How to Check & Improve the Reputation of Your Domain

It has never been easier to build a website and online business. You can create a site from scratch and start promoting and selling your product in a matter of hours. Amazing as this is, such convenience also has a dark side. Cyber-criminals can do that just as easily. They can infect your website with malware or mimic its appearance to lure your unsuspecting customers. Running a website became a technically challenging matter: web server software, content management systems and other digital tools all have their vulnerabilities. There are malicious requests impinging at every website in every minute looking for the possibility of taking control over it. One successful attack could destroy your business completely.

However, search engines and email providers are keeping up, constantly updating the algorithms that assess all the participants in the digital sphere. When we're talking about this assessment, we're talking about domain reputation.

When it comes to domain reputation, there is good news and bad news. Let's start with the bad: your website is also being assessed. And just because you are not a cybercriminal, it doesn't mean that your website cannot receive a bad reputation score: you may easily run into some trouble e.g. because of some innocent misconfiguration or a security hole accidentally left open. Now, the good news. It is possible to measure and improve the reputation of your domain.

All it takes is some knowledge, solid API tools like Domain Reputation and Website Categorization, and a little bit of patience. So, let's begin!

Why is domain reputation important?

Whether you're still a beginner in the digital sphere or an established player, the reputation of your domain follows you wherever you go. Just like in "real life," bad

reputation means that many doors will be closed or become much harder to open.

Take email marketing for example. If you're running an online business, you are probably well aware of the importance of building a large email list. If you are still having qualms about investing in email list building, consider this real quick.

Email campaigns can be easily automated, yet they can still maintain a high level of personalization based on customers' demographics, preferences, and behavior. They are inexpensive compared to pay-per-click ads and allow you to nurture a loyal customer base. Stats support this:

- 85 percent of US retailers acknowledge email marketing as one of the most effective customer acquisition tactics.
- 72% of consumers prefer to receive promotional messages through email.
- 28 percent of US online shoppers subscribe for brand newsletters to stay informed about their activities and best deals.
- Conversion rate can reach up to 47%.

However, that stellar conversion rate may be out of reach if your domain reputation is in shambles.

How so?

Well, we mentioned that search engines and email providers are keeping up with the latest developments in the cybersecurity world. It is in their best interest to protect both businesses and personal users from malware and phishing attacks.

So, when they rank your content or deliver your emails, they assess your domain reputation. If it's too low, your emails will end up in spam folders, never reaching your potential customers. Your content and products will remain buried away from the top ten results for relevant search queries. Essentially, your business will be locked out of countless opportunities to grow and flourish.

So how can you fix this? The first step is to learn how domain reputation works.

How is domain reputation calculated?

When search engines and email providers assess your website or emails, they look at two aspects of your online credibility – IP reputation and domain reputation.

The “IP” address stands for “Internet Protocol” address, the unique number linked to your domain and by extension, all of your online activity. When it comes to your email activity, providers assess:

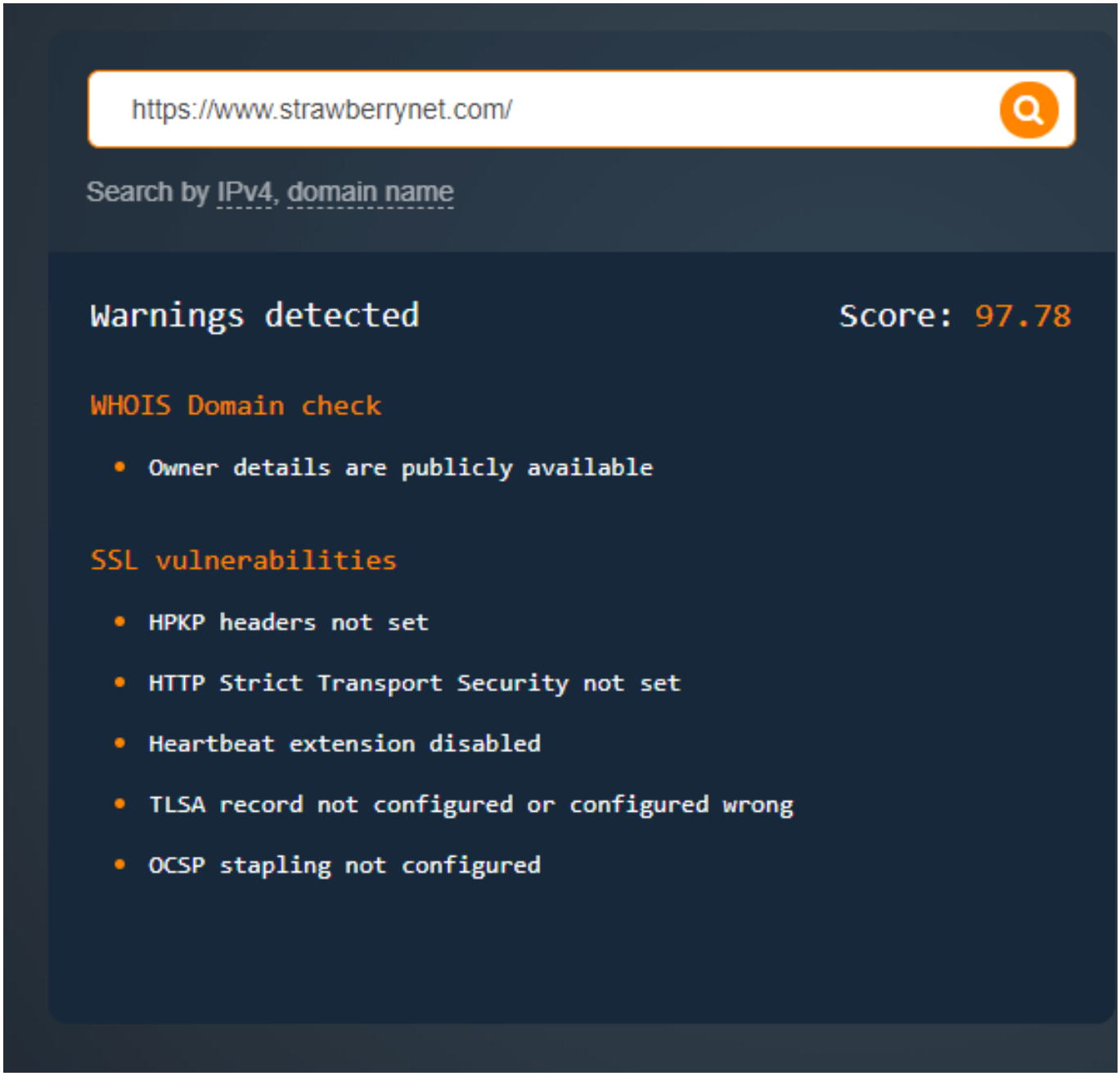
- The content you send should be high-quality, informative, without links to suspicious domains, malware, and “spammy practices”.
- The type of IP you use. A shared IP means you are using it together with several other domains, while a dedicated IP is connected to your domain exclusively. Obviously, a dedicated IP ranks higher, because it puts you in full control of your online activity and the reputation that stems from it.

When providers assess your domain reputation, not only do they do asses the IP reputation, but they also examine all of these behaviors coming from your domain alongside all the IP addresses you may use.

This irrevocably ties your online activities to your domain, brand, and business.

How to check my domain reputation

To check your domain reputation, go to Domain Reputation API, paste the URL to your website in the search bar and look at the results. You will receive a score, information about the availability of the owner details, as well as potential vulnerabilities that could be exploited by cybercriminals.



If you want a more detailed report, you can sign up for an API tool. The Domain Reputation API tool will enable you to perform a complete infrastructure check, including a malware scan. This will show you how well your domain is doing in terms of reputation. More importantly, this tool will also give you clear, straightforward feedback on the things you need to improve.

The thing that sets this cybersecurity tool apart from its competitors is Predictive Scoring. This method employs sophisticated algorithms that use real-time, dynamic datasets that allow you to check your reputation minutes after registration. This will allow you to curb any weaknesses in your domain before it builds a bad reputation.

So, how does this tool work? It examines:

- Your website content and its connection to other domains;
- Your website host configuration;
- Your website's track record in malware databases;
- The domain's SSL certificates, SSL connection, and configuration;
- DNS MX records configuration and corresponding mail servers;
- The domain's WHOIS record;
- Configuration of the name server;
- Infrastructure of the domain's IP addresses;
- Reverse IP lookup.

The results range between 0 and 100 – the higher the result, the lower the risk. If there are vulnerabilities you need to address, you can incorporate other API tools that will help you build solid domain reputation.

For example, you can use the Website Categorization API to:

- Investigate threats by singling out IP addresses that repeatedly visit your website and conduct suspicious, potentially dangerous attempts at phishing, fraud, and installing malware and spyware;
- Examine suspicious IP addresses' connected domains;
- Block unwanted content within your application or company network, making your own domain safer and more trustworthy;
- Monitoring references to your brand in unwanted categories;
- Monitor domains that include references to your brand or attempt to mimic it.

In time, as you fix underlying problems and create a safe environment within your domain, your domain reputation will grow. Keep in mind that this process takes

some time and patience.

Conclusion

Building a strong domain reputation also takes some investment – make sure it is spent on a reliable cybersecurity partner. With Domain Reputation API, you can start slowly and build trust over time – all you have to do is click here to get started with 100 free requests monthly. We won't even ask for your credit card details!

If you're interested in additional cybersecurity solutions such as Website Categorization API, keep in mind that Whois XML API solutions can be combined into a unique package that fits your business specifically. To learn more about it, click here and send us a message!