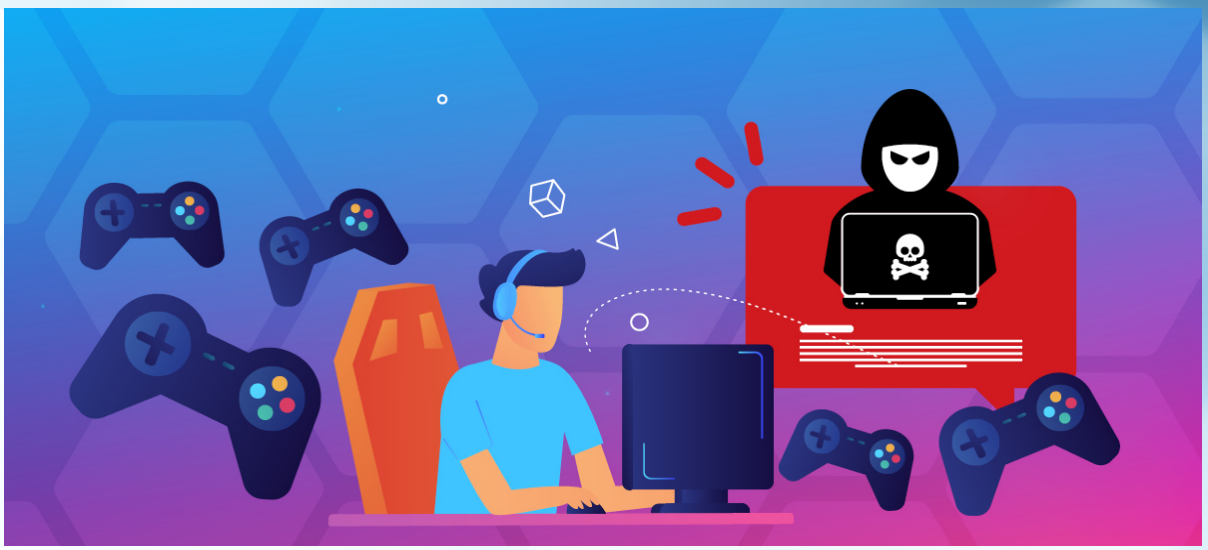
Gaming & Ad Fraud: 3 Part Series



Part 1: Preventing Online Game Fraud

We've extensively discussed ad fraud in various contexts, highlighting its detrimental impact. Regardless of the specific circumstances, the outcome remains the same: everyone loses when ad fraud is in play.

For instance, take fraud against gamers and companies in the online gaming industry. How could ad fraud impact the gaming industry? We're going to break that question down to its base elements, just as we would in any industry or segment.

We'll spend this series talking about this ever-growing industry, the companies that create the platforms, and the advertisers who desperately want to be in front of these gaming customers.

Do games attract consumers who are interested in spending money?

✓Check.

Does the industry trust its own defenses to protect itself from fraud?

✓Check.

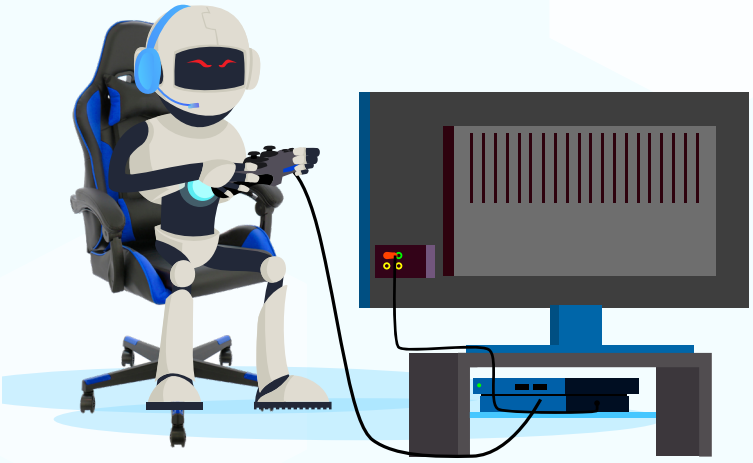
Is there an opportunity for creative fraudsters to use their skills and technology to monetize the pain of others?

✓Check.

An Overview of Gaming Fraud

Anyone who's purchased a game console in the last thirty years understands the nexus of their culture. Whether playing with friends on Fortnite, building a world on Minecraft, or training for the

military in Call of Duty, all of the popular games require disclosing a certain degree of personal information and, frequently, money exchanging hands.



As new games and gamers come online with these various platforms, the risk for all types of intrusions grows exponentially—for both the gamers and the platforms. In 2023, an estimated 3.07 billion gamers will be engaged in the industry, up from 1.9 billion in 2015. This sort of critical mass provides the impetus for fraudsters to find creative new ways to disrupt game designers and advertisers.

Any platform with automation set up to create and authenticate free or paid accounts can fall victim to bot or human click fraud. For example, when you look at the setup and function for games like Minecraft, APEX Legends, or HeartheStone—whether on desktops or mobile apps—they all require submitting a certain level of personal information to create an account online.

Further, gaming companies are under pressure to make it easier to create new accounts as gamers want less and less hassle to start or try a new gaming experience. Because of this push and pull, there's a constant balance between ease of use and security. And, unfortunately, we're seeing security being pushed down the priority list again and again.

The degree of fraud and exploitation in these environments is expansive. There are typically two types of fraud being committed:

1. Outright criminal fraud through intrusion and stealing of data, and
2. A more entrepreneurial type of fraud with fake accounts and accouterments being developed and sold on the black market.

Here's a quick overview of the many types of fraud targeting all the interests involved—the gamer, the gaming company, and the advertisers who play in the space between them.

Multiple Account Fraud

Multiple account fraud involves individuals who open different accounts on the same platform and use multiple logins to enrich or empower themselves inside the game ecosystem. At a Las Vegas casino in the real world, they would never allow you to sit across from a copy of yourself and play a game of poker. Online, the chance of multiple account fraud means this sort of fraud could and does happen, stacking the odds in favor of the fraudster.

Payment or Credit Card Fraud

Payment fraud is a more traditional type involving nefarious individuals actively trying to steal payment information from other gamers. They use fake accounts, not only inflating the number of accounts on the game but also creating chargeback situations that can negatively impact a gaming company's revenue. This type of fraud can affect the gaming companies' reputation and bottom line, hurting revenue targets and bogging down app installations.

Account Takeovers

Most of us are aware of account takeovers. The infiltration and impersonation of an account cross the line for both the gaming company and its gamers. Many of us have experienced it on a personal level, but it impacts the gaming company's reputation and sense of customer loyalty even more. It is worth noting that this type of fraud affects nearly one out of four of the 3.01 billion gamers online. Moreover, the impact of account takeovers can lead to other kinds of fraud. With access to a gamer's account, the fraudster can skillfully infiltrate the financial tools on the stolen account, and a takeover can lead to other types of fraud, including blackmail and illegal selling of the account.

Bonus Abuse

Bonus abuse is a more basic scam and a variation of multiple account fraud. Many of these games offer referral or bonus incentives that encourage users to build connections and a community. If a fraudster can leverage these bonuses by using multiple accounts, it can lead to waste and loss of game and ad revenue.

Affiliate Fraud

Affiliate fraud is not new and occurs in almost every industry. In the world of online gaming, affiliate marketing is an effective way to connect and grow. Unfortunately, the industry is also ripe for deceit. When you combine the power of ad fraud using automated bots with multiple account fraud, you have the possibility of rampant fraud. A calculated intrusion can cause real issues with ad budgets and revenue targets.

What Can You Do About Gaming Fraud?

How can these multi-billion-dollar gaming companies mitigate the risk of these types of fraud? Anura's technology is seamless. In a world where the user experience can make or break your game, Anura is in the background filtering out fraudulent traffic with 99.99% accuracy.

Removing up to 20% of the traffic—because it's fraudulent—would substantially impact gamers' in-game experience and game companies' revenue. Our free trial shows companies the true power of Anura. It can demonstrate—in real time—the amount of fraudulent traffic on your

platform and, as a result, what it's costing you when it's not adequately addressed or, even worse, ignored.

This type of fraud in the gaming industry is not going away anytime soon. Whenever a new authentication method is created or enhanced, fraudsters find ways around it. Filtering out the bad traffic while still allowing in the good traffic is the solution. Don't penalize users with a disjointed experience; use Anura to keep the traffic off your site before they even have a chance to get in.

Gaming and Ad Fraud Part 2: Online Game Companies Have to Win

Online gaming has always helped foster connections between people no matter where they are. This can also make them an easy target for online fraudsters. When the pandemic kicked into high gear, keeping people close when isolated created a rich environment for those with nefarious intent. Our overview of online game fraud demonstrated the most common types of fraud impacting the gaming world.

The industry shows no signs of slowing with the number of gamers expected to rise to 3.3 billion next year. The Entertainment Software Association estimates 65% of American adults play video games across various platforms. In addition, Deloitte found that 52% of Gen Z consumers and 46% of millennials routinely binge on video games. They rely on these platforms for entertainment and as a way to connect with family and friends.

With its impressive and expansive growth and revenue, game developers will remain a prime target for fraudsters. If left unchecked, fraud could eventually shut down the business model of online gaming by costing them more than their earnings. These attacks come on a variety of fronts, and the resulting impact on the bottom line and reputations can be catastrophic.

Consider the extreme popularity of Fortnite. Stolen game accounts and V-bucks (their in-game currency) are a $1 billion black market commodity! The good news is that there are ways game companies can fight back and protect themselves before disaster strikes.

What Does It Mean to Win?

Beyond earnings, game companies have to achieve a lot to be considered successful. They have to provide an entertaining and responsive gaming experience, build online communities, retain customer loyalty, and turn a profit. All while protecting their players and their company's reputation. The achievement of all of these goals relies on fighting back against online fraud.

Recognizing the Enemy

We've already explored the types of fraud affecting the game industry. Multiple Account Fraud, Payment or Credit Card Fraud, Account Takeover, Bonus Abuse, and Affiliate Fraud are all very real risks. The impact of online fraud on gaming companies is felt in a variety of ways.

Increased Need for Hard Resources:

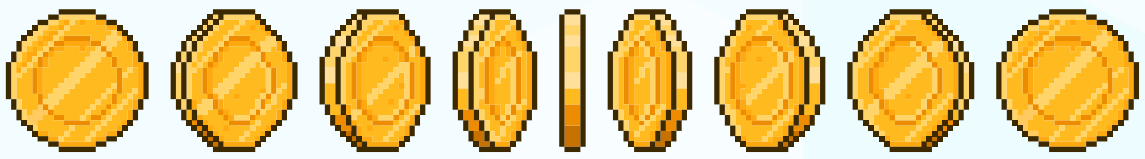
Bots use up resources and may necessitate additional hardware to keep the game responsive. Those additional resources could otherwise be dedicated to improving the experience for real players.

Degraded Experience:

When hardware can't keep up with the resource demand, the games can lag. Bots can degrade the in-game experience and drain precious resources, online and offline. The staff becomes focused on fighting fraudulent attacks and distracted from support and innovation.

Additional Overhead:

Dedicating employees to finding and fighting fraud can be expensive and diverts workers from providing support and focusing on innovation. An account takeover attack involving 500 players, cost one company over $60,000 in overtime and over a month to fix. Attacks like this are devastating on a large scale. Especially when you consider that some games can have up to 200 players ready to play at any moment.



Degradation of the Game Experience and In-Game Currency:

Using bots drains resources and available playtime without investing the same time and effort as legit players. This takes advantage of the in-game reward systems for prizes, bonuses, and even in-game currency. When bots collect rewards or currency too quickly, it can devalue, possibly even crash, the game's virtual economy.

With international games, hackers have also taken advantage of favorable exchange rates. Purchases can be made and then resold in more expensive markets using platforms like WhatsApp or Discord.

Increased Chargebacks:

Providing an easy opportunity for a variety of fraud practices can drive in a crushing number of chargeback claims. Online in-game shops are a prime target for testing stolen cards due to the small number of transactions.

Reputation Damage:

Trust is one of the most important aspects of consumer confidence. Degraded game performance and bots that compete fraudulently create damages that can be difficult to overcome. Not to mention the ad revenue hit that comes with reputation damage.

Making Sure Cheaters Never Prosper

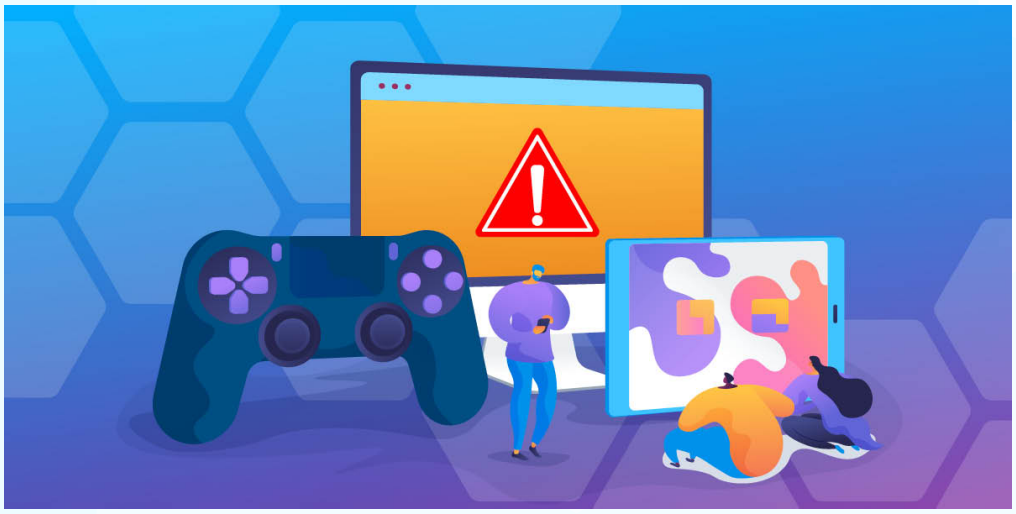
Companies can create a secure and effective platform with the right tools and strategies in their tech stack. It pays to stay one step ahead of malicious actors by improving existing security measures and staying informed about emerging threats.

Anura is well-versed in the techniques used by fraudsters. They can provide reliable and up-to-date tools and strategies for protecting game companies from these threats. In addition, having an online fraud detection tool like Anura can free up time and resources.

Anura's solution to combat online fraud has proven effective in every industry, including online gaming. Check out what Dennis Wierzbowski of Gaijin Entertainment had to say about his experience with Anura:

> We're running all of our relevant online traffic by Anura to eliminate user acquisition fraud for our online gaming titles. They have great and very responsive customer service that promptly handles questions and other inquiries. A definitive recommendation.

Anura's online, real-time fraud detection provides game developers with the tools for analyzing unauthorized game activity. With built-in machine learning capabilities, Anura's system monitors traffic to identify suspicious patterns and activities as they occur.



Gaming and Ad Fraud Part 3: Advertisers Should Level Up

In this three-part series focused on the gaming industry, we've provided a broad overview of ad fraud in online gaming and the threats that span across this industry. We have also explored what game companies must do to succeed and the challenges they face to make sure cheaters don't win.

Ad Fraud in Online Games

Ad fraud has always been a critical problem in the digital space for advertisers and marketers. Companies that advertise in digital channels are often at risk of wasting a quarter of their budget on ad fraud. Games provide audiences with a large potential reach for advertisers, so it's important that companies know how to protect themselves from risks when using them as an advertising channel.

In this blog post, we'll reveal the golden opportunity that online gaming presents and discuss ways advertisers can reduce the chance of falling victim to fraudulent schemes. With a better understanding of the opportunities and risks associated with game-based ads, you'll be poised to succeed without having to worry about the damage caused by those bad actors.

Online Gaming Is a Valuable but Underutilized Platform

The stereotype of who comprises the online gaming audience is now extinct. A majority of people now engage in video games on various platforms, with two out of three Americans participating.

According to Newzoo, gaming ranks as high as third place in how audiences spend their time (11.8 hours per week), barely being displaced from the top spots held by TV (13.9 hours per week) and social media (12.1 hours per week).

With the rise in gaming audiences and the amount of time they spend playing, advertisers would be wise to take advantage of it. It's clear that gamers are passionate and engaged, yet they remain largely overlooked by traditional marketing channels.

Gaming captures less than 5% of advertiser budgets. In 2023, ad spend in US mobile gaming is projected to grow 10.0% to $6.28 billion and remain steady between 8% and 10% over the next few years. While gaming ad spend grows, it is at a slower rate than other channels. Video game ad revenue grew by only 7% in 2022 from the previous year, while in that same period connected TV (CTV) revenue grew by 32% and social media revenue grew by 16%, according to data from eMarketer.

Ads That Are Valuable to Players Are Valuable to Advertisers

Looking at historical data, for more than a decade social and mobile gaming ads have outperformed traditional online ads by a shocking amount. While average click-through rates (CTR) may vary by product and industry, social and mobile gaming video ads have long proven to generate a CTR roughly 30 times higher than the CTR of banner ads.

In addition, social and mobile gaming "value exchange" ads (in which players receive a reward for viewing the full ad) generate an average CTR of 11%, which is more than 100 times higher than traditional online ads.

Clearly, ads can be more than just an intrusive presence. They can actually be used to create engaging, positive user experiences. By providing personalized experiences tailored to gamers, advertisers create a feeling of relevance and connection.

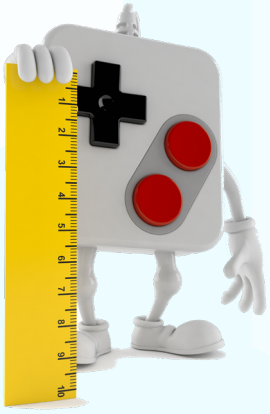
This encourages customers to explore content more deeply and for longer periods of time. An ad that is helpful, relevant, and easy to use can lead to satisfied customers who are motivated to return again and again.

In-game advertising today is more seamless than ever before. It creates an environment where both the ad creator and viewer benefit. In-game advertising can take many forms, including but not limited to: pop-ups, interstitials during gameplay; rewarded ads offering in-game rewards; native ads that blend seamlessly into the game environment; custom integrations such as product placements, virtual items, or even branded worlds.

Today, research by the IAB and eMarketer shows that 79% of consumers prefer opt-in advertising, while 71% of US mobile app users say that value exchange ads capture their attention more than any other form of advertising. Consumers are drawn to value exchange ads because they provide relevant rewards and also because the user has chosen to view the ad.

In order to build meaningful connections with consumers, it's critical to meet them on their terms.

Through the process of exchanging value for views in videos, you can foster a strong relationship with your potential customers—in fact, 76% of US mobile app users report that value exchange video ads make them like a brand more, and 73% say they want to buy a product because of it.



Changing Perceptions and Measurements

The Interactive Advertising Bureau® (IAB) looks to dispel five of the most common myths plaguing online game advertising. Their recent in-depth report, "Finding Success with In-Game Advertising: Perceptions of Buyers and Sellers," explores these misconceptions and makes the case why this valuable market deserves more investment.

While advertising campaigns frequently provide an easy way to measure ROI, online gaming offers unique opportunities for companies to grow their audience, brand awareness, and trust; and that requires new measurement guidelines for ads that appear within gameplay. By leveraging ads effectively, not only will you build meaningful connections with customers but also drive successful outcomes for all involved.

Advertising can be an invaluable asset for businesses, allowing them to form meaningful customer relationships. By strategically using ads and providing benefits, customers feel valued while businesses gain successful outcomes. With the help of advertising, both parties can reap the rewards—meaning everyone wins!

Strategies to Mitigate the Risk of Ad Fraud on Your Campaigns

While ad fraud has sky-rocketed in recent years, game developers are taking multiple steps to prevent it by implementing tools such as dynamic anti-fraud measures and analytics systems. This ensures that users have fair, fun, and safe gaming experiences every time they log into the platform.

Spotting potential fraudulent activities in online advertising can be tricky, but with a few key indicators, you can begin to identify risk factors. One of the first signs is an unusually high amount of online traffic with a low conversion rate and high bounce rate—this indicates that something is not quite right.

Furthermore, if you're seeing strange sources of online traffic that appear unrelated to your online presence, it may be a cause for further investigation. By taking note of these warning signs, you have the ability to protect yourself online and minimize online fraud.

Ad fraud can be costly and damaging for advertisers, so it is important to protect against it with anti-fraud solutions. Relying on a combination of trustworthy anti-fraud vendors, transparent publishers, and ongoing campaign performance monitoring are key best practices. Working in tandem with anti-fraud vendors allows you to take a proactive approach, as they can identify suspicious trends early on that may otherwise stunt your campaigns.

Transparent publishers give you the ability to understand where your ads are running and who might be trying to bypass anti-fraud protection. And lastly, regularly monitoring the performance of your ads will help you maintain control over any changes and identify problems before they become significant losses.

A great way to get up to speed is to work with a trusted advertising partner, such as Anura. As an industry leader providing safe, secure, and sophisticated ad fraud solutions, Anura helps protect your business from fraud with an easy user experience. To see all the benefits Anura can offer you, we invite you to request a free 15-day trial today.