The Search Engine Results Scam that Anyone Can Fall For

September 17, 2022 - It's being called "malverting." In plain English, malverting happens when you use a search engine and click on a result that actually diverts you to a malicious website. Hence the name. And it's a problem that is now creeping into paid advertising on all of the major search engines. And unfortunately, it's very difficult to spot these ads before you become a victim.

When you search the internet for information, most of the major search engines return links to their paid advertisers at the top of the first page. On Google, these returns look very similar to the non-paid links, but if you look a little more closely you'll see a little "ad" symbol in the results. These types of ads are where malverting is taking place and it's happening on Google, DuckDuckGo, Bing... pretty much any search site that has paid advertising is susceptible.

The ads that contain these malicious links look legitimate. So let's say that you do a search for the logon page of a brokerage or bank that you use. There is a good chance that a link will be shown in a paid ad, and that ad will look like it is linking directly to the page you want to go to. If it's legitimate, then you don't have a problem. But if the ad isn't legitimate, then you could find yourself landing on a page that downloads malware to your computer. Or you could find yourself on a page that looks exactly like the login page for your bank. If that happens and you enter your information, you've just given the criminals running that page everything they need to drain your accounts and steal your information.

As difficult as they are to spot, there are things that you can do to protect yourself against "malversion." Your browser should have a feature that displays the actual destination of any links when you hover over them. In Chrome, you can usually see the actual destination of links at the bottom of the browser window when you hover of the link. Other browsers offer similar capability.

Additionally, there are browser plugins that can help with this too. I use one called Link Revealer. It's free to download from the Google's webstore and should work in both Chrome and Microsoft's Edge browser. I haven't checked but there may also be a version of it available for Firefox. It has the benefit of showing the link very close to your mouse cursor and it highlights it. This makes links easier to work with and can help you spot anything suspicious with greater ease.

When looking at destination link addresses, there are some things you need to look for. If the link ends in anything other than .com, .net or .org, then you may want to do a little more research before clicking on it. There are other legitimate destinations, but it pays to be careful. If it ends in .ru (that's for Russia), .cn (thatâ€™s for China) or any other two-letter

grouping, it isn't taking you to a site in the United States. So unless you are planning on visiting an overseas website, avoid clicking on it.

You also need to check the spelling of the link addresses. For instance clicking on Google.com is just fine but clicking on Googl.com (missing the "e") isn't. Slight misspellings of web addresses is a common tactic of cybercriminals.

The bottom line here is that to be safe, you need to be vigilant. Just because you see a link in a paid advertisement doesn't mean that it is safe to click on. All of the major search engines are trying to combat this sort of thing, but it is up to users to make sure that they remain safe when browsing online.
by Jim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow ACCESS