

Sneaky Amazon Google ad leads to Microsoft support scam

By [Lawrence Abrams](#)



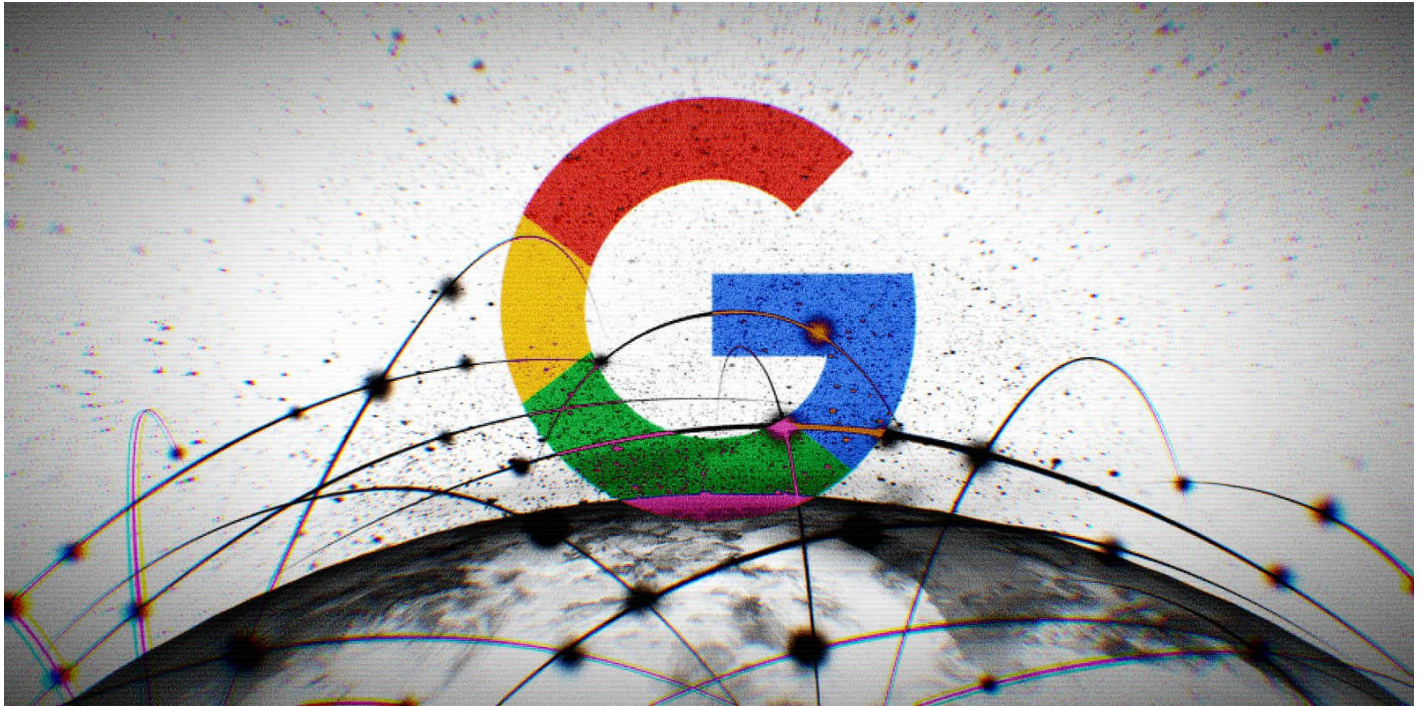
August 21, 2023



01:52 PM



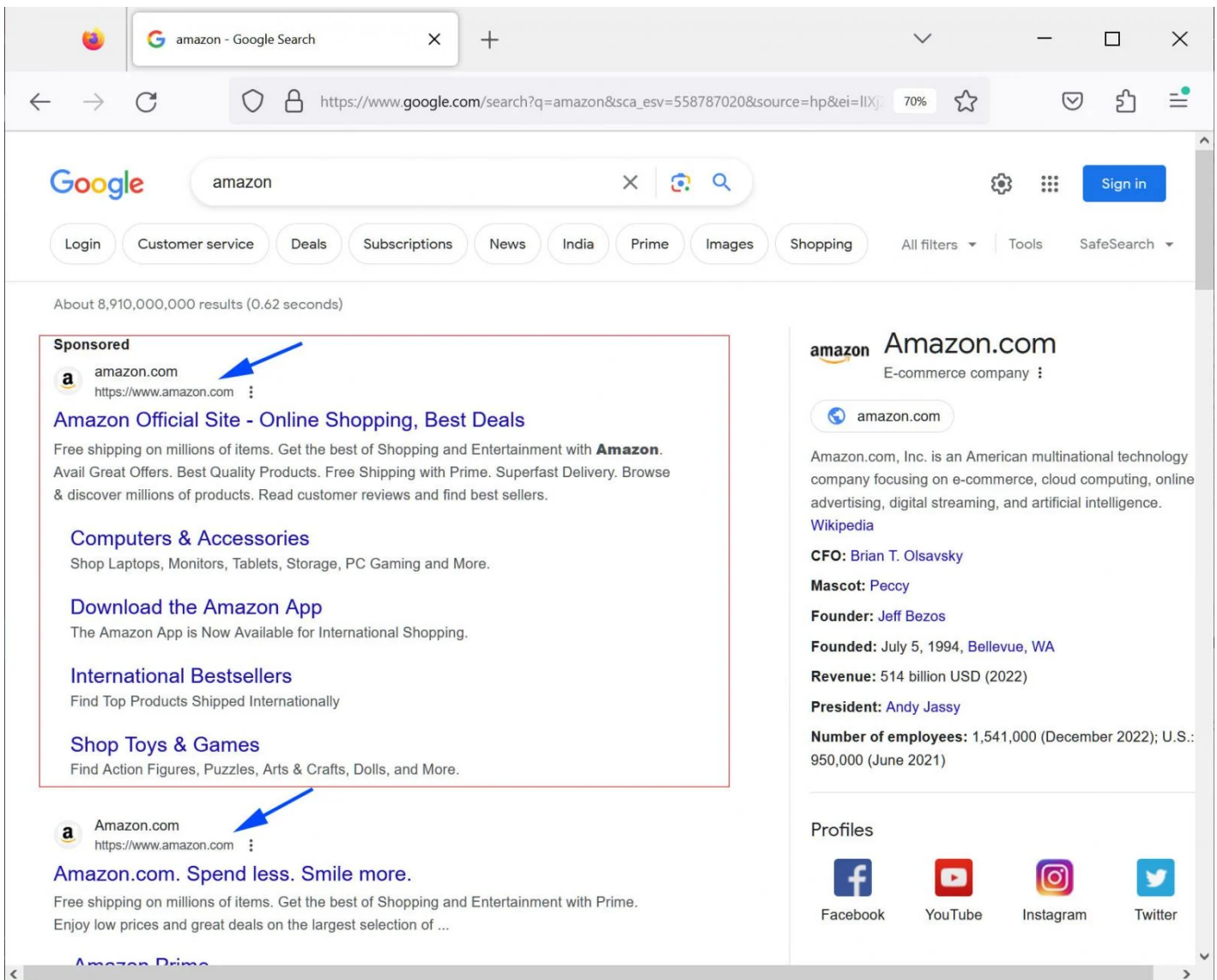
6



A legitimate-looking ad for Amazon in Google search results redirects visitors to a Microsoft Defender tech support scam that locks up their browser.

Today, BleepingComputer was alerted to what appeared to be a valid advertisement for Amazon in the Google search results.

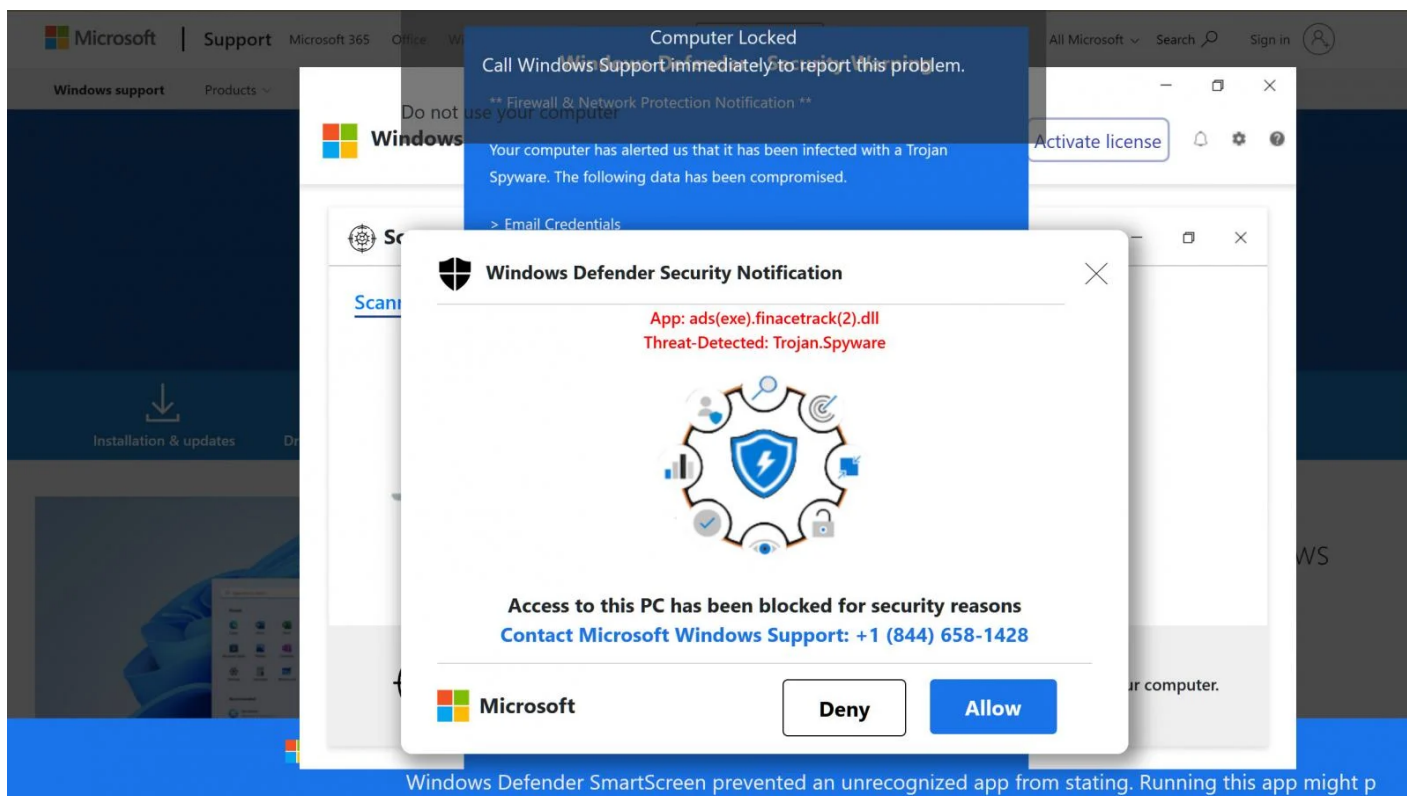
The advertisement shows Amazon's legitimate URL, just like in the company's typical search result, as shown below.



Fake Amazon ad in Google search results

Source: BleepingComputer

However, clicking on the Google ad will redirect the person to a tech support scam pretending to be an alert from Microsoft Defender stating that you are infected with the ads(exe).finacetrack(2).dll malware.



Tech support scam from fake Amazon ad

Source: BleepingComputer

These tech support scams will automatically go into full-screen mode, making it hard to get out of the page without terminating the Google Chrome process.

However, when Chrome is terminated in this way, on the relaunch, it will prompt users to restore the previously closed pages, reopening the tech support scam.

A demonstration of today's fake Amazon Google ad leading to the tech support scam site can be seen below.

In June 2022, Malwarebytes discovered a legitimate-looking YouTube ad that also used the platform's URL, leading to the same [tech support scam](#).

It's unclear why Google allows advertisers to impersonate other companies' URLs to create these convincing advertisement scams.

Google ads abused to distribute malware

BleepingComputer reached out to both Google and Amazon regarding this malvertising but has not received a response at the time of this publication.

Google advertisements have been heavily abused over the past year by other threat actors to distribute malware, which sometimes leads to ransomware attacks.

The threat actors would create replicas of legitimate sites but swap the download links to [distribute trojanized programs that install malware](#).

The Royal ransomware operation also creates Google advertisements promoting [malicious sites that install Cobalt Strike beacons](#). These beacons are used to provide initial access to corporate networks to conduct ransomware attacks.

AMAZON

GOOGLE

GOOGLE ADS

MALVERTISING

TECH SUPPORT SCAM



LAWRENCE ABRAMS

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

< [PREVIOUS ARTICLE](#)

[NEXT ARTICLE](#) >

Comments



Mahhn - 12 hours ago



"It's unclear why Google allows advertisers to impersonate other companies' URLs to create these convincing advertisement scams."

MONEY - its why they put up adds for criminals impersonating our FI, we also pay for adds on Goog. We called them, they REFUSED to take the scam adds down because they were paid - so we went after the web host - who took the fakes sites down immediately. Goog supports criminals and loves their money. There is no doubt as the fact is they do this.



Knight_of_BAAWA - 11 hours ago



I keep telling my customers who fall for these things to STOP clicking on the first link they see. While it may not prevent all of these, it should stop most.

Also: why do people search for sites like Amazon instead of just typing amazon dot com?



iam-py-test - 11 hours ago



This is why people should just software to block ads. Obviously there are other ways to end up on tech support scam sites, but that at least a good content blocker should kill off Google search ads and any malware which comes with them.



Dominique1 - 7 hours ago



A www.googleadservices.com redirection. :facepalm: Very sneaky! This kind of links are used everywhere for phishing because they are trusted by email clients and people. Google need a mega Class Action Suite for not having a reliable and secure redirection service.



johnlsenchak - 6 hours ago



It would have been nice to show the redirect URL information for research purposes



dave_2023 - 4 hours ago



Google seems to be the worst, and have been for many years. This probably won't change until a government legislates to make it a crime for malware to be promoted in search results.

As others have said, use NoScript extension or other adware blockers to stop this.

Many browsers claim to warn against sites with malware. So Google takes money from the badguys to promote their links to malware, then warns you after opening the links?

That's why I don't use Google for anything.