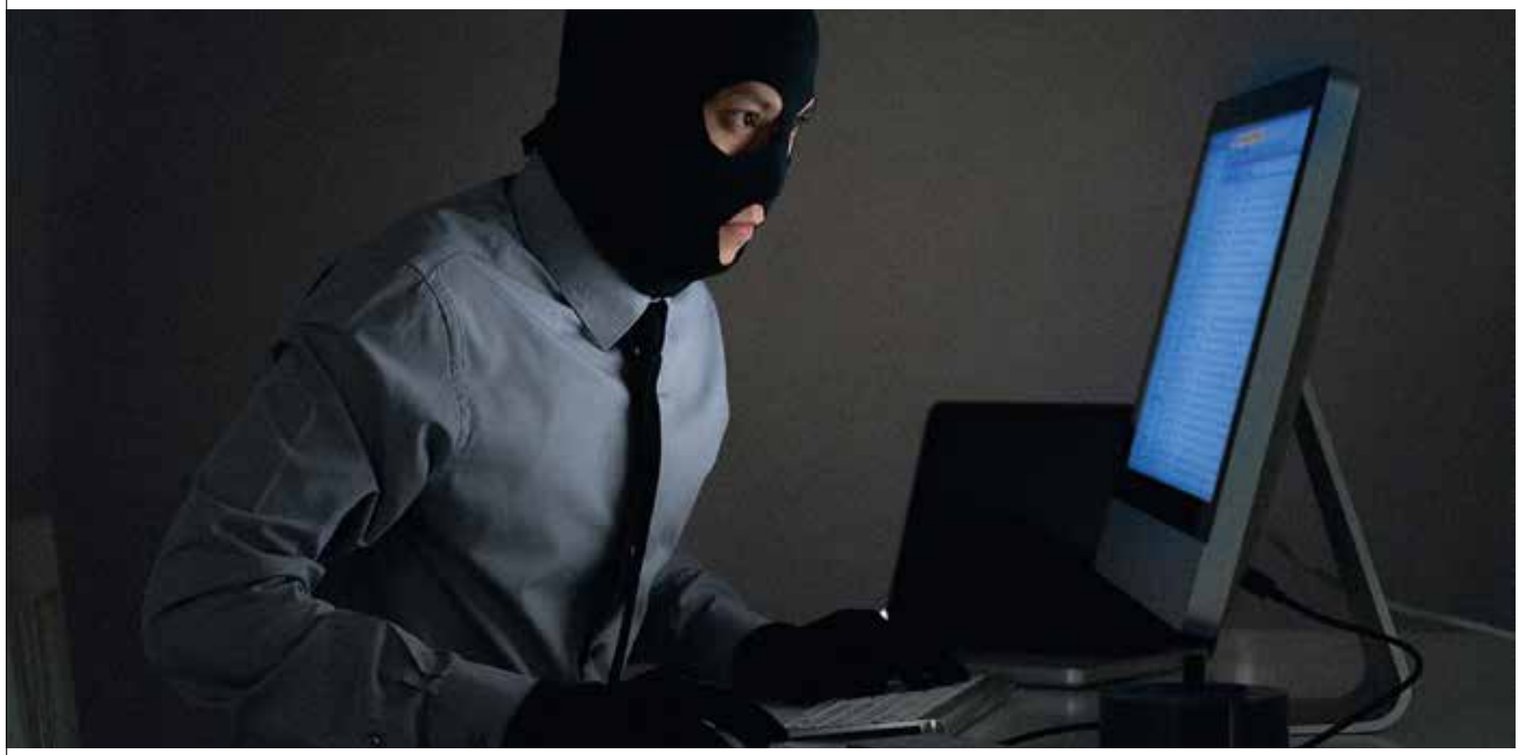
PAY-PER-CLICK SECURITY



Roy Dovaston *outlines measures companies can take to protect themselves from click fraud*

It has been reported that Uber recently filed a lawsuit against digital advertising agency Fetch over claims of click fraud; the fraudulent clicking of a company's online ads to deplete their daily advertising budget.

Frequently seen in the pay-per-click advertising world, this is a threat that can cost even the largest of companies thousands of pounds; as social media and subsequently online marketing have become an integral part of the public's digital lifestyle. It is, therefore, unsurprising that business owners are weary of such false traffic; click fraud is now endemic in the online advertising business – with some marketers claiming that up to 50 percent of their billed-for ads are generated by non-human traffic.

Click fraud may be encountered in various forms; for example, 'click farms' are often established in poverty-stricken countries – hiring staff at poor pay to manually click through your ads. Alternatively, 'click-bots' comprise of advanced software, which repeatedly clicks on ads without a computer owner's permission or human limitations; such as working hours or technology know-how. It, therefore, appears that click fraud is not only increasingly common, but ever-more versatile; degrading the success of online campaigns with ease. Unfortunately, it also seems that regardless of which methods are implemented – the source of such fraud often lies within the hands of your competitors; with the fundamental goal of diminishing your resources.

FALSE TRAFFIC

Within its lawsuit, Uber claims it asked Fetch in early 2017 to cease posting ads on all networks associated with Breitbart News due to seemingly false traffic. However, these mobile ads continued to appear – negatively impacting Uber's profits and digital campaign authenticity. The success of Uber's mobile advertisement is of particular importance, due to the nature of this business and being an app-based service hinged on the ease of its software for users across the world. Consequently, the millions claimed within its suit appears unsurprising and highlights the importance of pay-per-click security for all prosperous business reliant upon digital marketing – particularly as we now live in what has been dubbed 'the mobile and internet age'.

In addition, Fetch has since issued a counter-suit; suggesting that Uber merely began 'pointing fingers' at Fetch in an effort to increase its stature and avoid paying bills for services provided by numerous suppliers – totalling unpaid invoices of $19,736,925. Uber and Fetch are now embroiled in an ongoing legal battle; formulated on the basis of potentially untrustworthy sites and disingenuous clicks. This unnecessary dispute now hinders the development of these international organisations – and may have been avoided altogether.

Click fraud can cost even the largest companies thousands of pounds

In both cases, it appears that a substantial degree of money could have been saved, legal discrepancies avoided and brand awareness better protected if Uber's pay-per-click security had been more sufficiently managed and not automatically entrusted within the responsibilities of its advertisers. The use of in-house, savvy digital software may have allowed for a more successful screening process; while preventing against third-party discrepancies and eliminating the need for high external costs. Worthwhile protection efforts need not be extortionate; particularly when considering the affordability of online advertising itself.

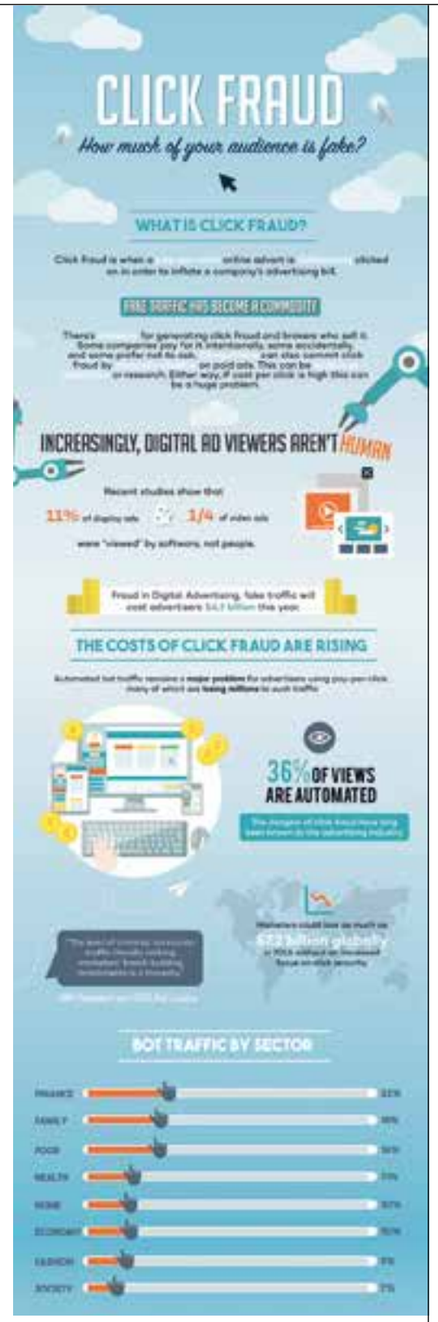
Despite this persistent concern, many businesses remain unaware of this ongoing threat to pay per click and may consequently fall victim to similar losses – not comprehending the ease with which their ads can be securely delivered if necessary measures are implemented. Similarly, it is not uncommon for small business owners when faced with news reports such as that of Uber and Fetch, to believe their organisation is not at risk. This

SOCIAL MEDIA AND ONLINE MARKETING ARE AN INTEGRAL PART OF OUR DIGITAL LIFESTYLE

simply isn't the case and all online organisations must invest in their online security.

Click fraud is fundamentally a criminal offence and so is prohibited across all marketing platforms, however it can be difficult to accurately distinguish between legitimate and fake clicks or to confidently assure click fraud has been entirely eliminated. In order to provide critical information with regards to click fraud prevention and better protect business' profits, here are some key ways in which this threat can be successfully eliminated within your digital campaigns.

Firstly; it may be argued that the most basic method of click fraud prevention is observing the behaviour of your competitors. You can monitor who is rivalling your keywords in search engines, for it is likely that these will be the businesses that are most inclined to be a potential source of competitor click fraud. However, while remaining vigilant with regards to your competitors is important, this does not diminish the extent to which you must monitor your own campaigns; on a daily basis it would prove useful to check your ratings for irregular spikes in clicks. For example, if over the course of several days your click-rating rises dramatically for no apparent reason, it may be necessary to delve more deeply into the source of said clicks. More specifically, the IP addresses these clicks are coming from.



When looking at the IP addresses appearing to click on your pay-per-click ads, it is useful to remember that these must all be different. Although a fairly obvious concept, this is essential in detecting fraudulence in its early stages. Your ad shows up for unique users every time and so there should never be duplicate IP addresses and if there are – this acts as an indicator for dreaded click fraud; in such instances, further action will be required. As a first step, limiting the damage caused by this pay-per-click fraud may be achieved by simply pausing your account until you can consider

appropriate further steps to take. This will prevent the wasting of your PPC budget – allowing for a strategic, carefully implemented response to this form of criminality.

It may also prove beneficial to limit the exposure of your ads by setting specific spending caps on your overall campaign or alternatively for your hourly or daily budget. This will allow for a regular evaluation of your campaign's success and will prevent any evident click fraud from greatly affecting your marketing budget. As well as this, use diverse or long-tail key words within your ads; particularly if your primary key words are highly sought after.

CHOOSING YOUR AUDIENCE

Once you have made essential alterations to your ads, accepting the unavoidable responsibility of checking them regularly in sufficient detail, it is necessary to consider the audience you are attempting to target. For example; notorious 'click-farms' as mentioned earlier are often developed in countries with low labour rates; as these can inherently provide workers for the sole purpose of clicking on ads, with little financial outlay. Due to this, it may prove beneficial to not run ads in countries where you are more inclined to experience such sabotage; strategically selecting those in which your target audience predominantly appears – most commonly the UK, Europe and the United States.

While being increasingly selective with regards to which countries you target, it is useful to select only high-value websites for your display ads. Many low-quality sites are notorious hotbeds for click fraud, as these themselves have less advanced security measures in place. Many pay-per-click platforms, such as Google AdWords, allow you to set up ad campaigns that only run ads on sites you approve. If this is not the case, proactive filtering may be required.

Finally, it may be argued that the most efficient method of click fraud prevention is the use of a click fraud prevention service or software. For example, Click Guardian offers a detection and protection service that monitors all clicks on your ads, tracks the behaviour of your visitors and automatically blocks AdWords if excessive clicking is detected. Once a block is issued, ads are no longer delivered to the perpetrator; meaning valuable advertising budgets will remain intact. The use of such proactive software eliminates pressure to prevent click fraud on behalf of business owners and managers alike who often solely react to an issue. Alongside this, the affordability of many external programmes allows for their use in any size of business.

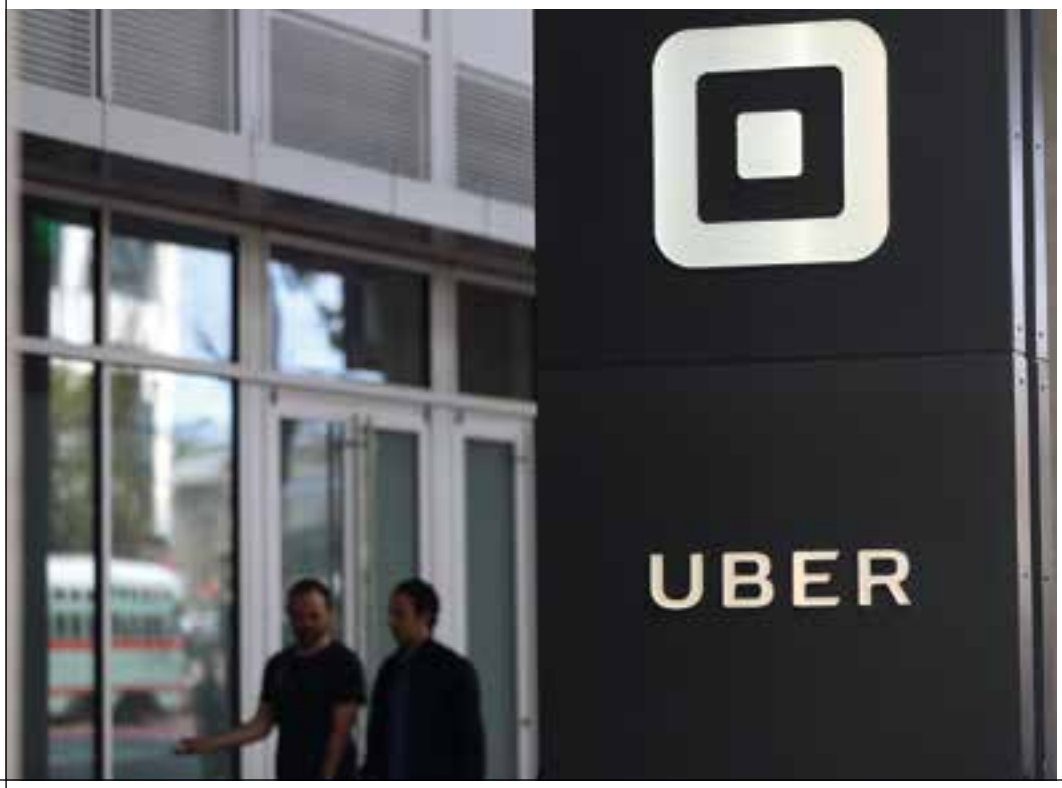
If faced with click fraud – in the absence of click fraud prevention software – there are several steps you can take. If necessary; you can block IPs on your campaigns or report the issue to Google: requesting a click investigation. However, as Google has recently been criticised for demonstrating "a very limited incentive to prevent third-party click fraud", reliance upon its security efforts may be somewhat in vain – enhancing the need for further measures.

IT CAN BE DIFFICULT TO ACCURATELY DISTINGUISH BETWEEN LEGITIMATE AND FAKE CLICKS

It may similarly be argued that the main hesitation with regards to the use of external software is the additional cost. However, when compared with the billions potentially lost in controversial lawsuits such as that put forward by Uber – this expenditure is necessary.

In conclusion, the ongoing threat of click fraud is on the rise and so business owners must consider their efforts to prevent such criminality within their own organisation. For a seamless prevention procedure, external prevention services prove to be the most efficient method of maintaining such security and should be considered within marketing strategies ●

Roy Dovaston is the owner of pay-per-click agency and anti-click fraud specialist Click Guardian. Having been managing Google Ads since the inception of Google AdWords, in 2014 Roy realised a major issue was going undetected in the form of excessive clicks on his client's ads. Click Guardian was born from this insight and now actively protects thousands of AdWords advertisers in the fight against click fraud.



Uber filed a lawsuit against digital advertising agency Fetch over claims of click fraud

Picture credit: Getty