Why Monitoring Mail Settings for Your Domain is Crucial

Ensuring that your domain's mail settings are properly configured and regularly monitored is essential for safeguarding your email communications. Without proper monitoring, your domain is vulnerable to a range of threats, including phishing, spoofing, and unauthorized use of your domain. Regularly checking your mail settings helps maintain your domain's reputation, ensures that legitimate emails reach their destination, and protects your users from potential threats.

I have covered topic of using domain records to ensure email deliverability for your business widely, but let's just start from recap and quick reminder of basic definitions that may be required later on.

How SPF Protects Your Domain

Sender Policy Framework (SPF) is a critical tool in your domain's email security arsenal. It works by specifying which mail servers are authorized to send emails on behalf of your domain. When an email is received, the recipient's mail server checks the SPF record of the sending domain. If the server is listed as an authorized sender, the email is accepted; if not, it is marked as suspicious or rejected. This simple but effective protocol helps prevent spammers from using your domain to send fraudulent emails.

Sample SPF syntax in TXT record: v=spf1 +a +mx -all

How DKIM Protects Your Email and Domain

DomainKeys Identified Mail (DKIM) adds an additional layer of security by allowing the sending server to digitally sign its emails. This signature is attached to the email's header and is verified by the recipient's mail server using a public key published in the domain's DNS records. If the signature matches, it confirms that the email has not been tampered with in transit and that it genuinely originates from the claimed domain. This also allows you to get better scores in antispam filters meaning it is more likely that your messages won't be forwarded to SPAM folder of receiver. This protects your email and domain from phishing and spoofing attacks, ensuring that your recipients can trust the integrity of the messages they

receive.

How DMARC Works with SPF and DKIM

Domain-based Message Authentication, Reporting, and Conformance (DMARC) builds on SPF and DKIM to provide comprehensive protection for your domain. It specifies how your domain handles emails that fail SPF or DKIM checks. DMARC policies can be set to monitor, quarantine, or reject such emails, helping to prevent unauthorized use of your domain. Additionally, DMARC provides feedback in the form of reports that detail how your domain's emails are being handled, allowing you to fine-tune your email security settings.

By filling DMARC record on your domain you tell receiver server how often would you like to receive XML reports with information about how many mails that server received passed SPF and DKIM, and how many failed checks.

Who is the Postmaster?

The postmaster is the individual or team responsible for managing and maintaining email servers for a domain. This role involves configuring and monitoring email settings, handling mail delivery issues, and ensuring that the domain's email practices comply with industry standards and regulations. The postmaster is also the contact person for receiving and resolving issues related to mail delivery and domain security.

Postmaster email specified in DMARC settings will receive all automated DMARC reports from other mail servers.

What Are Available DMARC Settings?

DMARC (Domain-based Message Authentication, Reporting, and Conformance) provides a range of settings that allow domain owners to define how their emails are authenticated and how they want to receive reports about their domain's email activity.

1. **`v` (Version)**: Specifies the DMARC version, typically `DMARC1`.
2. **`p` (Policy)**: Defines how emails that fail SPF/DKIM checks should be handled (`none`, `quarantine`, or `reject`). These settings give you control over how

your domain handles suspicious emails, allowing you to balance security with email deliverability.
3. **`sp` (Subdomain Policy)**: Sets a separate policy for subdomains, overriding the main domain policy.
4. **`rua` (Aggregate Report URI)**: Designates the email address or URI where aggregate reports should be sent.
5. **`ruf` (Forensic Report URI)**: Specifies the email address or URI for receiving detailed forensic (failure) reports.
6. **`pct` (Percentage)**: Indicates the percentage of emails the DMARC policy should apply to.
7. **`adkim` (DKIM Alignment Mode)**: Determines how strictly DKIM must align with the domain in the “From” header (`relaxed` or `strict`).
8. **`aspf` (SPF Alignment Mode)**: Controls how strictly SPF must align with the domain in the “From” header (`relaxed` or `strict`).
9. **`fo` (Forensic Options)**: Configures conditions for generating forensic reports based on SPF/DKIM failures.
10. **`rf` (Report Format)**: Specifies the format of forensic reports, typically `afrf`.
11. **`ri` (Report Interval)**: Sets the frequency, in seconds, for receiving aggregate reports.

Sample DMARC domain record: v=DMARC1; p=quarantine; sp=none; rua=mailto:dmarc-reports@yourdomain.com; ruf=mailto:dmarc-errors@yourdomain.com; pct=100; adkim=s; aspf=s; ri=86400;

Who Receives DMARC Reports?

DMARC reports are typically sent to the email addresses specified in the DMARC policy record. These reports can be received by domain administrators, postmasters, or other designated recipients who are responsible for monitoring and analyzing the domain’s email traffic and security.

How to Filter DMARC Reports – FREE automation!

DMARC reports are sent even if all SPF and DKIM checks were passed. This can cause an overwhelming amount of emails on postmaster mailbox. On the other hand, they are necessary to detect early phishing attempts or invalid domain settings, so you should not resign from receiving them.

DMARC reports can be overwhelming due to the sheer volume of data they contain. To streamline the process, you can filter and analyze only the necessary information. One way to do this is by using automation workflows, such as the free solution available here on n8n automation workflow. I have created this FREE N8N Automation workflow to streamline analysis of my DMARC reports, and now I am sharing this with you! This workflow automatically parses DMARC reports, saves them in a database, and notifies you of any DKIM or SPF errors. It allows you to focus on critical issues without manually sifting through extensive data.

Summary: Automation in Sailing Byte and Your Business

At Sailing Byte, we leverage various automations to streamline processes and enhance security for our clients. Whether it's through software development or business process automation, we are committed to helping you achieve your goals. Automating tasks such as DMARC report analysis not only saves time but also ensures that potential issues are addressed promptly. Our expertise extends beyond software—we understand the business needs behind these solutions and can tailor our services to meet your unique requirements.

By working with Sailing Byte, you gain a partner who can help you navigate the complexities of automation, ensuring that your business is both secure and efficient.