SEARCH SMART!

RECOGNIZE AND AVOID SEO POISONING

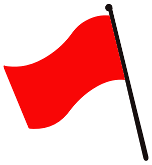
What is SEO Poisoning?

Search Engine Optimization (SEO) Poisoning is a tactic used by cybercriminals to make malicious websites appear at the top of search engine results. These sites are meant to look legitimate but can either harm your computer or steal the university's information.

How Does an Attack Happen?

When we search for something online, we frequently click on the top search result that seems trustworthy. Cybercriminals use our habitual nature to their advantage and pay search engines to push their website to the top of the search list, hoping you won't notice the red flags. If you click, the malicious site can install malware on your device or try to trick you into giving away sensitive information.

Watch Out for Red Flags!



- Free online tools like "file converters," "PDF conversion tools," "virus scanners," or "free software downloads."
- Unusual or misspelled website addresses ("amzon.com" instead of "amazon.com").
- Websites labeled 'sponsored' or 'ad'.
- Sites that require a download, or ask for personal or login information to gain access.

Safe Searching Tips

- **Use Trusted Sources -** Stick to verified websites and official sources, and use Rutgers-approved tools and applications to do your work.
- **Check URLs -** Always double-check the website address before clicking.
- **Update Security Software -** Keep your antivirus and security software up to date.
- **Stay Skeptical -** If something feels off, trust your instincts and avoid the site.
- **Report Incidents -** If you accidentally fall victim to SEO Poisoning, report the incident immediately to abuse@rutgers.edu.

Questions?

Contact the Information Security Office:
info_security@oit.rutgers.edu

RUTGERS IT