

How to check the origin of a website most accurately

How to check website origin through who.is, whoIsHostingThis, Wayback Machine



On the internet today, it is not difficult to find websites that specialize in scams. Therefore, checking the origin of the website is extremely necessary to avoid unfortunate incidents. So how to check the origin of the website is accurate? Let *TipsMake* help you find the answer in the article below!

Why is it necessary to check the origin of a website?

Checking the origin of a website will bring the following benefits:

Determine the reputation of the website

A reputable website usually has a long history of operation, receives many positive reviews from users, and provides accurate, reliable information. On the contrary, websites of unknown origin may contain false information or even be fraudulent.



Why is it necessary to check the origin of a website?

Checking the reputation of a website helps you avoid unnecessary risks. For example, when you want to buy something online, you need to know if the website is trustworthy to avoid being scammed or buying poor quality goods. In addition, for websites that provide information, knowing that the website is reputable will help you gain accurate and useful knowledge.

See who owns the website

This information helps you better understand the organization or individual behind the website, thereby assessing their transparency and purpose. Typically, trustworthy websites will publicly disclose information about the owner including address, phone number, and contact email.

On the other hand, websites of unknown origin often hide information about their owners. This can be a sign of a website that is not trustworthy, is likely to commit fraud, or is not compliant with regulations regarding user security and privacy.

Is the website blacklisted?

A blacklist is a list of websites that have been banned or warned against due to violations of safety and security regulations. A website can be blacklisted for a variety of reasons, such as distributing malware, fraud, or copyright infringement.

Checking if a website is blacklisted is an important step in ensuring your safety when browsing the internet. If a website is blacklisted, you should stay away from it and not provide any personal information to that website. Blacklist checking tools are often available online and are easy to use, allowing you to quickly determine how safe a website is.

Is the website under legal dispute?

If a website is involved in a lawsuit or legal dispute, it may be a sign that it is not following the law or is engaging in shady practices. Legal disputes may involve intellectual property rights, privacy violations, or fraudulent practices.

If a website is in legal proceedings, it may be suspended or asked to remove content. This may affect your experience when visiting that website. Therefore, checking the legal information of the website will help you avoid unnecessary risks and protect your rights.

The simplest way to check the origin of a website

To check the origin of a website, you can apply the following methods:

Using data from Who.is

Who.is is a tool that allows you to check information about the owner of a domain name. To use Who.is, do the following:

1. Step 1: Access the website whois.domaintools.com
2. Step 2: Type the website address you want to check
3. Step 3: Scroll down to the IP Location section. Here you will find information related to the IP address and IP location. Now you will know which country this website is from.

Checking the information through Who.is helps you determine whether this website is a trustworthy website or not. If the owner information is clear and the domain name registration date is old, it is likely a legitimate website.

Using WhoIsHostingThis

WhoIsHostingThis is also a tool to determine the hosting provider of a website. You just need to enter the domain name into the search box on the WhoIsHostingThis website, the results will return the following information:

1. Hosting provider.
2. The IP address of the website.
3. Location of the server.

Information about the hosting provider is important, as it can help you assess the quality and reliability of the website. Reputable hosting providers often have better security measures in place, which help protect the website from cyber attacks.

Using the Wayback Machine

The Wayback Machine is a tool developed by the Internet Archive that allows you to view older versions of a website. It is useful for checking the history of a website, thereby assessing its continuity and stability. To use the Wayback Machine, you just need to enter the domain name in the search box and select different time points to view the website.

Reviewing older versions of a website can help you determine if the site has been hacked, changed ownership, or had its content changed in an unusual way. This information can help you assess the current reliability of the site.

IntoDNS

IntoDNS is a tool to check the DNS configuration of a domain name. By entering the domain name into the IntoDNS website, you will get information about:

1. DNS server in use.
2. DNS configuration (NS, MX, A records).
3. Errors and warnings related to DNS configuration.

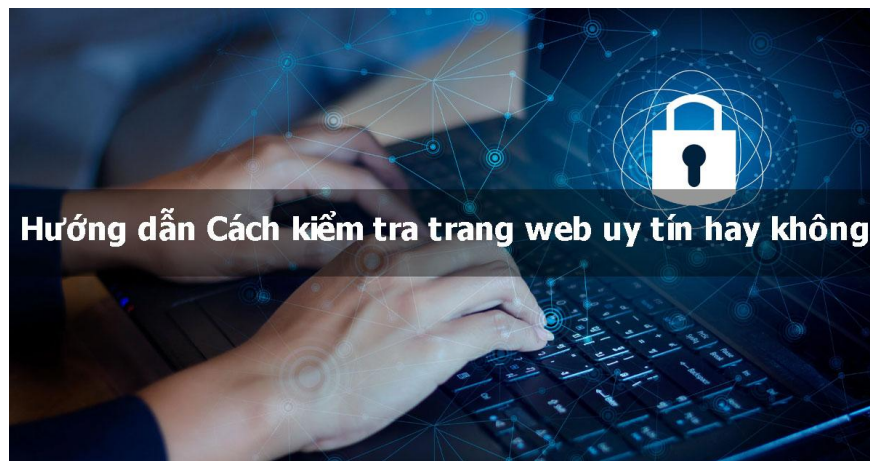
Checking your DNS configuration helps you detect technical issues that may affect your website's performance and security. A correct and error-free DNS configuration will help your website operate more stably and avoid security risks.

How does a 'clean' website affect SEO?

A clean website affects SEO a lot with the following factors:

Page load speed

'Clean' websites often have correct DNS configuration and are hosted on reputable servers, which improves page load speed. This is an important factor in SEO rankings, as users tend to abandon slow-loading websites, leading to high bounce rates.



How does a 'clean' website affect SEO?

Security

Clean websites are generally more secure, thanks to modern security measures and reputable hosting providers. Good security helps prevent cyber attacks, keeps your website up and running, and protects user information. Google gives higher rankings to secure websites with SSL certificates.

Stable and continuous content

Because of its history of stable and continuous operation, the website usually has quality content and does not change abnormally. Google will also appreciate websites with continuous, quality content that is relevant to user queries.

Reliability and credibility

Clear information about the owner and hosting provider helps increase the trust and credibility of the site. Google tends to rank higher for reputable sites that users trust.

Avoid being penalized by search engines

A clean site is less likely to violate Google's guidelines and will therefore be less likely to be penalized and lose rankings. Sites with a history of hacking, inappropriate content changes, or improper DNS configuration may be reviewed and penalized by Google.

It can be seen that checking the origin and legitimacy of a website is very important to ensure that you are interacting with a safe and trustworthy website. Along with the above ways to check websites, we hope to bring you useful information to evaluate websites effectively.

You finished reading the article "**How to check the origin of a website most accurately**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.