Don’t Click Google Adverts!

Online ads are often annoying, but now they've become dangerous as well. In the past six months, Google search results have been invaded by fake adverts that infect your computer with malware and steal your private data, and the problem appears to be getting worse. Even searching for the latest versions of your favourite programs puts you at risk from these increasingly sophisticated and convincing scams. Here we lift the lid on this fast-growing threat, and explain how to avoid clicking malicious ads.

What's gone wrong with Google adverts?

Last July, cybersecurity company Malwarebytes reported that fraudsters were abusing Google's advertising network to run 'malvertising' campaigns, which trick web users into clicking fake ads for well-known brands. See this site for detail.

Since then, the hijacking of Google search ads for malicious purposes has escalated, and gone beyond the usual tech-support scams to fool users into downloading malware that steals their personal data. The most common fake ads are for popular programs including 7-Zip, Audacity, CCleaner, LibreOffice, VirtualBox, VLC Media Player and - most recently - the password managers IPassword and Bitwarden.

Scammers pay for these ads to appear at the top of Google search results, and give them convincing titles, descriptions and URLs, so that unsuspecting users click the links, believing they'll be taken to genuine software websites.

What happens if I click these ads?

Clicking a fake advert typically takes you to a mock-up of the software's official site that contains an apparent download link for the program - or the download link may appear in the ad itself. When you click this, it installs a malicious script in your browser that connects to the hacker's server and downloads malware to your computer. According to security news site Bleeping Computer, this malware "collects sensitive data from browsers (credentials, credit card, autocomplete info), details about the system (username, location, hardware, security software available), and cryptocurrency", while other sources have reported ransomware being installed on victims' PCs.

Is it easy to spot fake Google ads?

These ads take advantage of the fact that many Google users click the top results for their searches without checking them first. Although some contain tell-tale spelling mistakes or use obviously fake URLs, many look almost exactly like the real thing and use descriptions copied from legitimate software websites

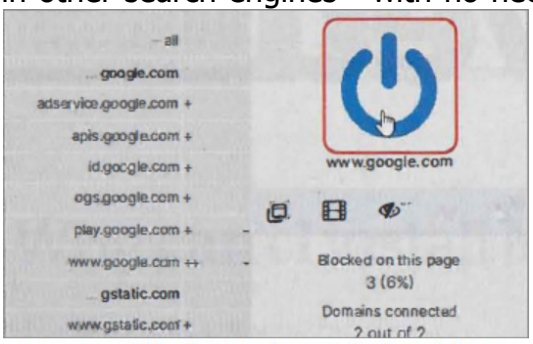
Particularly devious scammers 'cloak' domain names, so the web addresses in ads look like the authentic sites but redirect you to phishing pages when clicked.

How to Avoid Google Ad Scams

Install a reliable ad blocker

Ad blockers make the web less annoying . and intrusive by removing adverts and trackers from sites. But in the case of phishing ads in search results, they boost your security too, because you won't be tempted to click what you can't see.

The best ad blockers, such as uBlock Origin, automatically hide ads in Google search results - and in other search engines - with no need to configure any settings. Not only will this protect you from malicious links masquerading as ads, but it will also clean up your search results so the most relevant sites for your queries aren't given less prominence than those that have paid to be included.



Use an ad blocker such as uBlock Origin to hide all adverts in Google search results

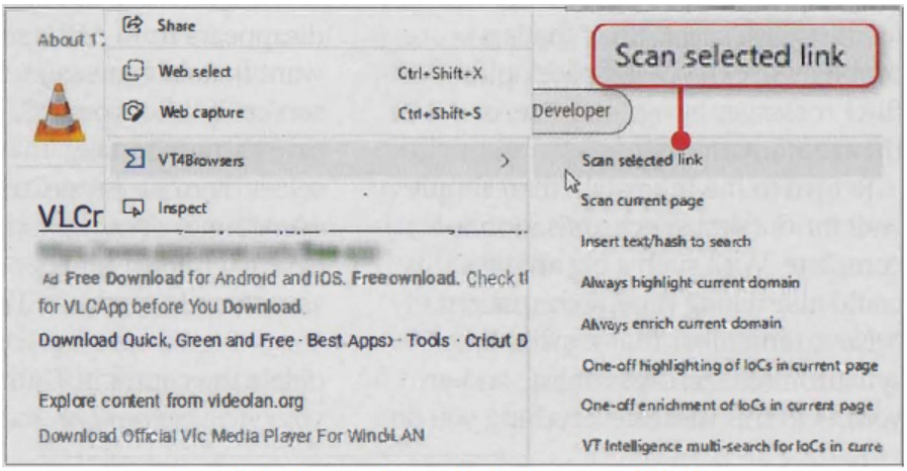
There is an ethical argument that ad blockers deprive websites -of the revenue they need to provide content for free, but it's easy to disable them on sites where ads are necessary and unobtrusive. With uBlock Origin, for example, simply click the extension's toolbar button, then click the large power icon (see screenshot above) to turn ad blocking off or on for the site you're currently visiting.

Even the FBI now recommends you use an ad-blocking extension when carrying out internet searches, to hide malicious ads that "appear at the very top of search results with minimum distinction between an advertisement and an actual search result" (see their announcement).

If your active ad blocker is showing adverts in search results, it may be set to allow 'acceptable' ads, even though some of these are now dangerous - such is the case with AdblockPlus. To stop this happening, open the extension's settings and untick the option to 'Show acceptable ads'.

Scan search results before you click them

As we mentioned earlier, scammers try to replicate legitimate URLs as closely as possible, and the links in fake ads may only differ by a letter or two, or an alternative domain extension, such as '.site' instead of '.com'. If you're unsure whether a web address is genuine, it's best to avoid clicking it altogether, but this is easier said than done when you're in a hurry to download a program and can't see an alternative link.



Scan links in search results before you click them using the VT 4Browsers extension

One solution is to install VirusTotal's VT4Browsers extension for Chrome and Firefox browsers. This lets you right-click links in search results and choose 'Scan selected link' in the VT4Browsers menu (see screenshot alongside) to check the destination site for threats using dozens of security engines. It's not completely failsafe, because it can't scan - for example – downloads hosted in online-storage services, but it could prevent you from blindly clicking into dangerous territory.

Switch to a different search engine

Google isn't the only search engine being targeted by malvertising - fake ads have also been spotted in Bing and DuckDuckGo results. Although an ad blocker is the best way to combat the problem, switching to an alternative search provider will also help.

What is Google doing about fake ads?

Google's 'Prevent malware in ad content' support page (www.snipca.com/44967) states that "any ad distributing malware is pulled to protect users from harm" and that Google uses malware-detection tools to identify rogue ads. In 2021, it blocked or removed more than 38 million ads for "misrepresentation".

However, the scale of current malvertising campaigns suggests Google needs to improve its detection software to keep up with the scammers' increasingly sophisticated tricks. Its Safe Browsing technology, which is part of 'Enhanced protection' in Chrome, is catching some, but far from all, of these threats, and users are spotting the ads long before Google. You can help by reporting phishing pages at www.snipca.com/44969.

Google is also planning to add a feature to Chrome that blocks all 'insecure' downloads. This will help combat fake ads that redirect you to files and pages hosted on unencrypted HTTP servers. The new 'Block insecure downloads' option recently appeared in Chrome Canary (the version of the browser aimed at developers) as an experimental 'flag'.

Neeva (which launched in the UK last October, is one of the few search engines to be completely free of ads, and promises not to store or sell details of your search queries. Its homepage claims that, in a blind test, nine out of 10 users preferred its results to Google's, but it will eventually limit some features to a paid-for subscription.

The privacy-focused Brave Search now includes ads in its search results (unless you use it in the Brave browser), but these are more clearly labelled and closely vetted than in Google and Bing, and less likely to be targeted by hackers.

Enable enhanced protection in your browser

Keeping your antivirus software up to date, and always installing the latest Windows security updates, is essential for safeguarding your system against malicious ads, but it's also worth enabling 'enhanced protection' in your browser. This warns you about dangerous websites before you click through to them, and blocks some - though not all - risky downloads.

Switch on Chrome's 'Enhanced protection' to block malicious down loads and sites

In Chrome, open Settings, click 'Privacy and security' and select 'Enhanced protection' in the Safe Browsing section (see screenshot alongside). In Edge, click 'Privacy, search and services' in Settings, switch on the 'Enhanced security on the web' option and choose Strict to block security threats and add 'security mitigations' for all sites. And in Firefox, go to Settings, then 'Privacy and Security' and select 'Block dangerous and deceptive content'.