west
protect

SAFE Tip Sheet

Search Engine Poisoning

Sept 2019

When good things go bad... The advent of the search engine (Google, Yahoo, Bing, etc.) is a good thing. But search engine "poisoning" has turned what used to be a quick and safe way to find exactly what you want, into something bad. Something dark. And something that can make you a victim and ruin your day.

What is Search Engine Poisoning?

It's a common scam: Criminals set up websites that supposedly contain news, videos, photos, or other information about a hot topic or current event (like the U.S. elections, the Olympics, or latest natural disaster). Then they rig these sites so they appear high up in your search results so you see them first.

What does this mean for you?

The search results you receive might not be safe. If you click on a compromised website, criminals could steal your information or infect your system with a virus.

What Can You Do?

- When you conduct Internet searches, **look carefully at the results**. Try to find well-known, popular websites. Stay away from sites with strange or unknown names.
- Instead of conducting a general Internet search, **go straight to a trusted site** to conduct your search. For example, if you're looking for a news item, go to the website of a major newspaper or TV station and search that site.
- Be aware that **when you add the word "free" to your Internet search, you might receive a higher rate of infected results**. For example, the term "free music downloads" is often tied to infected results.
- **The more popular the topic**, for example about a celebrity or a news event, **the more likely there will be poisoned search results**.
- If you click on a site and immediately see **pop-up windows asking you to download software, close your browser and re-open it**. Do not return to that site.

Good Habits to Remember:

- **Learn to recognize dangerous websites** that could be ripe for poisoning campaigns, like lots of popup ads, web ads, and especially **scareware** portals that trick you into thinking your computer is already infected and needs their "antivirus" software now!
- **Directly type the URL** of the websites into your browser, rather than clicking on search engine results.
- **Enable your browser's security features now!** If you visit a website and your browser warns you that it might be fishy, leave right away!
- Make sure your **antivirus, anti-malware, and firewall programs are all up-to-date**.
- Donations for disaster relief: **Never donate to an organization you don't know that sends you a link** in an email, on Facebook or Twitter, or from pop-up ads online requesting urgent donations as you search for more news on what is happening. Check out legitimate charities to give your donations to.