SEO - Avoid Negative Tactics

Negative SEO Tactics: What Is It?

Anytime one of their competitors attempts to negatively impact the ranks of a competitor's website or web page; they engage in Negative SEO. In addition to being unethical, this practice is often prohibited. Negative SEO in past decades can be described as simple as hacking a website and replacing its source code with dubious popup adverts. Negative SEO has significantly grown darker and more complicated in recent years.

Negative SEO Tactics: Types

Website Hacking

Though expensive, this strategy may be the most effective. As might be experienced here, a hacker can do whatever they want to a website's SEO performance by manipulating it. It may qualify as a Negative SEO attack if such a breach causes a decrease in search engine visibility.

Making Negative Backlinks to the Website with Spam Anchor Texts

These kinds of unfavourable links are frequently produced by automated tools, link farms, and PBNs (Public Blog Networks). Usually, one or two hundred to many thousands of connections and links are possible.

Gathering Content From Websites And Building A Duplicate Of Them

Producing copies of websites or specific pages of them, using hotlinking to disseminate the fakes over the internet, and other similar tactics are the foundation of this practice.

Falsely Reviewing A Website And Leaving Fake Negative Comments

This strategy may destroy the credibility of a website or a company, which may result in a decline in visitors.

Eliminating Backlinks From A Website By Contacting Publishers With Fraudulent Removal Requests

Company backlink profile might become the focus of hackers attempting to impact your SERP rankings negatively. To convince the website administrators to remove the links

referring to your site, they could contact them while posing as an individual or a company working on your behalf.

Spam Link Attacks

The following three techniques can help you find spam links referring to the website that developers did not create –

Identify spammy connections immediately

Monitoring new backlinks that lead to your website is the quickest approach to spot an active link spam attack.

Examine the graphs of referring sites and webpage

To rapidly detect peaks in your backlink profile, utilise the referral domains and webpages graphs provided by the Site Explorer Tools (Ahrefs' Site Explorer).

Examine the report on the anchor

When someone overflows your website with many links, those initial two techniques are the most useful for detecting high-volume cyberattacks. However, identifying an attempt to change your anchor text ratio is simple.

Examine the analysis on Referring IPs

A further indication of a negative SEO attack may be the presence of links on the identical subnet IP from numerous referring domains, as this frequently suggests that the websites are located in the same place.

There is a strong possibility that the same individual is the owner of several sites that are stored in the exact location. Furthermore, a PBN is presumably involved if the same individual manages both. Look at the Referring IPs analysis in Site Explorer to get an overview.

Ways To Respond To An Attempt Involving Link Spam

You need to actively disavow spammy links because it is improbable to have them eliminated.

Faux Link Removal Request

Negative SEO practitioners use this extremely cunning technique by sending emails to websites connected to your company.

Ways Fraudulent Link Requests Could Hurt Your Website

There needs to be no uncertainty as to whether a link spam strategy on your website will succeed. Despite being uncommon, such incidents can have significant consequences. Take the hypothetical loss of many of your most excellent backlinks in one day. Your ranks will plummet as quickly as a meteor as a result.

Ways To Recognise A Link Removal Attempt

Unfortunately, there's no method to prevent false removal requests from being sent out; you have no control over that. To safeguard your backlinks, however, you may monitor for indications of a running link removal attempt and initiate immediate measures if necessary.

Ways to deal with fraudulent requests to remove links

Two options are available after you become suspicious that a link removal attempt has begun to take place –

- In the unlikely event that your link was already taken down, contact any websites responsible for doing so, inform them that you did not request to remove it, and request their permission to return the link.
- Keep an increased focus on the backlink notifications if the website is still linking, and if it stops, take the necessary steps to recover any lost connections.

Content Exploitation

Copying of content occurs when a specialist replicates your work and publishes it in its entirety on a different website. Usually, it's not done maliciously. Most of the time, those who steal your website merely look for free content. They aren't intentionally aiming to damage your website, but they still might.

A Website's Vulnerability To Content-Brushing Incident

Whenever information appears on several websites, Google refuses to approve it. Usually, they select a specific version and overlook the others while ranking them.

Ways To Recognise A Brushing Attempt On Content

Copying a portion of text from the website and pasting it into Google with enclosed quotation marks will provide the fastest and most straightforward approach to determining whether your content was maliciously stolen.

Solution Against Content-Scrapping

- Submit a complaint under the Digital Millennium Copyright Act.
- Request a reference link for crediting.
- Make sure the internal link framework is correct.

DDoS Case

While DDoS assaults can additionally be regarded as hacking, they try to entirely shut down the website rather than disrupt it. DDoS, or distributed denial-of-service, is an unauthorised attempt to block legitimate traffic and queries from accessing your website by overloading the server or the infrastructure behind it until its hardware and software are depleted.

A DDoS Attack's Detection Method

Be sure to monitor incoming traffic and requests, either yourself or with your technical department. The more powerful DDoS attacks, however, can quickly bring your online operation to a complete stop. But a technical team aids in detecting the more subtle attacks with DDoS.

Ways To Counter DDoS Assault

In most scenarios, this will be a problem neither you nor the team can deal with effectively.

False Online Review

Pay attention to what comes up when the company name is searched for online. Research every month to get an idea; additional tracking might seem excessive in this case. Report any false reviews you encounter on reviewing services. Expect the platform owners to wait to remove them.

Hacker Accessing Your Website

Negative SEO tactics that cross the boundary into crime include hacking and cyber-attacks.

Identifying Website Breache

This is typically the most straightforward negative SEO tactic to spot out of all those on this page. A website that has been hacked commonly suffers greatly. If you need it, visit the "Security issues" option in Google Search Console.

Ways to Counter Website Hacking

The best defence is prevention. Your website's cybersecurity and server configuration affect its safety.

- Consider adding a security plugin.
- Make effective use of credentials.
- Update both your CMS and your plugins.
- Allowing security systems to receive regular automatic upgrades.

Conclusion

Negative SEO is quite difficult to succeed in the modern world, as was stated repeatedly throughout the article. Maintain an overview of the amount of traffic to your site and links from other websites, though, as it pays to be on the lookout for threats.