TOP 3 WAYS **FRAUDSTERS** CAN TRICK YOU

How the mobile advertising industry gets hurt by malicious activities

www.optickssecurity.com

Opticks

Did you know...

...that in 2019, companies around the world suffered an estimated collective **loss of $42 billion** due to ad fraud? Mobile advertising has become an attractive target for individuals looking to make money quickly. Even after this considerable loss, there's a lack of awareness about the different types of Ad-Fraud and their impact to the mobile advertising industry.

Mobile ad fraud tends to be a tricky business. It is **difficult to identify** and even after it has happened, it's **difficult to prove** that any type of fraud occurred in the first place. This practice has become a rising concern. Think about it, as mobile ad spending grows, fraudsters are looking for new ways to get a share of their own. Their strategies have evolved quickly over the years and fighting them has become an ongoing (dare we say never-ending?) battle.

The team at Opticks has developed a deep knowledge of mobile ad-fraud and has become an expert in **identifying fraudulent behavior affecting marketers' campaigns before it happens**. There are different types of fraud that affect mobile advertising; each one varies in techniques and cleverness but in the end, have the same effects for marketers: an increase in budgets and a collection of misleading data for future reference and decision-making processes.

In this ebook, we gather the most common methods fraudsters use to trick advertisers and how to prevent them.

Harmful Applications

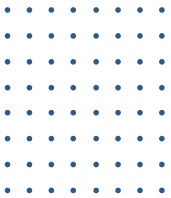
Harmful application is the industry term for **malware or virus on a mobile device**. Fraudsters use infected mobile devices to perform fake clicks and impressions, click spamming, unauthorized premium subscriptions, and other types of ad fraud.

According to Tech Radar, in 2018 there were over **116 million mobile malware attacks** detected; a volume that will continue to rise with an increasingly mobile world.

The most common way for fraudsters to transfer malware to users' devices is by using **compromised applications**. This means that malware operators choose popular apps, like weather or gaming apps, to infect a device.

These types of applications are usually found on third-party app stores with lower entry barriers that make it simple for fraudsters to offer malicious (infected) apps and are attractive enough to generate a lot of downloads. However, there is an **alarming increase in cases of harmful application inside the Google Play Store**.

Some signs of malware infections are pretty common, such as battery draining faster, pop up ads, a surge in data consumption, unexplained carrier charges or simply a reduced device performance, even if the infected app appears closed.



The best way to prevent fraudulent traffic from malware sources is to use a third party tool that analyzes your traffic and tells you what how many clicks, or even conversions, of your campaign are a result of those applications. These are not the types of conversions you should be looking for when launching a campaign.

The next step will be to either talk to your network or DSP to stop sending you traffic from those sources or use a prevention tool to blacklist them, thereby protecting your campaigns.

Campaign optimization shouldn't just be about CTRs or CPAs but analyzing where your traffic is coming from, and if you trust these sources or not. Stop spending your ad budget in fraudulent sources.

Opticks can detect and prevent traffic from devices infected with malware. Our machine-learning technology uses cloud intelligence to detect new threats and report unusual activity. This type of activity can be stopped in real-time without resulting in a fleet of (un-real) conversions from infected devices.

Bots

Bot fraud is a global issue that affects apps and websites across all industries. A single bot can simulate user behavior with extreme accuracy and with their evolution, they have become even harder to detect.

How do they work?

They are **programs that disguise themselves as real** (organic) human traffic generating fake clicks, fake social network logins, traffic with fraudulently obtained IP addresses, account takeovers, spam and many other forms of abuse. All with the goal to build large audiences of fake users, and consequently feed on the online advertising ecosystem.

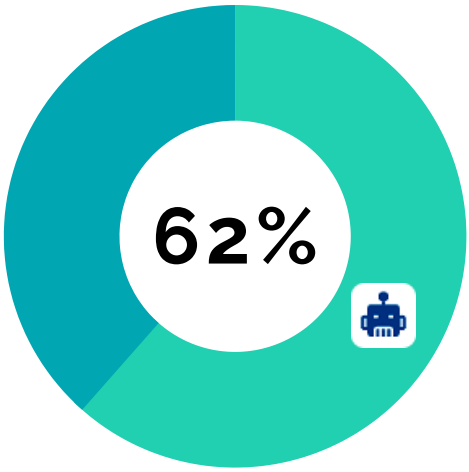
The monetary losses caused by bots are exponential within the advertising ecosystem. Ad spending flows through to the different exchanges (user, operators, networks, publishers, content creators). Problems arise when ads run on publisher sites with fraudulent traffic, including those where clicks are generated by bots instead of humans.

In this way, the advertisers are tricked to believe that a large number of real users clicked their ads while the ads never reach organic audiences.

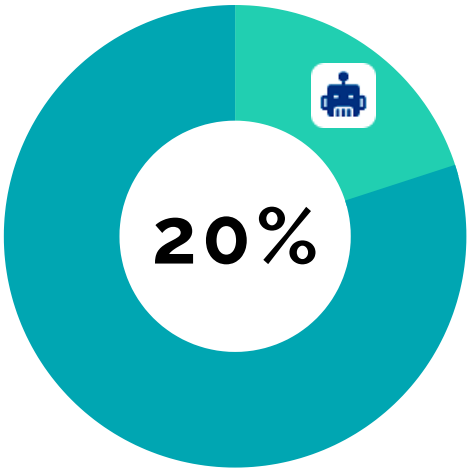
Bots are becoming more and more sophisticated, making detection increasingly difficult. As a matter of fact, more and more infected mobile devices are being used as bots instead of desktops and servers. Some Anti-fraud tools like **Opticks are able to identify bot traffic and allow users to block clicks** before they become a problem to advertisers, publishers, carriers or even the final user.

Traditionally, bots have been infected desktop computers or servers situated in data centers around the world. Data demonstrates the magnitude of this problem:

ONLINE TRAFFIC PRODUCED BY BOTS



AD CLICKS PRODUCED BY BOTS



Malicious Iframes

An **iFrame**, also known as inline Frame, is an HTML element that allows an **external webpage to be embedded inside another HTML**. It is often used to insert content from another source, like an advertisement, into a web page.

A malicious iFrame is a code inserted into a websites' search results, ads, pop-ups, and other items, agnostic to the website itself. When a visitor clicks a link from the compromised platform, he is **redirected or subscribed to a malicious site or tool**.

Another use for iFrames is when a **1x1 pixel is placed on a site**, sometimes through an ad unit. Unbeknownst to the user, these pixels can end uploading an entirely different website.

The site that loads out of view in a 1x1 iFrame often contains advertising - **none of which is ever seen by a user**, faking a genuine click

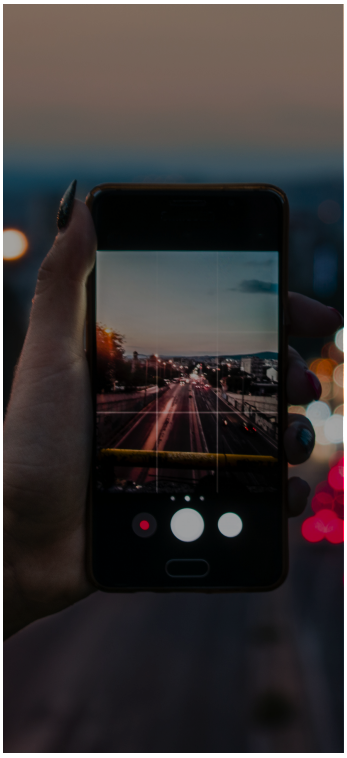
While this fraud method can be used to simulate false ad impressions, it's also often used in **affiliate marketing scams**, where the non-visible site tags the visitor and then gets to share the attribution of any conversion or purchase the user did on the website he is actually viewing.

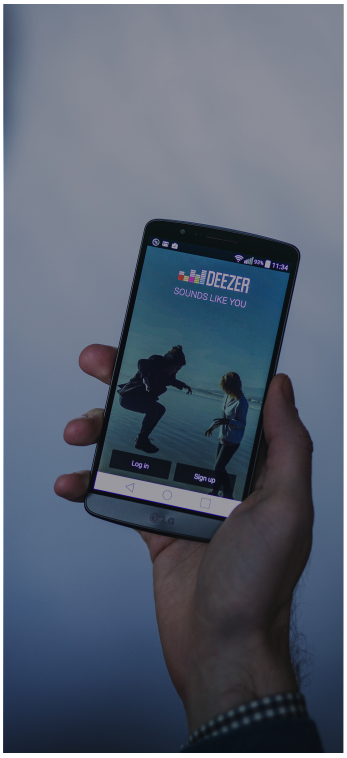
This results in fraudulent attributions and spending that can damage anyone in the mobile advertising value chain.

So what can we do to Stop Ad Fraud?

As we mentioned before, stopping ad fraud seems like a never ending battle between fraudsters and advertisers or third part tools, like **Opticks**, committed to create a **transparent advertising ecosystem**.

Ad fraud has become a serious problem permeating the advertising industry, and the **monetary and non-monetary losses it causes are exponential**. Even if fraudsters become smarter and smarter by the minute, this shouldn't mean advertisers should stop trying to mitigate their attacks.





Becoming a transparent and healthy mobile ad industry

How many times have we heard about fraud detection? At Opticks, we believe all industry key players, including Anti-Fraud tools like ourselves, should focus on **preventing fraud rather than detecting it**.

The reason is simple, by the time fraud is detected, **the budget has already been spent** and possibly collected by the wrong person; even worse, decision-makers are presented with misleading data about campaign performance and results. This is impossible to revert and extremely time-consuming for everyone involved.

By preventing fraudulent activities before they happen, we can eliminate dishonest attributions, tampered traffic, untrue conversions, and several other types of fraud.

Third party anti-fraud solutions like Opticks can act as a **preventive agent between the advertiser and network or publisher** by monitoring traffic and helping to mitigate or block, the effects of the aforementioned types of fraud.

Our proprietary technology is capable of **detecting the most advanced fraud techniques** and its ever-evolving machine learning nature keeps ahead of fraudsters at all times.

Our team believes that no anti-fraud tool alone can be responsible for stopping mobile ad fraud, however, we strongly agree that all agents involved in the advertising industry should work together towards a common goal: **to have a transparent mobile ad environment**.

Opticks

Opticks provides leading **brands. agencies and networks** with unmatched **antifraud solutions**. Ever-evolving machine learning and proprietary **fingerprinting** technology monitors your sources and helps you block **fraudulent** traffic before it depletes your budgets.

Our relentless mission is to deliver reliable and innovative software to beat digital fraud.

For more information on our solutions or to book a demo, contact sales@optickssecurity.com

www.optickssecurity.com