Trends in Mobile Click Fraud During COVID 19

CHEQ ClickCease

Mobile Fraud on the Rise during COVID-19 Epidemic

Marketers have suffered a 62% rise in mobile-device based click fraud attacking their ad budgets, during COVID-19, we reveal in this study. Of this mobile-based fraud, Android devices are responsible for more than two-thirds of invalid clicks which are draining millions from advertising budgets on paid search campaigns, such as Google and Bing. In this report, we analyze the state of mobile click fraud and rise during COVID-19.

Methodology

We analyzed more than 1.8 billion clicks across 5,000+ online ad accounts in 78 countries. The clicks were analyzed using the ClickCease fraud detection engine, set to uncover non-human, fraudulent or invalid clicks.

What is Click Fraud?

Companies purchase Pay Per Click (PPC) ads through contracts with online advertising platforms, most notably Google, under which businesses pay a certain amount of money for a particular number of clicks on PPC ads per day. Click fraud is the act of clicking on a pay per click advert with no intention of buying or using the product or service. It is either done by competitors in a cut-throat sector, with the objective to divert or negatively impact the advertiser's budget, or in an automated manner by bots.

The rise of mobile-based click fraud on paid search campaigns is part of a click fraud problem that will cost businesses $23.7 billion by the end of 2020. This challenge occurs as digital mobile commerce sales are vital to economic recovery of businesses, with mobile sales set to hit $2.92 trillion in 2020. However, as we shall see the majority of click fraud is mobile-based, increasingly threatening the ad spend that brings in sales.

The COVID Effect

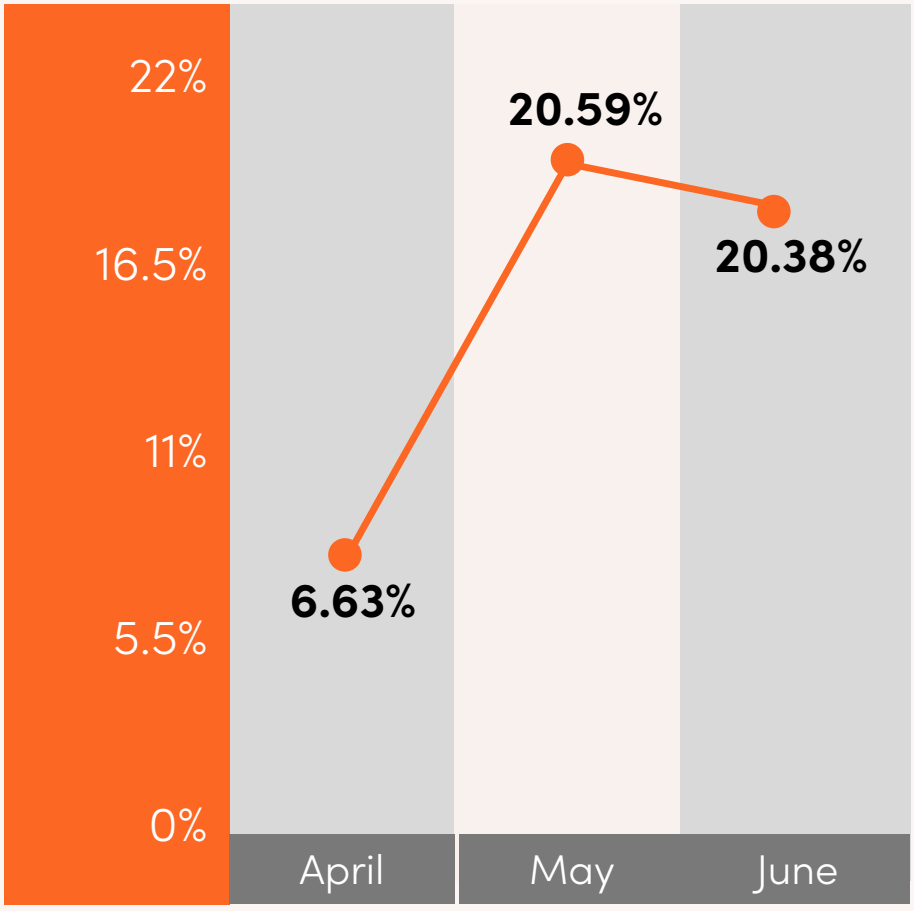
The total amount of invalid clicks (mobile and Desktop) is at an average of 14% across all countries examined and rose during the period of March to May 2020 as COVID struck and many economies were in lockdown.

In the United States, the rate of invalid clicks hit 14% during COVID-19 (rising from 11% pre-pandemic), the UK rose from 13 to 21%, while click fraud in Spain rose from a rate of 18% to 23% and in France reached a staggering 32%.

Mobile click fraud up from 6% to 20% during peak COVID months

We've seen a large increase in invalid / fraudulent traffic rates on mobile from April to May of this year.

Mobile Click Fraud



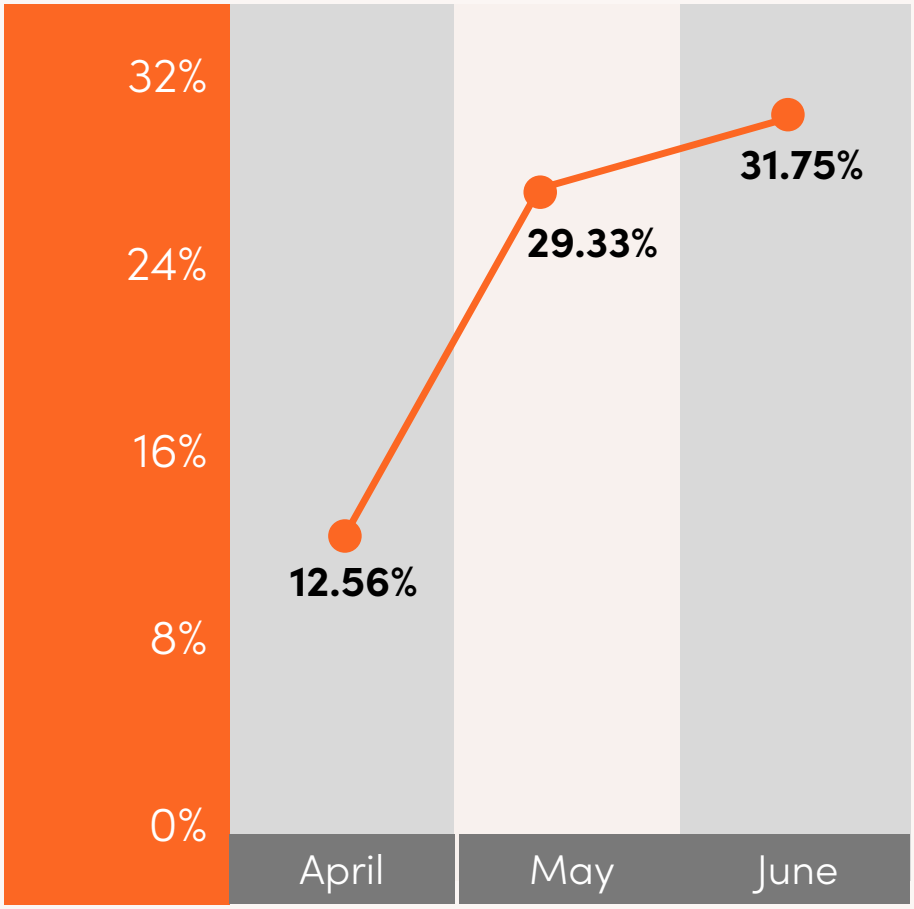
CHEQ ClickCease

Click fraud on Android devices up from 12% to 29% during peak COVID months

Of the total click fraud during COVID-19, by June 81% of mobile fraud originated from Android devices (compared to 19% for IOS devices). High rates of fraud are due to the fact that Android is an open-source platform, and malicious actors have low-level access to the system. In addition, rooted Android devices (the equivalent term for Apple devices is jailbreaking) generated significant fraudulent activity compared to non-jailbroken phones. In addition, high levels of mobile attack point to the rise of click farms.

This often involves rows upon rows of phones, automatically clicking through ad after ad. In addition, criminal groups are increasingly targeting users of Android mobile devices with malware for conducting ad fraud on a massive scale. This has been heightened with malicious applications, masquerading as innocuous coronavirus apps, designed to take control of your Android device. Threats hidden with these apps enable hackers to take intrusive control of your device to click on ads.

Mobile Click Fraud - Android



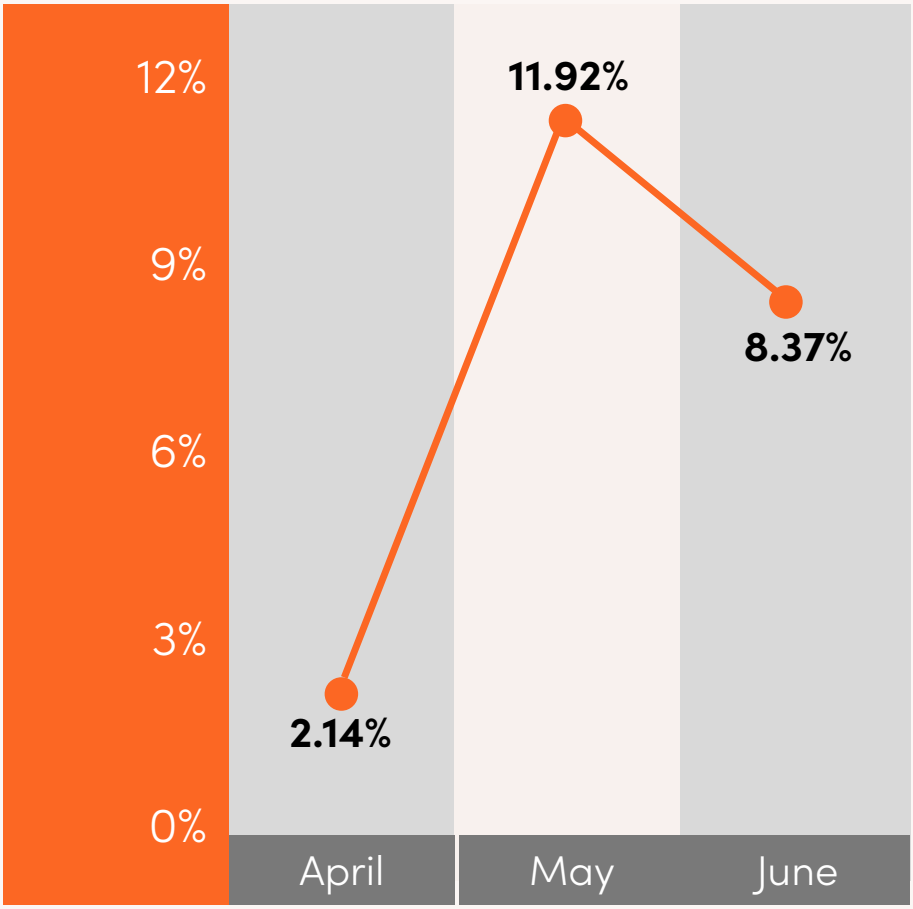
CHEQ ClickCease

Click fraud on iOS devices up from 2% to 12% during peak COVID months

Though in general Android makes up the vast majority of click fraud attacks, during May, IOS devices brought a spike in attacks against ad spend. There was a 56% increase in the use of IOS-based click fraud between April and May 2020. In fact we have seen that affluent and younger users of iPhones resorting to "competitor click fraud" - rivals clicking on paid ads with no interest in completing a purchase.

This correlates with what we have labelled “white collar click fraud” in particular lawyers and realtors seeking cut throat hacks to eliminate competition, with law firm click fraud rates rising by 30% during the period of COVID 19 lockdown, and realtors seeing a jump in invalid clicks on their online ads by 42% .Indeed with 80% of realtors reported to have an iPhone, and 75% of lawyers, IOS has emerged during COVID-19 as a rising weapon of click fraud against competitors.

Mobile Click Fraud - iOS



Stopping mobile fraud

When it comes to invalid clicks the vast majority now occur on mobile. This challenge continues to rise as digital advertisers seek to increase ad spend to recover economic growth. The rising challenges of mobile fraud encompass a broad range of threats: everything from manual competitor clicks, botnets, malware, click farms and other sophisticated methods to defraud advertisers.

While mobile provides a major source of bringing leads to businesses post-COVID-19, the threat of click fraud cannot be ignored. You can sign up for a free trial of ClickCease to find out for yourself how much automated or fraudulent traffic there is on your PPC ads.