EINPRESSWIRE

Click fraud detection firm Polygraph warns advertisers of fake conversions scam

Polygraph has identified a fake conversions scam which organized crime gangs are using to hide their click fraud schemes.

BERLIN, GERMANY, May 27, 2022 /EINPresswire.com/ -- Click fraud prevention firm Polygraph is warning of a new cyber-crime targeting advertisers who offer no-cost products and services as part of their customer acquisition process.

“Some advertisers try to acquire customers by getting them to sign up to a mailing list or download a free report”, said Trey Vanes, Chief Marketing Officer at Polygraph. “Criminals use these free offers to help disguise their click fraud schemes.”

Click fraud is a sophisticated internet crime targeting online advertisers. Fraudsters place genuine advertisements on their scam websites, and use technology and trickery to generate massive amounts of fake clicks.

“The criminals earn a small fee from the advertising network every time an ad is clicked, so by generating thousands of fake clicks each day, they’re able to earn hundreds of thousands of dollars every month”, added Vanes. “Click fraudsters are stealing billions of dollars from advertisers every year”.

Some of the advertising networks, including Google Ads, are able to track advertisement conversion rates, meaning they can see which ad clicks resulted in a sale. According to Vanes, this presents a problem for the criminals, as their fake ad clicks never convert.

“The fraudsters often use bots – software pretending to be human - to click on the ads. These clicks are worthless, and will never convert into a sale at the advertisers’ websites. The ad network can see this, and will flag the criminal’s account as being suspicious.”

To get around this problem, the criminals manually generate conversions at websites offering no-cost products and services.

“The criminals try to find adverts for products such as reports or brochures which can be downloaded free of charge. They force those advertisements to display on their scam websites, and then manually click the ads and complete a conversion such as downloading the report or brochure. This tricks the advertising network into believing a real conversion took place, resulting in a reputation boost for the criminal's website.

"From the perspective of the ad network, these conversions are real, so they're fooled into thinking the fraudster's clicks are converting into real sales", added Vanes. "By mixing fake conversions amongst their fake clicks, the criminals are able to make their traffic seem real."

Polygraph helps advertisers monitor fake clicks, so any fraudulent conversions are easily identified. "By using Polygraph to monitor your ads for click fraud, Polygraph can tell you which clicks are fake, why they're fake, and where the click came from. Advertisers can use this information to prevent click fraud and get refunds from the ad networks", added Vanes.

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

Trey Vanes
Polygraph
+49 160 98058592
email us here