Cybercrime Prevention Flyer

CPF 00011-2021-CID361-9H 7 September 2021

Search Engine Optimization (SEO) Poisoning

What is SEO?

You may be wondering, how exactly do websites get to the top of search engine results? Search engine optimization (SEO) is a common online technique used by companies and individuals so that their website appears higher in the order of results on search engines such as Google, Yahoo, Bing, etc. Using SEO will likely get more web traffic to any given website.

How does SEO work?

Companies or individuals will research what the commonly searched terms are for the product, service, or just general information they may be advertising. They will then put those words more frequently into their website and advertisements, making their website appear more frequently in search engine results. This can sometimes be referred to as keyword stuffing. SEO in general is not malicious in nature.

What is SEO poisoning?

SEO poisoning is a form of SEO in which cybercriminals place malware on legitimate websites that rank high on search engine results. The way cybercriminals do this is by looking for high-ranking websites that have vulnerabilities within the website structure. Cybercriminals may look for URLs that begin with HTTP, meaning that the website is unsecure and the website structure is easily accessible. On infected websites, the malicious content may be disguised in the form of a download or in a link that will redirect you to a website with the malicious content.

Cybercriminals may also create fake websites and use SEO to generate traffic to the website. For example, cybercriminals may create a website around a holiday because they know many people will be searching for holiday ideas. The website, which may appear legitimate, ultimately may lead to a downloadable file containing malware or a site selling a fake item to get you to input your credit card information.

Anyone can be a victim of SEO poisoning, so it is important to be vigilant when surfing the web.

Report a crime to U.S. Army Criminal Investigation Command

Major Cybercrime Unit

27130 Telegraph Road
Quantico, Virginia 22134

Email

MCU Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

Cybercrime Prevention Flyer

What can users do to protect themselves?

- Keep your browser and antivirus software up to date.
- Avoid clicking suspicious-looking links, use common sense.
- Do not download anything from a website if you are unsure of the credibility.
- Use a VPN when possible, especially when using a U.S. government computer while teleworking or when travelling.
- Be smart about providing personal or credit information online. If you question the legitimacy of a site, do your research. If you question whether the communication with a site is secure, check the browser bar for the lock icon or https at the beginning of the URL.

Tip: Hovering over a link in a search engine will show the full URL in the bottom left of the screen.

Additional Resources

SEO poisoning (search poisoning)

What is SEO Poisoning (Search Engine Poisoning)

How to Identify and Protect Yourself from an Unsafe Website

Go Gold Cybersecurity

How to Spot Poisoned Links

To receive future MCU Cybercrime Prevention Flyers, send an email to: Subscribe CPF