Avoid Website Blacklisting with Whois History Search, Domain Research Suite, and Other Tools

Posted on December 10, 2019

Now and then, users encounter warnings that deter them from accessing certain sites. These warnings include:

- The site contains malware
- Deceptive site ahead
- Your connection is not private
- Warning: Visiting this site may harm your computer

Most users would close their browsers or go back to the search results to find another website. If you're the site's owner, that means fewer visitors and lost business opportunities.

Studies show that 95% of users who run across blacklist warnings on sites do not proceed. This number represents a massive amount of lost organic traffic that impacts site owners' sales, especially if they mainly rely on their website to sell goods or offer digital services.

Unfortunately, most website owners only discover they are on a blacklist if customers report seeing warnings. More often, they may not even be alerted at all, as some blacklisted sites are no longer included in search results. Search engines automatically remove them from their indexes.

If you've been losing traffic and suspect that your website is on a blacklist, you can take immediate steps. This post also discusses best practices to prevent your website from ending up on a blacklist in the first place.

Why Sites End Up in a Blacklist

Websites may be blacklisted for a variety of reasons, which include:

- Improperly configured hosts or domains
- Unauthorized redirects to external pages
- Abnormal inbound or outbound traffic
- Keyword stuffing or thin website content
- Pop-up ads or malvertising
- Ties to spam or phishing campaigns

Threat actors can bypass website security protocols or existing control measures due to network flaws or human error. They do so specifically by compromising user accounts, brute-forcing entry into accounts with weak passwords, social engineering, and abusing host misconfigurations.

Any site that has been breached, of course, can be made to distribute malware as drive-by download hosts or used in phishing campaigns.

Blacklists Site Owners Should Not End Up On

Blacklists are maintained by security product vendors, search engine and browser operators, or independent organizations. They are classified according to domain infrastructure elements, such as IP address or nameserver. Often, blacklists are named after the organizations that maintain them. Here are the blacklists that site owners should avoid at all costs:

Google Safe Browsing

Google Safe Browsing is a blacklist that alerts Chrome users to unsafe websites. Popular browsers apart from Google's own such as Safari, Firefox, Vivaldi, and GNOME Web use

blacklists to protect their users from malicious sites.

Malware Blacklists

Malware blacklists comprise threat blocklists and databases that contain malicious URLs and compromised sites. Like other blacklists, malware lists are updated at varying intervals depending on their owners' (typically security service providers) discretion.

Domain Name System (DNS) Blacklists

DNS blacklists monitor nameservers and mail servers related to spam and phishing campaigns. These lists scan the Web for IP addresses to map out servers and connected domains so users can block all future communications coming from them.

Phishing Blacklists

Anti-phishing blacklists list down websites involved in phishing activities. They scan the Web for fake sites. Browsers and certain applications like email clients block access to sites on these lists.

Spam Blacklists

Spam blacklists trace the sources of spam. These lists are used by Internet service providers (ISPs) and data loss prevention (DLP) solution providers to filter malicious emails from their users' inboxes.

IP Address Blacklists

Most corporate servers verify user log-ins based on their devices' IP addresses. These are cross-referenced with IP blacklists to ensure that unauthorized users are not allowed access to private data.

How to Avoid Becoming Part of Any Blacklist

Prevention is always better than cure, as the website clean-up and blacklist removal process can take months, depending on the severity of the violation. We recommend that website owners and administrators observe the following best practices:

- **Ensure the domain you intend to purchase is not on any blacklist.** WHOIS history search tools allow users to examine a domain's history to discover if it was previously used for illegal cyber activities. That way, anyone interested in buying it won't have to suffer dire consequences should it be part of any blacklist.

- **Run a domain health check on your site periodically.** Track your domain reputation and risk profile as part of your mitigation plan. Using a domain reputation API can help users monitor their domains and sites for potential violations.

- **Enable IP geolocation monitoring on your site to avoid unwelcome visitors that could drop malware.** An IP geolocation API can help users retrieve detailed information on any IP address, such as connected domains, email addresses, ISPs, Autonomous System (AS) numbers, and other information that reveals important details about its owner. Any malicious individual's IP address can be prevented from accessing your Web properties with the tool's help.

- **Spot your domain's ties to malicious campaigns.** Identify potential phishing sites riding

on the popularity of your brand with Brand Monitor. Use its typos feature to automatically generate domains that may be mimicking yours. Report these to the relevant authorities so if they should be found malicious, they can be taken down thus preventing your clients from falling into eagerly waiting phishing traps.

- **Check your site for the malware and unnoticed violations that could land it on a blacklist.** Pieces of malware can find their way onto your site through security loopholes. Misconfigurations in your Secure Sockets Layer (SSL) certificates, meanwhile, can land your website on a blacklist. Make sure your Web properties are free from malware infection, configuration errors, and other issues with Threat Intelligence Platform. Regular health checks can lessen your site's chances of violation.

Whois XML API's various domain research and monitoring tools can be your trusted partners in ensuring that your domain remains threat-free. Only by keeping organizations' domain infrastructure secure can they prevent blacklisting and the consequent productivity and revenue loss.