Polygraph: Cyber Criminals Find New Ways To Target Online Advertisers

Click Fraud Prevention Firm Polygraph Uses Insider Knowledge To Tackle New Fake Clicks Scam Targeting Online Advertisers

BERLIN, GERMANY, May 4, 2022 /EINPresswire.com/ -- A growing trend where online fraudsters monetise popular advertising keywords, using real clicks by unsuspecting website visitors, can now be tackled by insider knowledge sourced directly from those involved with the cyber fraud.

While 'click fraud' is a relatively new type of crime, it is fast establishing itself as the premier method criminal gangs are using to make millions of dollars illegally.

English teachers working overseas have been recruited to create a respectable face for the operations, and often do not realise they are involved in fraud, as they are tricked into believing it is a legitimate business. One teacher who has spoken out about the scam said he was able to earn tens of thousands of dollars before cutting ties with the criminals once he realised it was fraud.

Polygraph has developed techniques for monitoring the activities of cyber criminals involved in click fraud, establishing methods for detecting and eliminating the fake clicks they use to profit from online ads. By using their own playbook, built using inside information on the techniques the fraudsters have developed, Polygraph's teams are able to protect advertising budgets, and eliminate further attacks.

Cyber criminals who use click fraud the most are targeting the three sectors which work closely together in online marketing; the advertiser, the publisher, and the advertising network.

With the advertiser paying for the 'ad clicks' and wanting to attract visitors to their website, they are at risk from click fraud which is committed by fraudsters posing as legitimate publishers.

The click fraud is committed by displaying adverts which use high value keywords – those in demand by advertisers -- and uses technology and trickery to force large numbers of web traffic to click on the ads.

The publisher receives money every time an ad is clicked, with the advertiser's fee split around 60/40 between the publisher and the advertising network.

By creating their own publisher accounts -- websites which display adverts -- the click fraud gangs are able to choose which ads are displayed and how many times they are clicked.

One industry targeted by the click fraud gangs is the 'pay day loans' sector due to its high paying ad keywords. Cyber criminals are displaying ads based on over 1,000 pay day loan related keywords, resulting in huge losses for advertisers.

According to Trey Vanes, Chief Marketing Officer at Polygraph, this new scam often stays under the radar due to its use of real web traffic.

"In the past the cyber criminals used bot traffic – software pretending to be normal website visitors – to click on the ads. But due to the recent rise in bot detection software, the criminals now frequently buy real website traffic and use trickery to force the visitors to click on the ads. This helps the fraud remain undetected, as it comes across as legitimate ad clicks by people.

"Each click only makes a small profit for the fraudsters, but multiply that by millions of clicks per day, and dozens of publisher websites, and the profits are massive."

By utilising the insider knowledge it has gathered, Polygraph can detect this fraud and help advertisers:

- tell which of their ad keywords are being targeted
- see which ad networks are sending the most fraud
- provide details of every fake click so they can get refunds from the ad networks
- block bots from seeing their Google ads

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

About Polygraph

Established in Berlin, Germany in 2021, Polygraph monitors the activities of click fraud gangs, including how they operate, who they target, the techniques they use, and how to detect their fraud. We go far beyond bot detection to ensure your ad budget is not stolen by cyber-criminals.

Contact Details:

Trey Vanes
Polygraph
+49 30 22044851
email us here