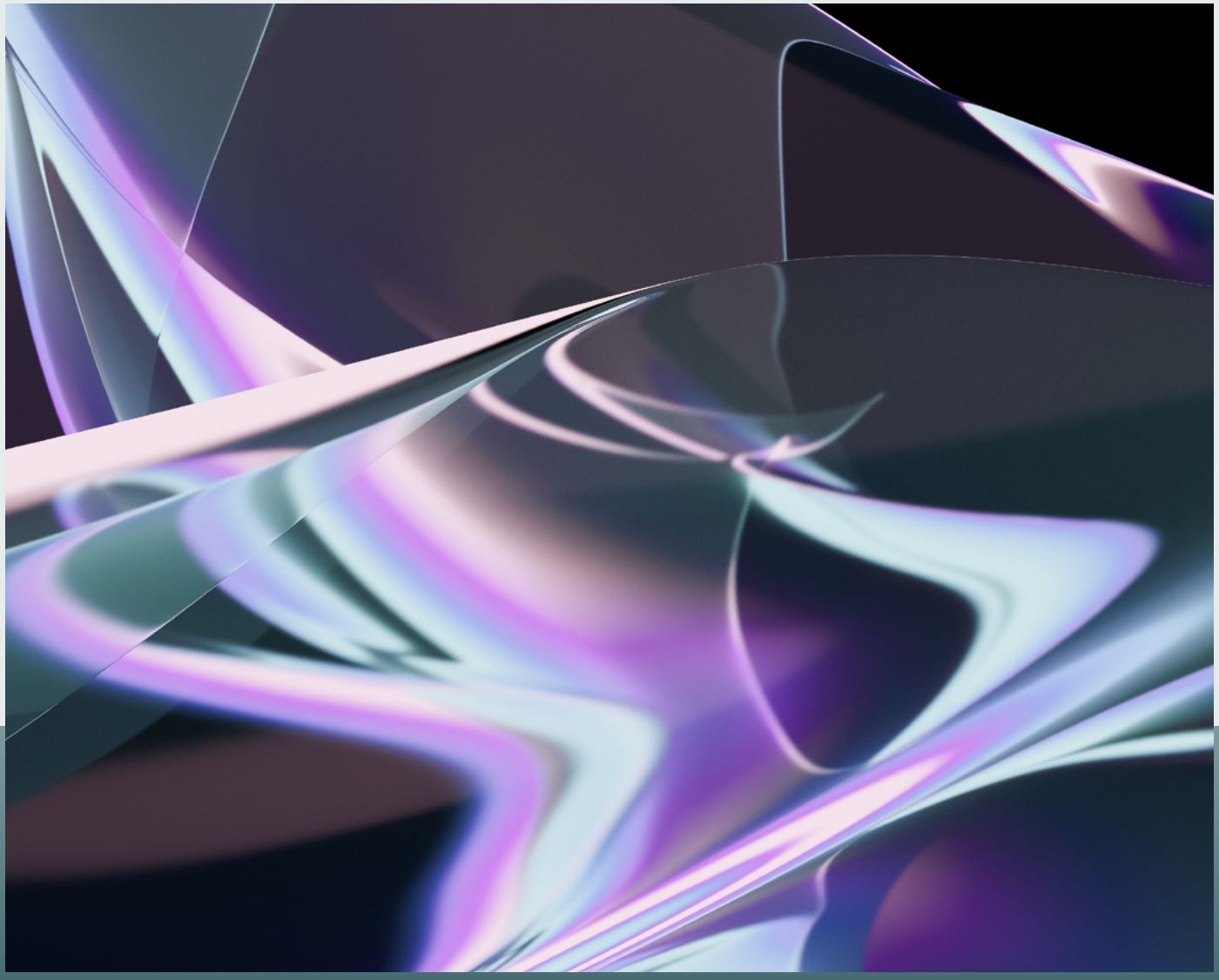
Click Fraud in Digital Advertising: An Industry Guide to Protection and Prevention



HUMAN

Click Fraud in Digital Advertising: An Industry Guide to Protection and Prevention

Table of Contents

1 Introduction 3

2 Executive Summary 4

3 What is Click Fraud? 5

4 Understanding Invalid Clicks and Their Impact 6

5 The Evolution of Click Fraud Tactics in a Performance-Driven Ecosystem 9

6 The Unique Challenges of Click Fraud in Programmatic Advertising 12

7 How Click Fraud Affects Advertising Stakeholders 15

8 HUMAN + LinkedIn: A New Approach to Click Protection 18

9 Best Practices for Advertisers 20

10 Future Outlook & Industry Implications 21

11 The HUMAN Advantage 23

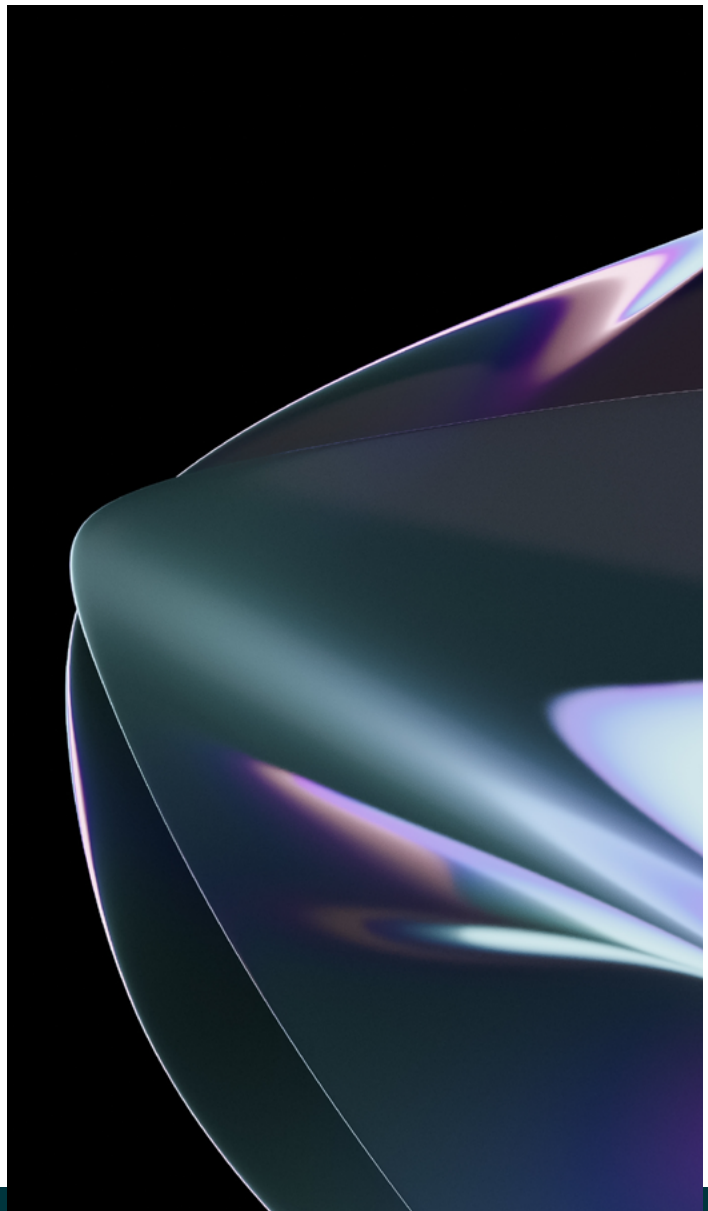
12 Conclusion 24

1.

Introduction

Every day, billions of dollars flow through the digital advertising ecosystem, providing the economic backbone of the internet as we know it.

But as performance-based advertising models such as cost-per-click and cost-per-conversion increasingly dominate, fraud has evolved to exploit these metrics. Throughout these changes, click fraud has emerged as one of the key challenges in the advertising industry.



2.

Executive Summary

Click fraud has re-emerged as a serious threat to digital advertising, fueled by the shift to mobile-first, performance-driven buying models.

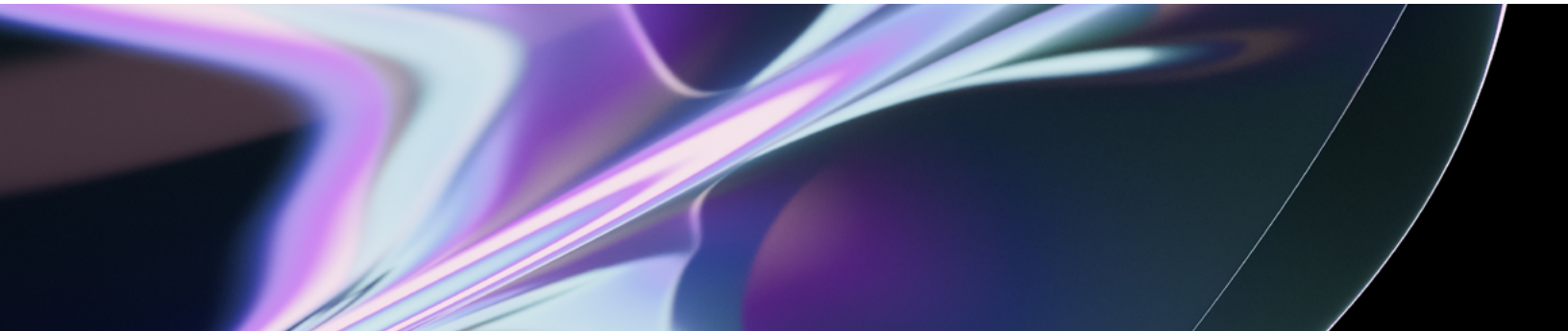
Invalid clicks now come from multiple sources —automated scripts, incentivized engagement, accidental taps, and even creative scanners—and many attacks occur after an impression or without one at all. This makes traditional impression-level defenses insufficient.

In April 2025, LinkedIn integrated HUMAN's Ad Click Defense across display inventory on the LinkedIn Audience Network. By layering real-time behavioral analysis and click validation to native safeguards, LinkedIn **improved invalid traffic detection over the first four months**, ensuring advertisers are not billed for illegitimate engagement.

Protecting against this evolving threat requires layered, click-specific defenses: validating the click itself in real time, classifying both GIVT and SIVT accurately, and integrating these protections directly into reporting, billing, and optimization systems to preserve trust and performance.

What You'll Learn in This Whitepaper

- How click fraud tactics have evolved and why the problem is resurging
- The technical vulnerabilities in the click lifecycle that fraudsters exploit
- The broader ecosystem of actors—bots, click farms, and platforms with weak safeguards
- The financial, operational, and trust impacts across advertisers, publishers, and ad tech platforms
- Real-world results from LinkedIn's deployment of HUMAN's Ad Click Defense
- Best practices and checklists to audit, protect, and validate click-level engagement
- Future trends and the industry's path toward shared standards for click validation



3.

What is Click Fraud?

Click fraud is a type of digital ad fraud where bots, scripts, malware, or human click farms generate fake clicks or touch events on ads.

These interactions aren't driven by real consumer interest, but aim to inflate performance metrics, claim last-touch attribution, drain competitor budgets, or drive revenue to publishers without delivering actual engagement.

Although click fraud was once considered a solved problem in the desktop era, when rudimentary filters blocked most bots, it has returned with new force, stemming from two shifts in advertising: mobile-first and performance-based buying.

The shift to mobile-first advertising introduced more touch-based interactions, where cramped interfaces and in-app ecosystems created new fraud opportunities. Tactics like click spamming and in-app click injection emerged, targeting attribution systems with precision.

At the same time, the industry's shift to outcome -based models like cost-per-click (CPC) and cost-per-acquisition (CPA) increased the value of each individual interaction. As advertisers focused on measurable results, fraudsters adapted—moving from impression inflation to performance manipulation.

Once limited to simple scripts, click fraud tactics have evolved into complex operations utilizing advanced techniques like residential proxy networks, machine learning, click injection, and device emulation—techniques that mimic real users and evade detection.

This evolution hasn't gone unnoticed, major global platforms now invest heavily in protection mechanisms, confirming that what once appeared "solved" has merely transformed into more complex challenges requiring renewed vigilance.

Click fraud affects every stage of the customer journey. It skews click-through rates, misleads campaign optimization, and can inflate billing metrics. As a result, advertisers pay for engagement with no chance of conversion. As performance and return on ad spend (ROAS) become central measures of campaign effectiveness, click fraud is becoming increasingly harder to ignore. It demands stronger, more sophisticated click-level defenses to protect ad budgets and maintain trust in digital advertising.

4.

Understanding Invalid Clicks and Their Impact

Click fraud is a major concern, but it exists within a broader landscape of invalid clicks: a set of behaviors—both automated and human-driven—that distort the metrics advertisers rely on to make decisions.

When we talk about click validity, we're referring to whether clicks reflect legitimate engagement and intent. Advertising loses its effectiveness when it is served to bots, uninterested users, or people who never meant to click in the first place. Below, we outline various types of invalid clicks that advertisers and platforms may encounter. While not all invalid clicks are fraudulent, they all represent instances where advertisers aren't receiving the value they paid for.

Automated Clicks from Bots and Scripts

Bot activity remains one of the most widespread sources of invalid clicks. These simulated interactions are generated by software that mimics user behavior. This traffic can come from data centers, hijacked devices, residential proxies, and, increasingly, from legitimate devices running apps with unknown background activity, which makes automated traffic even more difficult to distinguish from genuine human engagement. While some sophisticated forms of invalid activity can result in reported conversion events (such as those seen in attribution fraud or bot-driven downloads), these ultimately lack genuine user intent.

Incentivized Clicks without Genuine Intent

In some cases, invalid clicks come from real people who are paid to interact with ads. These are known as incentivized clicks. While they are technically generated by humans, the intent is artificial. Users click on ads in exchange for money, crypto, or access to pirated content, without authentic interest in the advertiser's offer. This tactic is commonly used in cash reward-based mobile applications, sites that offer pirated content, and paid-to-click websites.

Accidental Clicks

Not every invalid click is the result of fraud. Accidental click and touch events occur when users interact with ads due to flawed interface design, small tap targets, or misleading placement. These clicks are often triggered during scrolling or navigation, especially on mobile devices where physical screen space is limited. These interactions aren't malicious, but they still waste ad spend, distort performance data, and mislead optimization systems by making it appear that certain placements or audiences are effective when they are not.

Creative Verification and Validation

Creative scanners, publishers, platforms, and ad verification vendors use automated tools to scan ad creatives for malware, content policy violations, and brand safety concerns. These scanners typically load ads in controlled environments and may trigger click events to measure CPU/GPU/browser performance, visit and verify landing pages, and overall assess the ad creative's integrity, including redirect chains. While these activities serve crucial security and quality assurance functions, they generate non-human clicks that can distort campaign metrics if not properly identified and filtered.

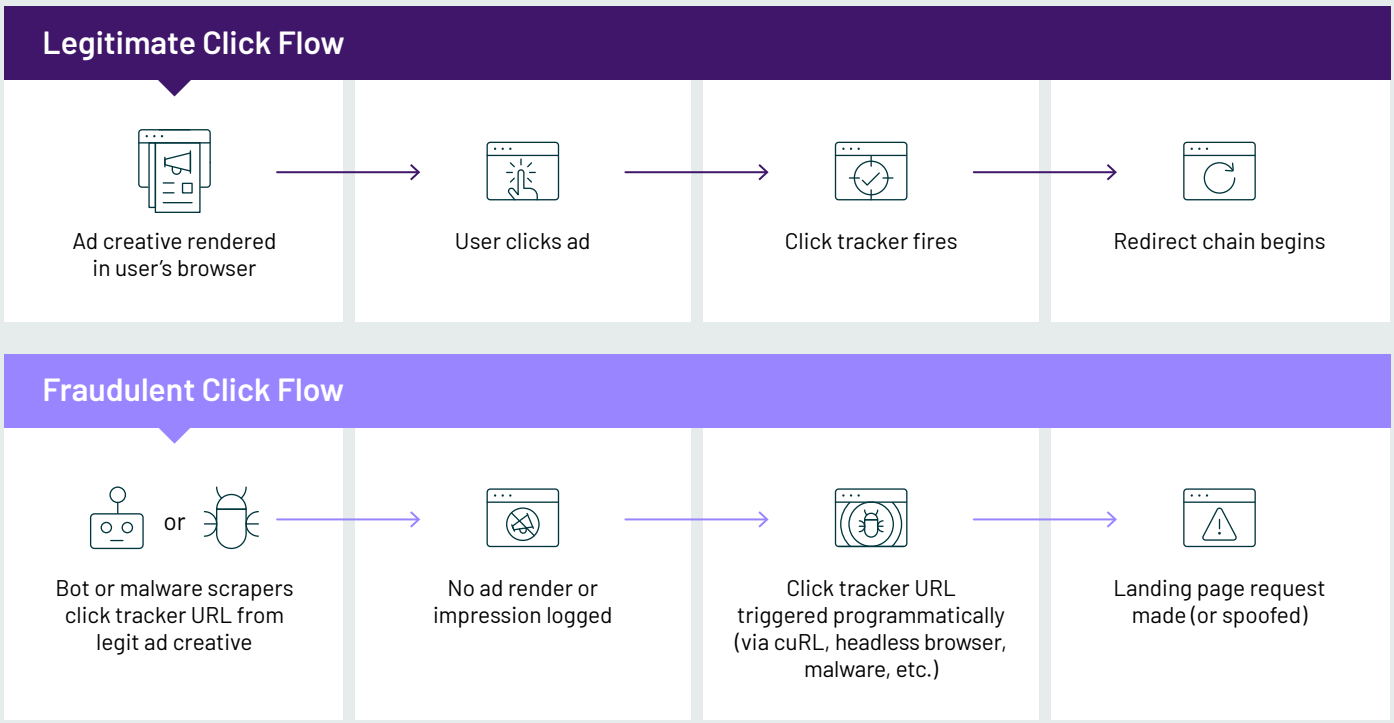
Impression Fraud vs. Click Fraud: Why Comprehensive Protection is Necessary

Advertising fraud prevention solutions are usually designed to avoid invalid impressions. These systems focus on filtering out non-human traffic before an ad is served, often through real-time bidding (RTB) pre-bid filters or impression-level scoring. While important, this only protects the first step in the advertising interaction.

Click fraud, by contrast, can occur after the impression is delivered. A bot might avoid detection at the impression level but still trigger a fake click through malware, session hijacking, or deferred interaction. In some cases, bad actors

How Bots Can Trigger Clicks Without an Ad Impression

Some sophisticated fraud operations harvest click tracker URLs from legitimate ad creatives and store them in a database. Later, bots can be directed to "click" those URLs programmatically, simulating engagement without any user present or ad displayed. Because these clicks occur out-of-context—outside of the ad slot or without a prior impression—they're difficult to tie to a legitimate user session, but may still pass basic validation checks and get counted for billing & tracking purposes.

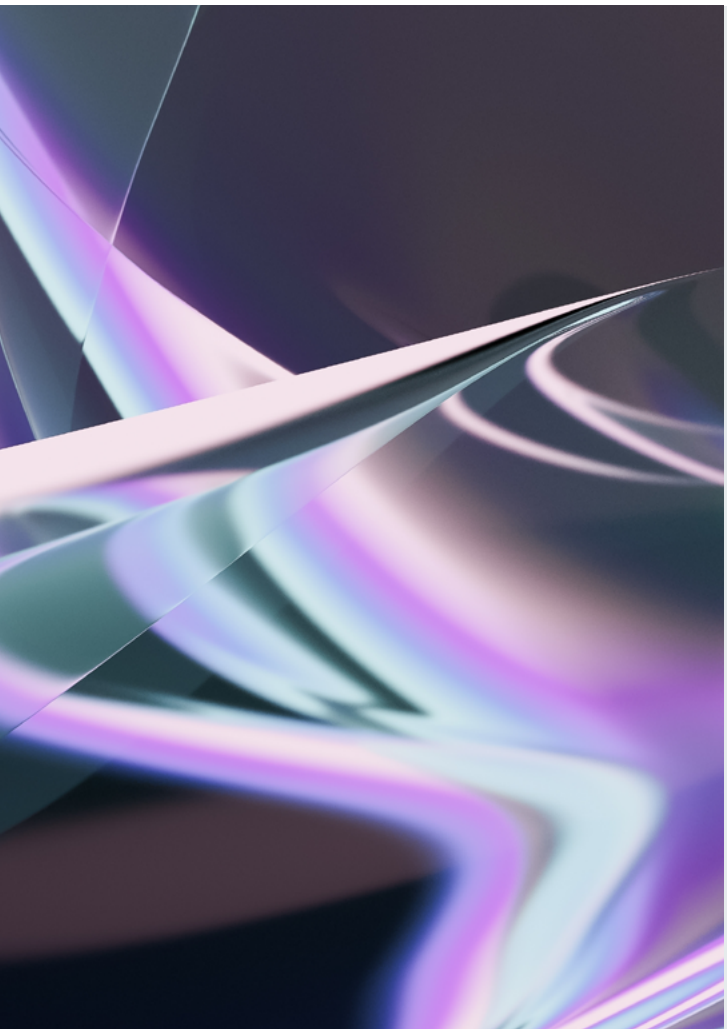


bypass the impression entirely by accessing the click tracker directly, creating fraudulent click signals without a corresponding ad view.

Given that click fraud exploits a different stage of the ad lifecycle than impression fraud, it requires different detection signals and response strategies. Impression fraud is often identified by its origin—bots, spoofing, invalid placements, or stacked ads—while click fraud is identified through both technical and behavioral data.

Examples of potential indicators of click fraud include unusually high click-through rates without corresponding engagement on landing pages, repetitive or rapid-fire click behavior, or clicks that appear to originate from malware operating on real user devices. These patterns are often invisible at the impression layer and require systems designed to monitor click-specific events in real time.

Comprehensive fraud prevention platforms utilize a multi-layered approach, combining various detection methods to address threats across the entire ad lifecycle. However, effectively combating click fraud specifically requires defenses tailored to analyze and validate the click event itself, complementing impression-level protection. Protection must follow the user journey, not just the media buy. With new forms of fraud emerging in environments like retail media networks and in-app ecosystems, click fraud is expanding beyond traditional programmatic channels, and defense strategies need to evolve accordingly.



Threat Intelligence: Disrupting BADBOX 2.0 — A Sophisticated Botnet Fueling Click Fraud

Combating click fraud and sophisticated invalid traffic (IVT) requires constant vigilance. A prime example is BADBOX 2.0, a large-scale botnet uncovered by HUMAN's Satori Threat Intelligence and Research team and disrupted with industry partners.

BADBOX 2.0 is the largest connected-device botnet ever recorded: more than one million low-cost CTV boxes, tablets, and projectors left the factory with a hidden backdoor and were shipped to 222 countries and territories. Once powered on, these devices quietly joined a MoYu-run botnet that monetized them in several ways, including click fraud.

Investigators observed the malware pushing code that:

- Launches hidden WebViews to ad-heavy game sites controlled by bad actors.
- Steers the device to low-quality domains, automatically clicks display ads, then moves on.
- Renders ads in invisible layers while users watch legitimate content, creating fake engagement that looks human.

5.

The Evolution of Click Fraud Tactics in a Performance-Driven Ecosystem

The shift towards performance-based advertising models has led advertisers to prioritize concrete outcomes such as clicks, form submissions, app installs, and purchases, and introduced greater accountability and efficiency across the ecosystem, allowing for more precise measurement of return on ad spend and better alignment of media investments with results.

However, as performance became the primary currency of value, it also became the primary target for abuse.

Under impression-based models, fraud tactics focused largely on inflating impression counts using techniques like pixel stuffing, spoofing, hidden iframes, and ad stacking. As buying models shifted toward performance-based measurement, fraudsters quickly adapted their tactics to compromise more valuable metrics.

Click fraud was the first major wave. By generating fake clicks through bots, click farms, or malware, fraudsters could trigger payouts without delivering any real user engagement.

As buying models continued to evolve toward deeper-funnel outcomes—such as cost-per-install (CPI) or cost-per-lead (CPL)—fraud tactics became more sophisticated. Instead of simply clicking an ad, fraud operations began mimicking user behavior across the entire conversion path. These schemes now involve advanced tools and infrastructure designed to simulate legitimate engagement, complete with spoofed devices, hijacked sessions, and fabricated events.

Understanding the Ecosystem of Invalid Clicks

As click fraud tactics grow more advanced, it's important to understand the broader cast of players who benefit from click fraud and how their incentives and behaviors shape the threat landscape.

The modern fraud landscape is often characterized by specialization, where different actors focus on specific components of the fraud chain. For instance, some groups specialize in developing bots, while others provide critical infrastructure like large-scale residential proxy networks. This specialization creates a complex and interconnected ecosystem; for example, residential proxy capabilities enabled by the BADBOX 2.0 operation (referenced above on page 8) have been observed being leveraged by various other fraud operations, including Apollo.

Click fraud persists not just because it is technically feasible, but because it is profitable. Various actors across the advertising supply chain benefit—directly or indirectly—from inflated engagement. Whether through negligence, misaligned incentives, or deliberate abuse, these activities distort campaign data, drain media budgets, and erode trust between buyers and sellers.

Fraud Operators and Bot Networks

At the center of most large-scale click fraud schemes are professional fraud operators. These range from individual actors to well-resourced organizations. They deploy bots, click farms, and automation tools to simulate user behavior across digital campaigns. Their goal is to create fake engagement that appears legitimate to advertisers and platforms.

These operators often get paid through revenue-sharing arrangements with ad networks or publishers. In some cases, they operate under the guise of legitimate businesses, marketing their services as "traffic generation" or "engagement boosting" to unsuspecting clients. Their profits come both from direct participation in click fraud and from selling the tools and infrastructure that enable others to do the same.

Publishers with Conflicted Incentives

Not all publishers engaging with invalid clicks are malicious, but some are complicit—whether actively or passively:

- Publishers that monetize via CPC can see immediate gains from increased click volume, often yielding extensions to insertion orders and campaign renewals.
- Publishers that monetize via CPM, sold directly or programmatically, see tailwind benefits from increased click activity, which artificially enhances the perceived value of their inventory, enabling them to command higher CPMs, attract more buyers, and generally boost their standing within programmatic marketplaces.

Click Farms and Human-Driven Fraud

Unlike bot networks, click farms rely on low-cost human labor to execute fraudulent activity. These operations employ individuals to manually click on ads, install apps, or engage with content in ways that appear organic. Because the traffic originates from real devices and real people, it is harder to detect using traditional bot filters.

Click farms often operate at scale and offer their services for sale, serving multiple clients and campaigns simultaneously.

Ad Networks and Platforms with Weak Safeguards

Some ad networks and platforms may contribute to the problem by failing to enforce strong click controls such as behavioral analysis and real-time validation. In some instances, these failures stem from oversight or limited technical capability. In others, the platforms may benefit from inflated performance metrics, as higher click volumes can drive greater revenue through commissions, performance-based pricing, or perceived platform effectiveness.

When click quality safeguards are lacking, these platforms become enablers—either passively or intentionally—of widespread click fraud. This creates a conflict of interest where the same systems meant to deliver quality traffic can profit from fraud.

Competitive Abuse and Strategic Sabotage

Click fraud isn't always financially motivated in a direct sense. In some cases, it is used as a weapon. Competitors may intentionally target each other's ads with invalid traffic (IVT) to deplete budgets, distort performance data, or limit reach. These tactics are especially damaging in auction-based pay-per-click platforms, such as retail media networks, where wasted spend can lead to missed opportunities, competitive disadvantage, and lost market share.

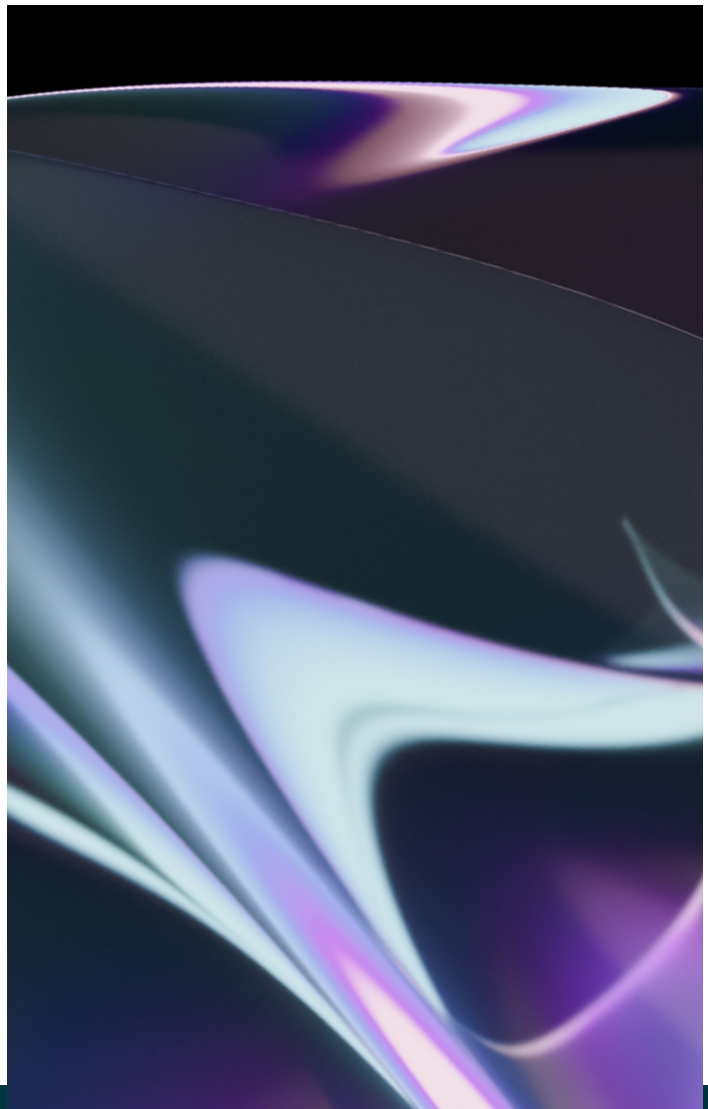
This type of abuse not only undermines fair competition but also puts additional pressure on advertisers to vet traffic sources and continuously monitor campaign integrity.

6.

The Unique Challenges of Click Fraud in Programmatic Advertising

The Lifecycle of a Click

In programmatic advertising, a click is often treated as a definitive signal of user interest— but it's just one link in a larger chain of interactions. A typical click involves a user engaging with an ad creative, triggering a redirect through a click-tracking URL, and (ideally) landing on a destination page. But what seems like a straightforward path is, in practice, vulnerable to technical issues and manipulation.



When a user interacts with an advertisement, they initiate a complex sequence of technical events that goes far beyond a simple tap or click. This process typically involves:

Initial Interaction

The user's tap or click registers on the ad creative, triggering client-side JavaScript that records device information, timestamp, and other environmental variables. However, JavaScript is not always present or executed reliably (e.g., in-app environments, privacy-restricted browsers, or when scripts are intentionally blocked), which can limit visibility into the event.

Click Redirect Chain

The interaction activates a sequence of redirects through multiple tracking endpoints:

- Primary click tracker call that records the event in the DSP or platform system.
- Secondary measurement pixels that notify third-party verification providers.
- Attribution trackers that establish the origin of the eventual site visit.
- Redirect mechanisms that pass campaign parameters to the destination URL.

Landing Page Request

The final redirect initiates an HTTP request to the advertiser's landing page, carrying UTM parameters and other identifiers that connect the click to its originating campaign.

Session Establishment

Analytics systems on the landing page create a new session, capturing referral information and connecting the inbound traffic to the click event that preceded it.

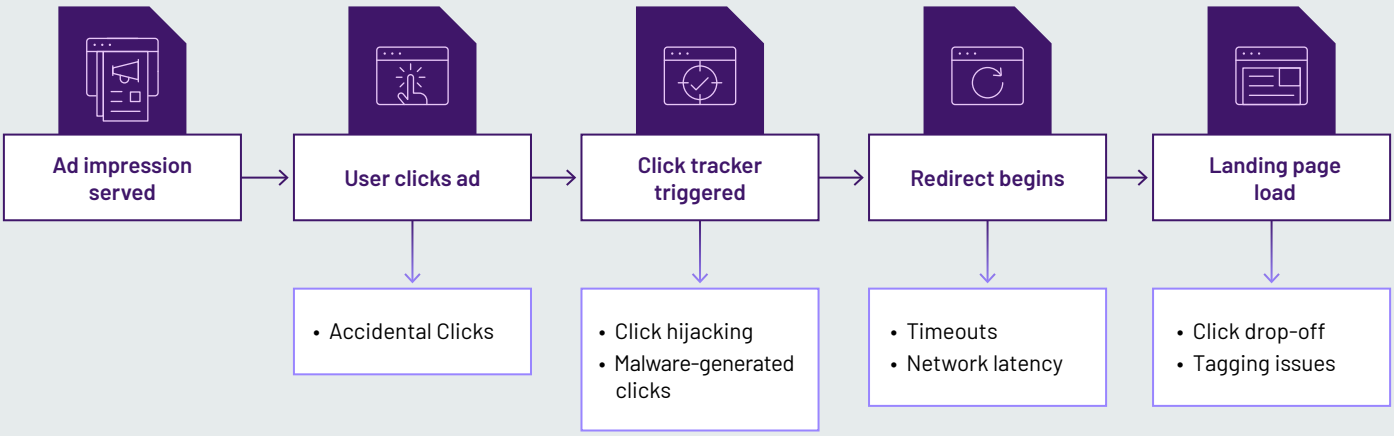
This intricate chain contains multiple points of vulnerability which sophisticated fraudsters can exploit. For example, a fraudulent actor might:

- Manipulate the initial client-side JavaScript to fire multiple click events from a single user interaction.
- Intercept and artificially trigger redirect calls without an actual user present.
- Extract tracking URLs from ad creatives and programmatically activate them outside of the intended delivery context.
- Inject false parameters into the redirect chain to misattribute traffic sources.

Each step in this process requires distinct protection mechanisms because exploits can target specific technical vulnerabilities at different points in the click lifecycle.

Many advertisers assume that a click logically equates to a landing page visit; unfortunately, deeper inspection and technical understanding of the click life cycle proves this assumption to be false. A click represents an action: the user (or bot) activating the ad. A page view, on the other hand, is a successful load of the landing page. Not every click results in a page view, and that drop-off can happen for a number of

Lifecycle of a Click: Key Events and Potential Issues



reasons: network latency, accidental taps, incorrect tagging, redirect chains timing out, or, in some cases, malicious interference. **Fraudulent actors have found ways to exploit the time and space between the click and the landing page to simulate engagement, effectively fooling various ad performance measurement systems.**

Click Drop-Off

Not every click leads to a landing page load—and yet not every click drop-off is fraudulent. Some clicks are accidental, some are disrupted by slow connections, and others are simply lost due to tagging misconfigurations or redirect loops. But when drop-off rates are unusually high, or when certain patterns repeat across traffic sources, these can be red flags for click-based fraud.

For example, a spike in clicks without subsequent user behavior on the landing page might suggest the use of malware or bots that trigger clicks programmatically without completing the redirect. In some cases, malware installed on legitimate devices can even silently generate multiple click events without the user's knowledge. Identifying these patterns requires analyzing traffic beyond the impression layer and understanding behavior after the ad is served.

Creative Validators and Pre-Bid Limitations

While traditional approaches to preventing click fraud often rely on analyzing either pre-bid signals or post-click landing page behavior, these methods leave a critical gap in protection. They miss what happens during the actual click event—those moments in the click life cycle when much of the sophisticated fraud occurs. This gap is further complicated by creative validators, which trigger clicks when scanning ads for ad quality and safety purposes. An effective click fraud solution must not only detect malicious activities but also properly classify non-human clicks from creative scanners as General Invalid Traffic (GIVT) rather than stopping the scanner from doing its job.

7.

How Click Fraud Affects Advertising Stakeholders

The interconnected nature of modern ad tech means that click fraud affects far more than individual campaigns. It undermines the trust that holds the digital advertising ecosystem together—trust between advertisers, publishers, and platforms. While each stakeholder plays a different role, all are impacted by the financial and strategic damage caused by invalid clicks.

Advertisers

Advertisers are often the first to feel the impact of click fraud, as fake clicks consume campaign budgets intended for reaching real customers. But the effects go deeper than wasted spend. Fraudulent engagement corrupts performance data, leading to flawed optimization strategies. Marketers may mistakenly increase investment in underperforming channels or scale back on those that are actually driving value.

This misalignment can persist well beyond the initial fraud event. Campaign performance models, audience segmentation, and attribution logic all rely on historical data. When that data is compromised, it distorts decisions months or even years later.

Publishers

Publishers, including content creators and media owners, rely heavily on advertising revenue to sustain their businesses. Yet they bear a disproportionate burden in maintaining traffic quality. A brief burst of invalid click activity can trigger automated platform penalties, ranging from disqualification from campaigns to revenue clawbacks. These clawbacks can be particularly destabilizing, requiring publishers to return income they have already booked and budgeted for.

Smaller publishers are especially vulnerable. They often face the same scrutiny as larger players but lack access to advanced fraud prevention tools, leaving them exposed to both fraud risks and enforcement actions.

Ad Tech Platforms

Advertising platforms, such as demand-side platforms, supply-side platforms, retail media networks, and walled gardens, depend on trust to maintain their place in the ecosystem. Advertisers expect these platforms to deliver scale and performance, along with safeguards that ensure the quality of results. When click fraud infiltrates their systems, it casts doubt on the platform's ability to deliver real business outcomes.

To preserve marketplace trust, platforms must continually strengthen fraud prevention measures while still delivering the efficiency and reach advertisers require. Falling short on either front threatens long-term credibility and confidence in the platform.

The Business Impact of Click Fraud

From campaign reporting to media planning and automated bidding, today's ecosystem runs on data. When that data is polluted by fraudulent activity, the consequences ripple outward, affecting every layer of advertising strategy and execution.

Distortion of Campaign Metrics

Invalid clicks degrade the accuracy of campaign data used for evaluation, optimization, and forecasting. In today's landscape, trust is built on accurate measurement:

- Advertisers rely on click data to evaluate campaign effectiveness and drive budget decisions.
- Publishers use click metrics to prove their value to partners and optimize content strategies.
- Platforms depend on clean, consistent data to power machine learning models and deliver performance at scale.

When invalid clicks contaminate this ecosystem, they don't just skew analytics dashboards—they interfere with predictive algorithms, conversion modeling, and automated optimization systems. The result is a breakdown in the feedback loops that modern advertising relies on to function efficiently. Over time, this leads to more conservative decision-making, reduced experimentation, and fewer opportunities for legitimate growth.

Waste of Advertising Budgets

Every fraudulent click diverts spend from legitimate traffic. These wasted investments mean fewer impressions, fewer conversions, and a lower return on advertising spend. While individual fraudulent clicks may seem insignificant, they accumulate quickly—especially in high-volume programmatic environments where small inefficiencies are magnified across millions of impressions and clicks.

The financial losses aren't limited to wasted media dollars. Click fraud also inflates customer acquisition costs, skews cost-per-action metrics, and can force marketers to reallocate budget away from high-potential channels due to artificially low performance indicators.

Damage to Optimization Algorithms

Modern advertising platforms rely heavily on machine learning and automation to allocate spend, personalize user experiences, and optimize outcomes. These systems learn by observing patterns of engagement: what gets clicked, what converts, and what doesn't.

Click fraud introduces false signals into those models. Optimization engines may mistakenly favor low-quality placements or audiences simply because they appear to perform well. This can lead to more budget being directed toward traffic sources that never had the potential to deliver meaningful results, compounding the damage and waste over time.

Erosion of Advertiser Trust

Click fraud ultimately undermines confidence in the ecosystem. When advertisers can't trust the signals they're using to make decisions, they become less willing to invest, test, or scale campaigns. This erosion of trust slows innovation, increases scrutiny on media buys, and puts pressure on both platforms and publishers to prove the legitimacy of their performance.

In some cases, persistent exposure to invalid traffic can lead advertisers to reconsider entire channels or partners, shifting budget toward more controlled or closed environments. This fragmentation reduces the efficiency and reach of open programmatic markets and limits opportunities for smaller players.

Protection Strategies and Solutions

Click fraud cannot be addressed with a single fix. Its impact spans across the ad lifecycle, with unique patterns that impression-level detection alone cannot identify. Even when an impression is verified as valid, the subsequent click can still be fraudulent through techniques like malware activation, click injection, or direct tracker manipulation. Protecting against click fraud requires a layered approach which goes beyond traditional invalid traffic detection and focuses on validating the click itself as a standalone event..

Most existing systems for detecting invalid traffic focus heavily on impression-level activity or analyze landing page engagement after the fact. These methods are valuable but incomplete. Fraud can occur independently from the impression, or long after it, and may never result in a valid page view. Fraudsters often use tactics that exploit weaknesses in the click path specifically—such as injecting fake clicks hours after a legitimate impression or triggering trackers directly without ever serving the creative. This is where click-specific defenses become critical.

To effectively address the complexities of click fraud, HUMAN recommends three core strategies:

1. Behavioral Analysis

Clicks generated by fraud tend to behave differently than those initiated by real users. Behavioral analysis focuses on identifying these subtle but telltale patterns. For example, patterns such as repeated rapid clicks from the same source, clicks that occur without corresponding mouse movement or touch behavior, and irregular timing patterns can all signal invalid activity. By examining how users (or bots) interact with the creative at the moment of engagement, platforms can distinguish legitimate interest from manipulation.

2. Real-Time Validation

Speed is critical. Many invalid clicks can still impact reporting, billing, and optimization decisions if they are detected too late. Real-time validation ensures that fraud can be detected and filtered before it has a chance to skew metrics or drain spend. HUMAN evaluates click behavior at the time of click, not just after landing page analysis. This real-time capability empowers platforms to make IVT decisions at the transaction level —filtering invalid activity from reports, billing systems, and automated optimization pipelines.

3. Actionable Insights

Beyond detection, click fraud prevention must deliver actionable results. Suspicious patterns like mismatches between click and impression timestamps or unexpected redirect chains signal potential manipulation. Advertising platforms need to be able to filter invalid interactions from billing systems and performance reports while integrating IVT decisions into dynamic optimization models for real-time campaign adjustments. The ability to classify both sophisticated (SIVT) and general (GIVT) invalid clicks empowers more precise fraud prevention and smarter campaign optimization.

8.

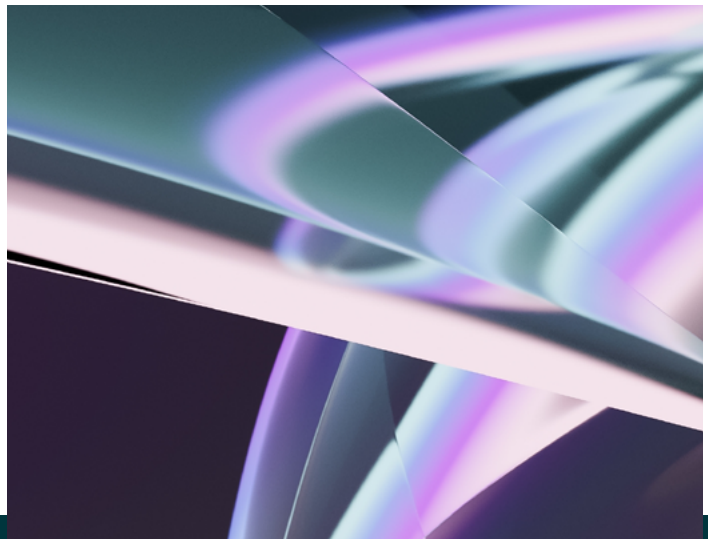
HUMAN + LinkedIn: A New Approach to Click Protection

After first integrating with HUMAN in May 2024 to enhance protection against invalid traffic, LinkedIn has expanded its protection framework to specifically address invalid clicks, which includes integrating with HUMAN's Ad Click Defense solution, further strengthening the accuracy and reliability of performance metrics across the LinkedIn Audience Network. This enhanced integration reflects LinkedIn's dedication to transparency, media quality, and performance metrics that advertisers can trust.

Advanced Click Protection: A Multi-Layered Approach

Protecting advertisers against invalid activity requires a comprehensive, full-funnel strategy. LinkedIn employs:

- **Proactive filters**, predictive signals and real-time decisioning to prevent invalid traffic and engagement before it impacts campaigns.
- **First-party safeguards** that block or down-rank suspicious activity based on patterns like anomalous click-through rate.
- **Independent post-bid validation** through HUMAN. This integration allows LinkedIn to filter any additional invalid impressions or clicks from billing that may have evaded initial filters.



LinkedIn's integration with HUMAN reinforces its commitment to protecting advertiser investments by providing them with reliable metrics that help them reach and engage decision makers with confidence.

Unlike alternative solutions that rely solely on device signals or landing page activity, HUMAN's approach evaluates actual click behavior in real-time with proprietary detection technology. As users engage with advertisements, Ad Click Defense identifies subtle indicators of both sophisticated (SIVT) and general (GIVT) invalid click traffic through advanced behavioral analysis including suspicious click patterns (such as multiple rapid clicks from the same source), behavioral anomalies (like clicks without expected mouse movement), timing inconsistencies, and discrepancies between click and impression data.

Performance Snapshot: Improving Invalid Traffic Detection

Since integrating HUMAN's Ad Click Defense in April 2025, LinkedIn has further advanced advertiser protection from invalid activity across the LinkedIn Audience Network. Over the first four months, HUMAN analyzed nearly half a billion clicks across display banner ad inventory (mobile, desktop, CTV, web, in-app), improving LinkedIn's invalid traffic detection by 10% and successfully identifying and filtering additional invalid clicks to protect campaign performance.

This integration demonstrates how LinkedIn's multilayered protection framework combines native safeguards with HUMAN's specialized behavioral click analysis technology. By incorporating HUMAN data into its filtering system, LinkedIn further enhances its ability to help ensure advertisers are not billed for clicks identified as invalid. This outcome reflects LinkedIn's dedication to traffic quality, platform integrity, and advertiser trust.

Profiling Invalid Traffic

HUMAN's initial analysis found that 54% of detected invalid clicks were classified as General Invalid Traffic (GIVT), for example creative scanners, and self-declared crawlers. The remaining 46% were Sophisticated Invalid Traffic (SIVT), originating mainly from automated browsing tools and false representation incidents where declared user information conflicted with observed behavioral signals.

Strategic Impact

Through this integration, LinkedIn and HUMAN have collaboratively established improved click validation across the LinkedIn Audience Network, enabling LinkedIn to identify and filter additional invalid clicks before they appear in advertiser reporting and billing. This additive layer of protection further strengthens LinkedIn's position as a premium advertising destination.

Looking ahead, over the coming months, LinkedIn and HUMAN are expanding their integration to apply these enhanced validation capabilities to additional formats and inventory across the LinkedIn Audience Network. This ongoing collaboration will continue to uncover new insights about emerging threats and traffic patterns, evolving alongside the changing digital landscape to ensure LinkedIn advertisers receive valuable and trusted performance.

9.

Best Practices for Advertisers

Integrations, such as those with LinkedIn, demonstrate how robust platform safeguards can protect advertisers from invalid clicks and deliver cleaner performance and billing data. But advertisers should reinforce these protections with their own checks. Use the checklist below to evaluate your click fraud posture.

Advertiser Click-Fraud Protection Checklist

Campaign Analysis

- Examine historical data for anomalies in click-to-conversion ratios, engagement rates, and spend.
- Flag warning signs: high CTR with low conversions, geographic mismatches, unusual time-of-day spikes.
- Monitor risk indicators such as sudden performance swings, unexplained budget drain or reporting gaps between ad platforms and analytics.

Protection Evaluation

- Trace the entire click path—from impression to landing page—to surface technical weak points.
- Audit existing verification tools for coverage of bot, incentivized-click and malware activity.
- Define non-negotiable solution criteria: behavioral-pattern detection, real-time decisions, easy integration, and clear differentiation between valid and invalid clicks.

Advertising-Partner Evaluation

- Ask partners to show how they detect and filter invalid clicks before billing and optimization.
- Verify their coverage of key fraud vectors (bots, click farms, incentive schemes, tracker abuse).
- Confirm they remove filtered clicks from performance data so machine-learning models stay clean and ROAS figures remain trustworthy.

10.

Future Outlook & Industry Implications

The Evolution of Click Fraud

The click fraud landscape will continue to evolve in sophistication as detection capabilities improve across the market. Fraud operators will develop increasingly advanced evasion techniques, leveraging intricate knowledge of ad network APIs to exploit system vulnerabilities while appearing legitimate to standard detection systems.

The tools available for conducting fraudulent activities are becoming more sophisticated and accessible. Powerful open-source solutions and emerging AI-enabled browsing capabilities provide advanced anti-fingerprinting techniques that significantly lower technical barriers to entry. This democratization of fraud tools will likely increase the volume and sophistication of invalid click activity targeting high-value campaigns.

Proprietary services offering comprehensive solutions for scraping and bot bypass continue to proliferate throughout the ecosystem. Beyond ostensibly legitimate companies providing components that can be repurposed for fraudulent activities, various malicious actors now offer turnkey solutions specifically designed for click fraud. This commercialization accelerates the spread of sophisticated methods that directly impact campaign performance metrics and budget efficiency.

The physical dimension of fraud remains significant, with click farms and datacenter-based invalid traffic continuing as dominant forms of click fraud across both desktop and mobile platforms. The advantage of controlling physical devices mirrors the benefits of controlling fully-fledged browsers—enhanced anonymity. Detection systems face substantial challenges distinguishing between genuine human interaction and sophisticated physical manipulation specifically designed to bypass verification systems.

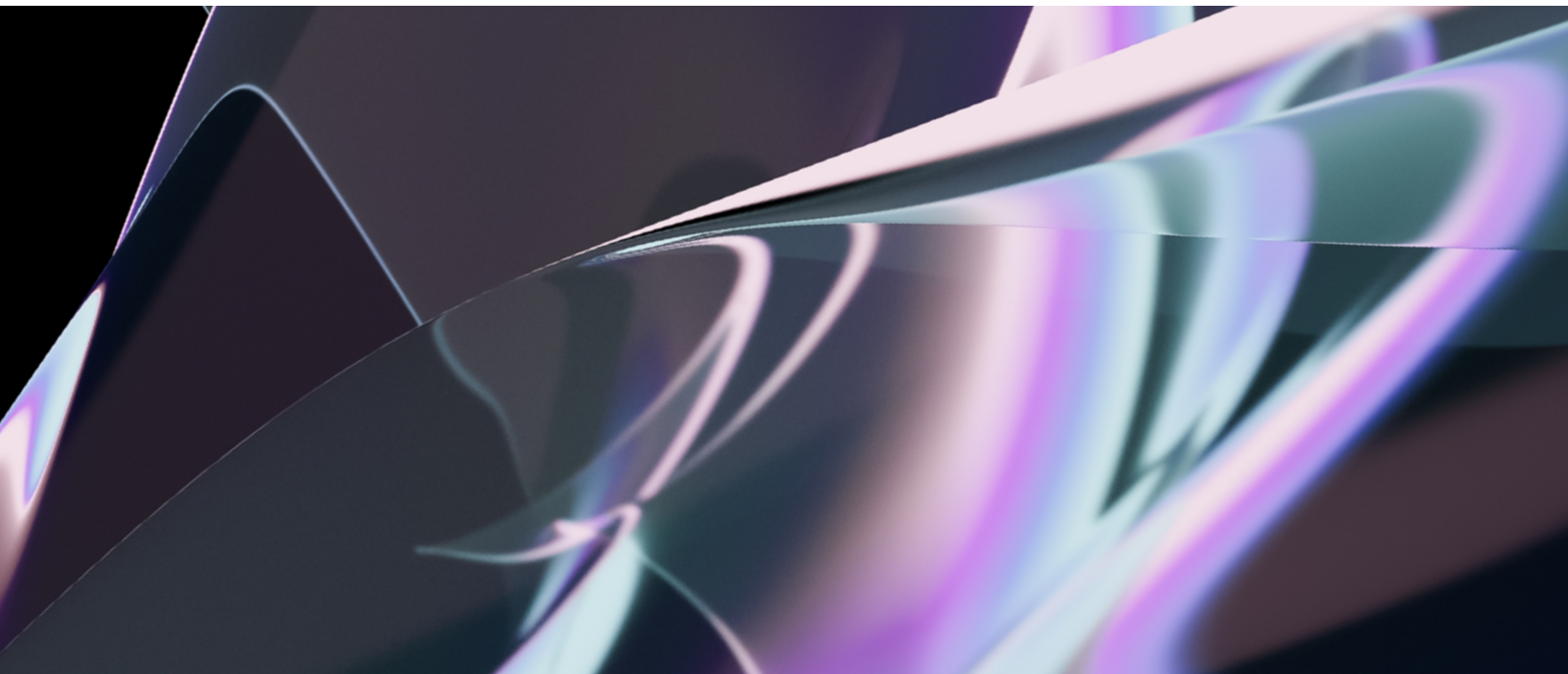
Malvertising will continue evolving as a multifaceted threat, combining security risks with click fraud capabilities. Operators will refine techniques for injecting malicious content into legitimate creative assets, establishing mechanisms to generate excessive clicks while potentially compromising user security. This blended approach allows bad actors to operate within seemingly legitimate advertising channels while manipulating measurement and attribution systems.

Industry Transformation

The digital advertising ecosystem will need to respond to evolving click fraud challenges. Performance-based buying models continue to drive heightened scrutiny of click validity, as every fraudulent click directly impacts campaign costs and ROI metrics. This will continue to place pressure on the ecosystem to implement click verification systems that maintain both the accuracy of performance metrics and the integrity of billing.

Collaboration is the next critical layer of defense. Stakeholders on the buy and sell-side must establish secure intelligence-sharing frameworks so new threats are neutralized quickly without exposing proprietary methods. A leading example is the HUMAN Collective—an alliance we launched in 2021 with founding members such as Omnicom Media Group, The Trade Desk and Magnite—that pools threat-intel feeds and joint response playbooks to raise protection standards across the ecosystem.

Regulatory frameworks may eventually emerge to establish baseline standards for click validation and reporting. These standards will provide clarity for navigating complex verification solutions while encouraging continued innovation in fraud detection.



11.

The HUMAN Advantage

HUMAN's Ad Click Defense analyzes the click itself—not just device signals or landing page activity. By observing click patterns in real-time and leveraging data from our global network, which processes over 20 trillion interactions weekly across 3 billion unique devices, it delivers high-precision detection of sophisticated click fraud.

As Abhishek Shrivastava, VP of Product at LinkedIn notes, "Embracing new solutions that help validate results is essential for advertisers to prove ROI." LinkedIn's implementation of HUMAN's Ad Click Defense demonstrates how leading platforms are prioritizing protection against the evolving threat of click fraud to maintain advertiser trust and campaign effectiveness.

12.

Conclusion

Click fraud protection represents a critical component of modern digital advertising strategy. Through understanding its nature, implementing comprehensive protection measures, and staying informed about emerging threats, the ecosystem can better protect advertiser investments and ensure campaign effectiveness.

The industry's continued evolution toward more sophisticated protection mechanisms, combined with increased collaboration and transparency, provides a strong foundation for the future of digital advertising.

By implementing robust click fraud protection strategies, platforms can maintain advertiser confidence while contributing to the overall health of the advertising ecosystem.