Boost Your Email Deliverability with Authentication Tools & Sending Practices

Problem: Emails from your business might be landing in spam folders or getting rejected altogether. This can hurt your marketing efforts and damage your brand reputation.

Google and Yahoo have also decided that they don't like all of the spam emails being sent, so they have decided to do something about it. Here is a longer article about the changes from a third party source. This isn't just me making stuff up to get you all worked up.

The changes are going to be required in February, 2024. That's next month. Yeah. If you don't implement these three authentication mechanisms and sending practices, your email will wind up in the spam box where you won't be able to sell anything.

Benefits of Email Authentication:

- Increased email deliverability: Land in inboxes, not spam folders.
- Improved brand reputation: Build trust with recipients.
- Enhanced email security: Protect against email spoofing and phishing.
- Valuable reporting: Gain insights into email performance and effectiveness.

Introducing the Pillars of Email Authentication:

- DKIM (DomainKeys Identified Mail): Prevents email spoofing by adding a digital signature to your emails.
- SPF (Sender Policy Framework): Verifies that authorized servers are sending emails on your behalf.
- DMARC (Domain-based Message Authentication, Reporting and Conformance): Tells inbox providers how to handle emails that fail authentication and provides valuable reporting insights.

DKIM Records:

- Establishing CNAME records in your DNS provider using a public key provided.
- This adds a unique signature to your emails, proving their legitimacy to receiving servers.

SPF Record:

- You'll add a TXT record in your DNS provider to allow authorization and authentication for email providers and senders like a CRM or other automated tool.

Tool For Checking DKIM and SPF Records On Your DNS Records For Your Website

I have used the super tool at MX Tool Box. It provides a great way to see if you have any of the DNS Records required for authenticating your email. I find it especially useful for the DKIM and SPF records that we just mentioned.

DMARC for Maximum Protection:

- Add a TXT record in your DNS provider with a DMARC policy.
- This policy tells inbox providers how to handle emails that fail authentication (e.g., quarantine, reject).

- DMARC also provides valuable reporting data on email traffic and authentication success rates.
- DMARC Checker - DMARC Report is a great tool to help you establish a free DMARC monitoring program. It can also help you set up this record.
- App Sumo Deal for DMARC Report is a steal. This will give you robust monitoring of all three mechanisms and what is going on with your email sending on a regular basis.

Metrics For Reputation

Google and Yahoo have traditionally relied upon specific metrics for reputation management of email sending. One of those drivers was read rates on emails. The bad news is that the changes that Apple implemented for privacy purposes has made read rates somewhat unreliable. So there are changes on that front as well.

- Spam Rate - You need to have your email marked as spam less than 0.3% of the time
- Unsubscribe Mechanism - If you send email without an unsubscribe link/button, you will be punished. It pisses people off and the email providers have noticed.
- Click Through Rates - They want to see users clicking on links in the email that you send.
- Reply Rates - If people are replying, it means that the content is useful and relevant.

Action Plan:

- Contact your website administrator. If that’s you, congratulations! You get to do this yourself.
- Verify the existence of the DNS Records for DKIM, SPF, and DMARC.
- Make sure that you have connected your email sending domain to your sending tools and implement robust email authentication protocols.
- The next step is to work on your sending practices to keep your metrics up.