Marketing and Web Analytics Benefits of Checking Reverse DNS MX Records

Posted on February 21, 2020

As email delivery is critical to most organizations that do business online, ensuring the integrity and reliability of their mail exchanger (MX) servers and their corresponding records is of utmost importance. But why is that so?

Well, MX records identify the mail servers responsible for receiving incoming emails and determining the recipients of outgoing ones. An incorrectly routed MX record, therefore, can cause problems with email delivery because of a mismatch in the sender's details, which could lead the email to be marked as spam or blocked. This can definitely affect a company's internal and external communications, particularly its marketing efforts.

For these reasons, marketing and IT departments need to work together to make sure that their mail servers are properly set up with the aid of tools like Reverse MX Lookup. The application identifies all the domains connected to a particular mail server, allowing users to check if all of their Domain Name System (DNS) MX records point to the right server and are configured adequately.

This post tackles the subject in more detail, looking at how to address email deliverability issues by reviewing what may be wrong with an organization's current DNS MX records.

Addressing Email Deliverability Issues via Checks of DNS MX Records

Both web analytics and marketing can benefit from a sound MX infrastructure. In addition to helping marketers improve their deliverability, it also helps web analysts to get more accurate and comprehensive insights into their visitors to improve user experience.

In fact, DNS MX records give users more in-depth information on website visitors. They can, for instance, let them recover the visitors' domains and consequently their industry or business to further enhance and personalize their marketing strategies and campaigns to deliver their desired message.

With a better understanding of how DNS MX records can help these professionals, let's now look at three issues that can impede their efforts.

1. Absence of a Reverse DNS MX Record

Several email servers reject incoming emails from IP addresses without reverse DNS MX records because the absence of the latter is a sign of spamming.

That's why it's essential to verify if an email server's reverse DNS MX or DNS pointer (PTR) record points to the company's domain and not to its Internet service provider (ISP). Usually, a PTR record points to the ISP that owns the IP address, not the organization that uses it.

In marketing, that may pose difficulties since the emails sent may look like they're coming from just any IP address owned by that ISP. In most cases, companies would need their ISPs' help to add their PTR record to their IP addresses. That way, each time they send an email, the recipient would immediately know that it came from them.

Marketers can use Reverse MX API to see if their domains have corresponding reverse DNS MX records. They just need to enter their mail server address into the API and check if their domain is in the resulting list. If that is not the case, they can create a DNS MX record for it to prevent email deliverability issues. Users who may not know their mail server addresses can use DNS Lookup API to obtain them.

2. DNS MX Records Are Misconfigured

After ensuring the presence of a reverse DNS MX record, the next step is to keep it appropriately configured and always up-to-date. If not, incoming and outgoing emails may not reach their intended destinations. That translates to lost potential customers and, consequently, revenue. Therefore, users can employ Reverse MX API to **check if their reverse DNS MX** or PTR records

point to their domains.

When keyed into the API, the resulting list should include their domain names. If it doesn't, they may have misconfigured their mail servers. They should fix issues until the results show their domains on the list. They can use Threat Intelligence Platform as well to check for DNS MX record misconfigurations.

3. Sharing Mail Servers with a Blacklisted Site

One of the reasons why users can't send emails is that their domains are blacklisted. But what most people may not know is that sharing a mail server with a blacklisted site means that they risk suffering deliverability issues as well.

Marketers and IT personnel can **check their reverse DNS MX** or PTR records to see if that is the case. All they need to do is key in their MX server address into Reverse MX API to list all the domains that share the same host. Using a publicly available blocklist, they can then check if a particular domain on the list is a blacklisted. Examples of these include Phishtank and Stop Forum Spam.

Reverse MX Lookup can help improve marketing and web analytics efforts. By doing regular **checks of reverse DNS MX records** to see if they are correctly configured and updated at all times, they lessen their chances of missing and failing to send relevant emails.

It also helps them make sure that their domains are not in any way associated with malicious activities, which may affect not just their email deliverability but also their reputation. Overall, clean and threat-free reverse DNS MX records are a must if they want to reach their target audiences continually.