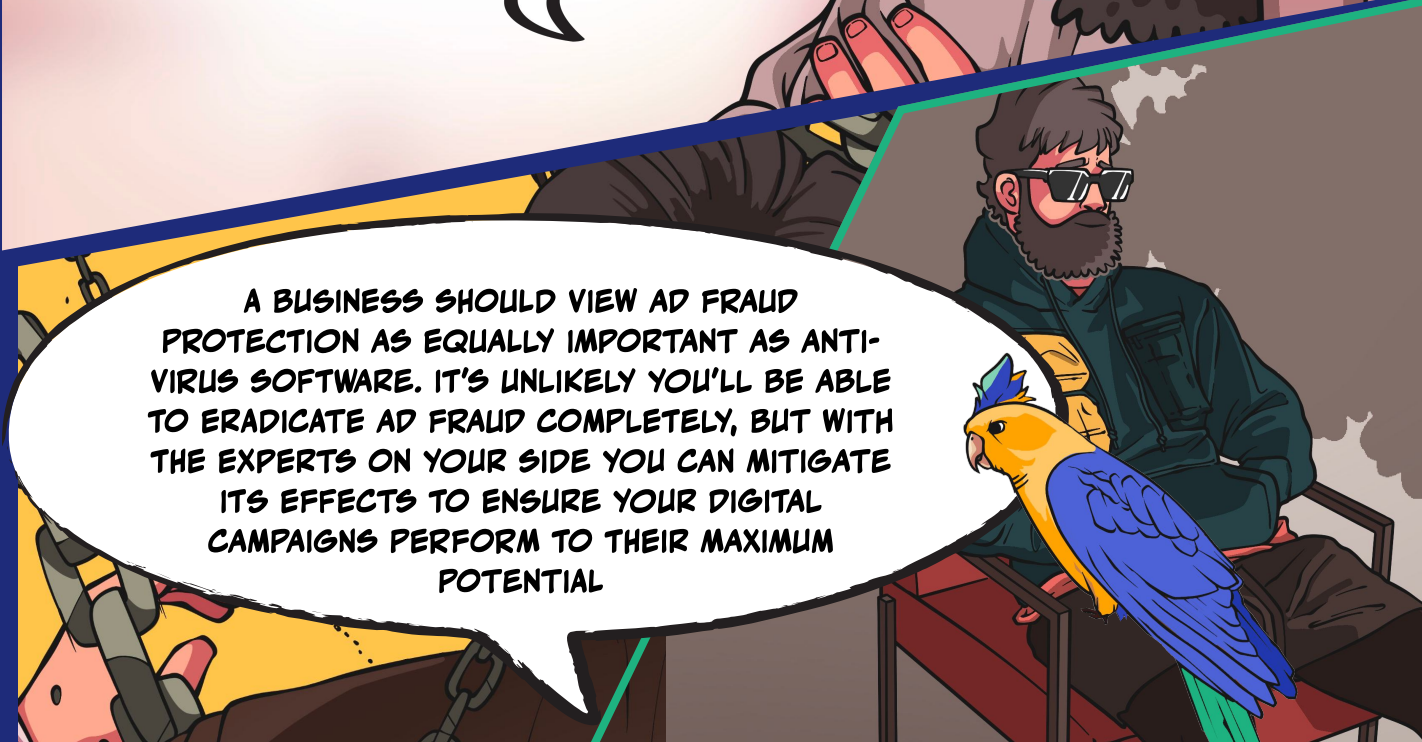
KNOWING HOW TO FIND AD FRAUD IS VERY IMPORTANT FOR BUSINESSES. IT HELPS THEM SAVE MONEY ON ONLINE ADVERTISING. BUSINESSES CAN LOOK FOR SIGNS OF AD FRAUD. THEY SHOULD TRACK WHERE TRAFFIC COMES FROM AND USE ANALYTICS. HAVING AUTOMATED TOOLS CAN HELP TOO. THIS WAY, THEY CAN STOP LOSING MONEY AND PROTECT THEIR REPUTATION. IT IS KEY TO LEARN ABOUT THE TYPES OF AD FRAUD. USING SMART STRATEGIES ALSO HELPS WITH PROTECTION.



BY FOLLOWING GOOD PRACTICES AND STAYING ALERT, BUSINESSES CAN REDUCE THE RISKS OF AD FRAUD. THIS HELPS ENSURE THEIR DIGITAL MARKETING IS EFFECTIVE. ALWAYS STAY PROACTIVE AND INFORMED TO SUCCESSFULLY FIGHT AD FRAUD.

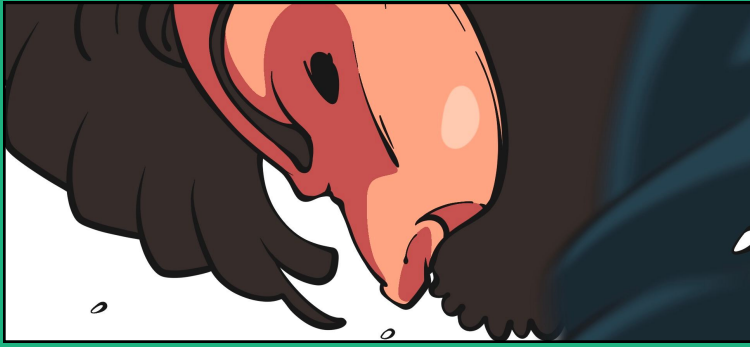


A LAST WORD ON AD FRAUD  
- CAN IT BE COMPLETELY ERADICATED?



A BUSINESS SHOULD VIEW AD FRAUD PROTECTION AS EQUALLY IMPORTANT AS ANTI-VIRUS SOFTWARE. IT'S UNLIKELY YOU'LL BE ABLE TO ERADICATE AD FRAUD COMPLETELY, BUT WITH THE EXPERTS ON YOUR SIDE YOU CAN MITIGATE ITS EFFECTS TO ENSURE YOUR DIGITAL CAMPAIGNS PERFORM TO THEIR MAXIMUM POTENTIAL





TO BE CONTINUED...

