Dmarc Records

Domain-based Message Authentication, Reporting, and Conformance (DMARC) is an email authentication protocol that is designed to give email domain owners the ability to protect their domain from unauthorized use, commonly known as email spoofing. The purpose and primary outcome of implementing DMARC is to protect a domain from being used in business email compromise attacks, phishing emails, email scams, and other cyber threat activities.

Develop a DMARC Policy

Before you add a DMARC record, decide on the policy you want to enforce. There are three types of DMARC policies:

- `none`: Treat the mail the same as it would be without any DMARC validation.
- `quarantine`: Treat the mail as suspicious. Depending on the recipient's email server, this typically means the email is placed in the spam/junk folder.
- `reject`: Completely reject the email; it will not be delivered to the intended recipient.

Create Your DMARC Record

A DMARC record is a TXT record in your DNS that looks something like this:

```
v=DMARC1; p=none; rua=mailto:dmarc-@example.com; ruf=mailto:dmarc-failures@example.com; fo=1;
```

This example tells email servers that:

- `v=DMARC1` indicates the DMARC version.
- `p=none` is the policy (none, quarantine, or reject).
- `rua=mailto:dmarc-reports@example.com` is where to send aggregate reports of DMARC failures.
- `ruf=mailto:dmarc-failures@example.com` is where to send forensic reports of individual failures.
- `fo=1` tells the receiving server to generate reports if both SPF and DKIM fail.

Access Your Domain's DNS Settings

- Log in to the domain management console or control panel provided by your domain registrar or hosting provider.

Navigate to DNS Management

- Find the section where you can add DNS records. This might be called "DNS Management," "Name Server Management," or "Advanced Settings."

Add the DMARC Record

- Select the option to add a new DNS record.
- The type of record you will be adding is a TXT record.
- In the "Name" or "Host" field, enter "_dmarc". This will make the full hostname of the record "_dmarc.yourdomain.com."
- In the "Value" or "Data" field, enter your DMARC policy (like the example given in Step 2).
- Set the TTL (Time To Live) as advised by your DNS provider. The default is often 1 hour (3600 seconds), but if you're uncertain, 24 hours (86400 seconds) is a safer choice.

Save the Record

- Save the new record. DNS changes can take anywhere from a few minutes to 48 hours to propagate worldwide.

Test Your DMARC Record

- Use a DMARC record checking tool to ensure your DMARC record is valid. Many of these tools can be found online for free : Mxtoolbox
- Enter your domain and run the test. The tool should show your new SPF record.

Setting up DMARC is a proactive measure against email spoofing and phishing—it's not an instant fix, but it's an important part of a comprehensive email security strategy. Keep tweaking and monitoring, and you'll be on the right track to keeping your domain's reputation clean and your emails landing where they should.

Revision #3
Created 9 November 2023 08:58:57 by Admin
Updated 9 November 2023 09:20:55 by Admin