Polygraph: Beware Of Click Fraud Protection Gimmicks

Cybersecurity firm Polygraph warns advertisers to beware of gimmicks which provide little to no protection against click fraud.

BERLIN, GERMANY, September 5, 2022 /EINPresswire.com/ -- Polygraph, a cybersecurity company specializing in click fraud detection, is warning advertisers to beware of click fraud protection gimmicks.

Click fraud is a lucrative online crime which steals tens of billions of dollars from advertisers each year. Criminals create fake websites, and monetize the content by placing genuine adverts on every page. Rather than wait for visitors to click on the ads, they use bots - software pretending to be human – to repeatedly click on the ads. These fake clicks, known as click fraud, generate huge profits for the criminals, and massive losses for the advertisers.

Polygraph helps advertisers protect themselves from click fraud, including detecting fake clicks, blocking scam websites, and getting refunds from the advertising networks. By following the criminals' playbook, Polygraph is able to eradicate click fraud and reduce advertisers' risk to zero.

According to Trey Vanes, head of marketing at Polygraph, advertisers need to be careful of click fraud protection gimmicks which offer little to no value.

"Polygraph puts a lot of effort into building systems which accurately detect and block real-world click fraud," said Vanes. "Unfortunately, there are a few click fraud protection gimmicks out there which sound good, but offer little value, as they aren't dealing with the reality of click fraud.

"For example, blocking IP addresses is often touted as an effective click fraud protection technique, when in reality blocking IP addresses misses more than 95% of click fraud. This is because most click fraud uses unique IP addresses for every fake click, meaning the same IP addresses will rarely if ever be used more than once.

"Another gimmick is pausing advertising campaigns whenever click fraud is detected. The idea here is the fraudsters will get bored and move onto a different target, rather than wait for your campaign to restart. The problem with this is almost all click fraud is automated, and the criminals are targeting your ad keywords rather than your specific ad campaign or company.

They probably don't even know your company exists. Therefore, as soon as you restart your ad campaign, the click fraud will continue.

"The correct way to deal with click fraud is to remove the at risk keywords from your campaigns, and block the criminals' websites from being able to display your ads. Polygraph makes this easy," said Vanes.

Vanes stresses that it's important to differentiate between "low quality clicks" and click fraud.

"Detecting click fraud is an objective science – either a click is real or fake. Unfortunately, some click fraud protection firms are flagging VPN traffic and high bounce rates as fraudulent. That doesn't make sense, as VPN use in and of itself has nothing to do with click fraud. Similarly, a high bounce rate can be due to many reasons, such as poorly written adverts and low quality landing pages.

"VPN traffic and high bounce rates should only be flagged as fraudulent if their corresponding ad clicks are fake. In other words, if the visitor is a bot or was tricked into clicking on an advert," added Vanes.

Polygraph uses a four step process which is both simple and effective at eliminating click fraud.

"Click fraud bots target hard coded lists of high value ad keywords. Polygraph monitors these lists, so we're able to warn our customers whenever their ad keywords are being targeted. Our customers simply remove the at risk keywords from their ad campaigns, and the click fraud bots go away.

"We also monitor the scam websites being run by click fraudsters, so we're able to provide this list of websites to our customers, who then block these websites from being able to display their ads. This is a powerful strategy for avoiding click fraud.

"Our bot detection software is designed to detect even the most cutting edge click fraud bots being used today. That means whenever the click fraudsters launch new websites, or change the ad keywords they're targeting, we're able to detect their click fraud and ensure our customers remain protected.

"Finally, we provide our customers with the details of every fake click (who, when, how), which can then be passed to the ad networks for click fraud refunds," said Vanes.

For more information, please visit https://polygraph.net

Trey Vanes
Polygraph
+49 160 98058592

email us here