SEARCH ENGINE RESULTS CAN BE DANGEROUS

BY JAY BORDEN

Almost everyone uses a search engine. Sometimes multiple times a day. When the results appear how often do we scroll past the first few results? Typically, people select something from that first page.

To take advantage of this, companies pay for ads that appear on the first search page. Companies pay for that placement because they know many people will scroll no further and just click their ad.

SEO, Search Engine Optimization, is a technique that uses the search engine's own algorithms to place links near the top of search results. Again, to be where people typically click.

Advertising is how search engine companies earn much of their income. SEO earns money for companies that do it successfully for others, and for the company that placed higher in the search results. Both of these techniques are legal.

But many of these ads and SEO-placed links are fake. The sites are corrupt and designed to download malware or to get you to share confidential information like passwords and credit card information.

A favorite topic for these types of activities is IT problems. When people are experiencing problems with their computers or printers, the internet is often the first place they go to find a solution. No wonder cyber criminals want to be on the first results page. They may get that placement by paying the advertising fee or through search engine optimization.

The term for this type of activity is malvertising, a combination of mal as in malware and advertising.

SEARCH ENGINE RESULTS CAN BE DANGEROUS

CONTINUED

The ads or SEO placed sites offer help in fixing computers or printers that aren't working properly. They often say new drivers are necessary to fix the problem. If you click the link to get the new drivers then malware will be downloaded to your device.

In some cases, the offer for help requires a payment by credit card. Once you enter your credit card, the cybercriminals have it and will use it themselves.

In more elaborate schemes clicking the link to download the drivers results in what appears to be an attempted download and installation of the drivers. But it is really only a video being played and shown to you. That video ends with a message saying a fatal error occurred. To prevent you from abandoning them they will display another message saying any further attempts to download or install anything or restarting your device may result in permanent damage and void the warranty. The recommendation is to call their technicians for help.

The technician typically asks to be granted remote access to your computer in order to fix the problem. Once this is granted they will install malware, steal your data including passwords, and other information, possibly even your bank or investment account credentials to steal your money.

Once a device is compromised it can be used to travel laterally, that is, spread to other devices on the network. It is dangerous regardless of whether it is a personal device connected to a home network or a company device connected to the company network. Either one can spread malware or ransomware.

In another type of campaign fake ads are being used to lure people to fake websites that appear to be popular sites. Researchers identified several of the impersonated sites to include Macy's, Kaiser Permanente, New York Life and others.

HE HIRING PROCESS,

SEARCH ENGINE RESULTS CAN BE DANGEROUS

CONTINUED

Once someone goes to those fake sites they receive fake HR pages with a goal of stealing the person's credentials to the HR and payroll systems. The bank account number for their direct deposit payroll is then changed to the attacker's account.

Clicking that fake link caused the loss of your bank account number and your pay. That loss will continue until it is noticed, reported, and someone figures out why it is occurring.

Search engine companies are doing what they can to eliminate malvertising. But cybercriminals continue to find new ways to avoid the search engine protections.

A newly discovered method uses artificial Intelligence, AI, to create innocent ad pages and websites that don't get flagged by the search engine. But that AI generated ad or site has links to malware infested sites.

No search engine is immune to these attacks. Of course, you should continue using search engines. Can we live without them?

But be very wary of ads, sponsored links, and what appears on the top of the search results. Look closely at any site you go to from the search results. Is the site address, the url, the one you really want? Is anything on the site suspicious or raise a red flag? Do not ignore red flags! Leave the site immediately!

Always ask yourself, does this person have a right to my personal information such as passwords or credit card information? Don't give it to anyone who shouldn't have it.

To learn all the ways we can help make your company and family safer, visit onebrightlycyber.com, contact OneBrightlyCyber at info@onebrightlycyber.com, or call (888) 773-1920.