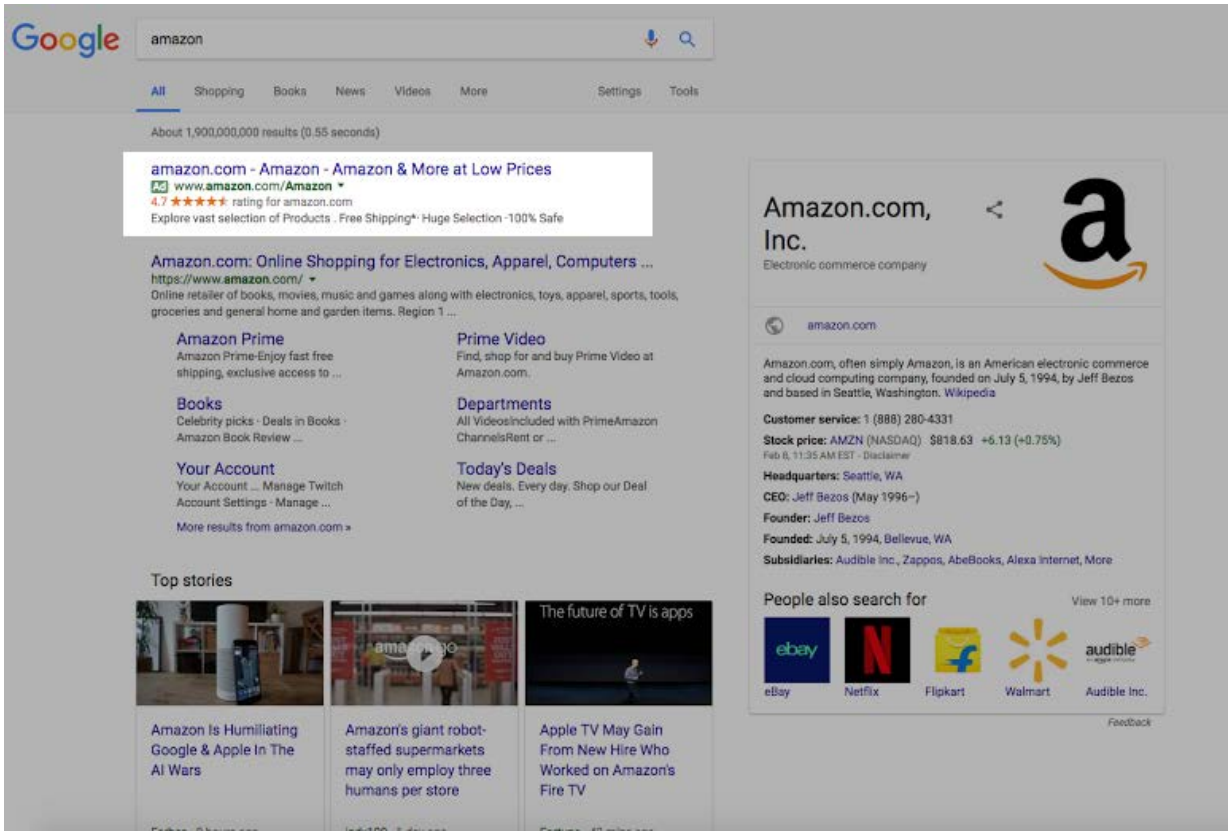
Google let scammers post a perfectly spoofed Amazon ad in its search results. Anyone who searched for "Amazon" were presented the rogue ad that aimed to trick users into falling for a **Windows support scam.**

By Zack Whittaker
February 9, 2017



Anyone who used Google search to look for Amazon, the internet retail giant, on Wednesday (2/7/18) was likely served a malicious ad -- and didn't even realize it.

The good news is that unlike other rogue ads, your machine wasn't infected or served malware in any way.

But anyone who clicked on it would not have been sent to Amazon.com as they would have hoped, but instead, they were pointed to a fake Windows support scam

posing as Microsoft. From there, scammers would have tried to trick the user into calling a number for fear that their computer was in fact infected with malware.

The ad appeared at the very top of the Google search result for anyone searching for "amazon," and it appeared above the legitimate search result for Amazon.com.

It's not known how many people may have seen the ad, let alone clicked on it. But according to Google's own most recent statistics, Amazon is the top search result as of the most searched for retail store on the search engine -- likely accounting for millions of searchers. But how a rogue and malicious ad got through the various levels of vetting required, let alone for one of the company's most sought-after and high-ranking ad units, remains a mystery.

On its own, Google took down 1.7 billion ads that violated its advertising policies in the last year, according to its blog. We examined the rogue ad with a tracer tool. The paid ad, served through Google's own ad network, appears to resolve fully to Amazon.com -- likely to trick Google's systems into accepting the rogue ad.

But, when a user clicks on it, the ad points them to the scammer's website.

The haphazard and unruly-looking page automatically detects the operating system you're using and displays differently. (Windows users are presented with a Microsoft-branded, blue-screen-of-death, while Mac users are told that their systems have been hit by crypto-ransomware.)

And if the user tries to exit the page, a popup will appear with a script that keeps adding random characters to the web address, forcing in some cases the browser -- and the computer -- to freeze. Depending on which browser or operating system you use, the page may forcibly go full-screen and prevent clicks, based on our testing.

These scams aren't uncommon. The Federal Trade Commission and other government departments have for years pushed back against these kinds of scams, which often result in malware or ransomware being installed on your computer. Scammers then force unwitting victims to pay up to have the malware removed.

We confirmed at the time of publication, however, that the ad no longer appears, but the website hosting the scam -- which we are not linking to -- remains active.

A Google spokesperson said that the company doesn't comment on specific ads.

Amazon did not return a request for comment prior to publication.

http://www.zdnet.com/article/malicious-google-ad-pointed-millions-to-fake-windows-support-scam