

Polygraph: 5% Of Marketing E-mails Are Opened By Bots

Bots are opening marketing e-mails as part of an elaborate click fraud scam.

BERLIN, GERMANY, December 12, 2022 /EINPresswire.com/ -- <u>Click fraud detection service</u> Polygraph is warning marketers about a click fraud scam which is causing marketing e-mails to be opened by bots.

Click fraud is an online crime which steals billions of dollars from advertisers every year. Criminals create websites and monetize the content using pay-per-click advertisements. Instead of waiting for real people to visit their websites, the criminals program bots to visit their websites and click on the ads. For each of these fake clicks, the advertisers pay money to the advertising networks, and the money is then shared with the scammers.

A challenge faced by the criminals is their bots never purchase anything at the advertisers' websites. This risks the advertising networks flagging the scammers' traffic as low quality. To get around this problem, click fraud bots are programmed to generate fake conversions at advertisers' websites, such as filling out leads forms or creating accounts.

According to Trey Vanes, head of marketing at Polygraph, fake conversions are causing marketing e-mails to be opened by bots.

"When a click fraud bot fakes a conversion by creating an account at an advertiser's website, the scammer receives an e-mail with a link to activate the account. To ensure these e-mails are handled correctly, bots are programmed to monitor the scammer's inbox for new e-mails, and click on any links in those e-mails," said Vanes.

"This tricks the advertisers into believing the sign-ups are real, so they start sending marketing emails to the scammers. These marketing e-mails are also opened by the scammers' bots, since they're programmed to open any e-mails and click on their links.

"Based on data collected from our customers, we can see roughly 5% of marketing e-mails are being opened by bots," said Vanes.

Polygraph helps advertisers <u>detect click fraud</u>, <u>prevent click fraud</u>, and get refunds from the advertising networks. Advertisers are shown which scam websites are clicking on their ads, so

action can be taken to block future click fraud. Additionally, details of every fake click are provided, such as which keywords are being targeted, and the click fraud techniques being used, so advertisers are given a complete understanding of their click fraud problem.

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

Trey Vanes Polygraph +49 160 98058592 email us here

This press release can be viewed online at: https://www.einpresswire.com/article/605889966

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire[™], tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information. © 1995-2022 Newsmatics Inc. All Right Reserved.