Why Tracking Your DNS History Is Important

Posted on October 11, 2019

If you have ever published a blog post and then got so much flack for it you ended up taking it down – and you still think this would make the problem go away, think again. If your readers have your blog on their RSS feed and click on its link, they'll still be very likely to be able to read a cached version of it.

The same is unfortunately true for domains. Every change a domain goes through is recorded on its historical WHOIS record, made possible by the introduction of passive Domain Name System (DNS) — a means to find out any modification made at some point in time to a specific domain.

As such, any bit of information related to a domain can still be seen via a passive DNS search. And this is the reason why making sure your domain has had no ties to any malicious activity throughout its entire life cycle is important.

A domain with a shady past can pose risks to any business as the following shows:

Past Search Engine Results Pages (SERP) Violations Can Haunt You

Although old domains are more likely to obtain better search engine optimization (SEO) rankings because they have operating for quite some time, that is only good if they did so for a good reason such as great content, popularity as evidenced by a huge number of visitors, and so on. It is not uncommon, however, for owners to abandon aged domains because these have been flagged for SERP violations such as sneaky redirects, using cloaked images, hacked sites, hidden text or keyword stuffing, spamming, and others.

Sites that have been cited for such instances are bound to maintain low SEO rankings no matter how good its current owner's SEO strategy is. So if you are, for instance, looking to obtain a new domain for your business, first, take a very close look at its past to make sure you do not end up suffering the consequences of its previous owner's wrongdoings.

You Don’t Want to Be Mistaken for a Cybercriminal or Cyber Attacker

In case you don’t know already, cybersecurity solutions work by blocking access to URLs that have been classified as “malicious” from their customers’ systems. So if your domain has been included in a security blacklist, potential readers or clients who wish to visit your website would always be alerted to its insecurity (based on historical data) through warnings, or they’ll never reach your site, which translates to lost opportunities for your company.

Even URLs that have been compromised and end up as unwary accomplices to cybercrime also get named in threat reports and news, not to mention be flagged for an SERP violation (i.e., hacked sites). This is another reason why you should use all available means to ensure your **DNS history** remains threat-free.

Using a Hijacked Domain Can Spell Disaster

The awkward truth: not all domains that are available for purchase have been lawfully obtained. Some may have been stolen from other individuals or organizations. And the only way these were made “available” is through hacking or compromise, which is unfortunately too easy to do with unsecured or insufficiently protected domains. Ending up with a hijacked domain, no matter how perfect it may be for your brand, may cause you to lose more than you gain.

Ties to Unscrupulous Content and Activities Not Only Result in SERP Violations but Also Blacklisting

The Internet, much like any other community, has its own “police” who are responsible for taking down sites that offer malicious content (e.g., porn, etc.), sell fake goods and services, or have ties to illicit activities online. There’s a reason why most of these sites end up on the Deep Web. Note

that domains that have been associated with violations and misdeeds end up in cybersecurity blacklists so if you need to decide on buying a domain or not, it's a good idea to carefully scrutinize its **DNS history** first.

No One Wants to Be Taken in by a Fake Domain Registrar

Just like buying a house or any property of great value, you don't want to be responsible for someone else's business and its brand, even over time.

That's why it's recommended that you do extensive background checks on people or companies you do business with.

The same care should be taken when purchasing domains because not all registrars are the real deal. If you've got your heart set on a domain and finally found a single registrar that offers it, find out all you can about the seller first. More often than not, the most coveted domain names are already taken. Hard-to-believe offers are just that because they almost always turn out to be fake and all you may have to show for your effort afterward is stolen personal information and your money let down the drain.

Staying safe from cyber threats shouldn't only focus on the present and the future – it's also critical to learn from the past. This is particularly true when it comes to choosing and purchasing a domain. Skeletons in a domain's **DNS history** closet can still have unwanted consequences.