BY DNS NINJAS

VIDEO AUDIT REPORT

NOVEMBER 2025
PREPARED FOR:
DIGGITY MARKETING

Summary

Your domain is correctly set up in some areas, but key records are either missing or misconfigured.

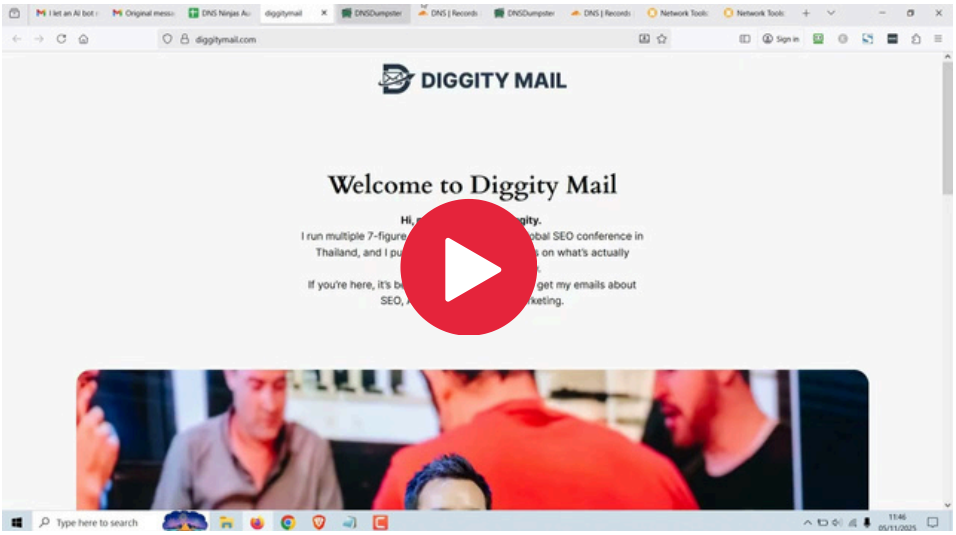
This may cause Gmail/Yahoo/Microsoft to treat emails as spam. Fixing these issues will improve inbox placement and reporting visibility.

Records that should be changed:

- **DMARC record** – There is currently no record for Diggitymail.com and the “p=none;” placeholder for Diggitymarketing.com. The first requires a record and both should be moved to “p=quarantine;” or “p=reject;” after analysing reports.

- **DMARC reporting** – You don’t have any DMARC reporting set up for your domain.

View your audit video



Audit Details/Corrections

Below is detailed information covering the recommended changes we suggest.

SPF

✅ – These seem okay, but see audit video for recommended changes. Add other sources per domain if sending from them (or use return-path).

DKIM

✅ – no changes required. DKIM records exist for email with Private Email, Rackspace, Active Campaign & SendGrid.

DMARC Record

⚠️ – Implement a correct DMARC record. No record on the mail.com domain and p=none; on the marketing domain. Should change to p=quarantine; and add forensic reporting (Aweber emails in Gmail spam).

DMARC Reporting

⚠️ – no DMARC reporting set up in DMARC record. Suggest adding to monitor, and switch both to quarantine after initial reporting.

SMTP

⚠️ – If diggitymail.com is used for form submissions using the Contact form 7 using SMTP on diggitymarketing.com, then you should configure DKIM and CNAME records from your provider. We'd recommend using the marketing domain though.

See a Google Sheet for copy/paste records here.

Audit Scope: we scanned your DNS records and have highlighted any suggested changes. We did not carry out any testing of your business, marketing or transactional emails.

Deliverability Risk Assessment

How your current DNS records can impact email deliverability.

Below are a set of items that should be implemented now, soon, and later.

The “now” fixes could be negatively affecting the deliverability of your domain-based emails right now and should be fixed at your earliest convenience.

1

HIGH RISK (FIX NOW)

Set up DMARC reporting this week. After two DMARC reports at 100% authenticating/alignment, switch to p=quarantine; and continue to monitor.

2

MEDIUM RISK (FIX SOON)

Setup a filter/report in AWeber for low percentage of opens/click-throughs by subscribers compared the your list average. Send them a “still want to hear from me?” email and then delist.

3

LOW RISK (FIX SOMETIME)

Decide whether to implement our recommendation of using the mail domain for marketing emails and the marketing domain for business and SMTP (transactional) emails. Test whether all emails pass DMARC.

Next Steps

Where do you go from here?

Below we have set out what the key main steps are after you've made changes to your DNS records from our suggestions.

01

Monitor DMARC Reports

Review the DMARC records you receive every week or month

02

List Hygiene

Set up a filter and remove/unsubscribe any email addresses from your list to help protect sender reputation.

03

Test All Types of Emails

Test your business, SMTP, and marketing emails using testing tools (see the next page for recommendations) to ensure they are authenticating/aligned.

Tools & Resources

Below are some resources and tools that you can use to help you make all of the changes to your DNS records to ensure the emails sent to recipients don't end up in spam folders.

DMARC Checker

Head to MX Toolbox to check your DMARC record (it will signal red if there are any errors or major issues).

DMARC Reports

We recommend using DMARC reports by Postmark here. You get a weekly summary that provides you with a quick check that everything is ok. (Easy & non-technical.)

Testing Emails

We use three different email testing services:

- mail-tester.com
- aboutmy.email
- dmarctester.com

Managing DNS

If you don't already use Cloudflare as your DNS provider then we recommend you do. Their service is robust and comes with added protections.

See the DNS Ninjas' learning portal for the Tools We Use and the Ultimate Guide to Authentication.

Next Steps

Want us to implement these fixes for you?

Click here to get it sorted within 72 hours.

Contact

DNS Ninjas
132-134 Great Ancoats Street, Manchester,
M4 6DE

www.dns-ninjas.com
hello@dns-ninjas.com