JUSTDMARC

Email safety policy

JUSTDMARC (Domain-based Message Authentication, Reporting and Conformance) is an email-validation system designed to detect and prevent email spoofing. It helps fight certain techniques often used in phishing and email spam, such as emails with forged sender addresses that appear to originate from legitimate organizations domain.

JUSTDMARC is developed as per DMARC policy that helps the organizations combat fraudulent emails, validate the email messages and secure the domain.

JUSTDMARC developed as per the DMARC policy & framework, allows a sender's domain to indicate that their emails are protected by SPF and/or DKIM, and suggests the receiver on the action if the messages fail both the authentication test method – such as junk or reject the message. JUSTDMARC removes guesswork from the receiver's handling of these failed messages, limiting or eliminating the user's exposure to potentially fraudulent & harmful messages. JUSTDMARC also provides two ways for the email receiver to report back to the sender's domain about messages that pass and/or fail DMARC evaluation. Aggregate reports contain statistical data, while forensic reports can include the fraudulent message.

SPF and DKIM Email authentication technologies were developed more than a decade ago. This provide assurance to receiver's identity of sender. These policies were already implemented but it couldn't address the problems of fraud and spam emails. Using spoofing technology, many phishing emails are still received by various email users.

JUSTDMARC is designed to fit into an organization's existing inbound email authentication process. This helps email receivers to determine the receiving message is from authenticated domain or not. It also provides a reporting mechanism of actions performed under those policies. It thus coordinates the results of DKIM and SPF and specifies under which circumstances the From: header field, which is often visible to end users, should be considered legitimate. Under JUSTDMARC a message can fail the authentication test even if it passes SPF or DKIM but fails alignment. JUSTDMARC verifies that the domain in the message's From: field (also called "5322.From") is "aligned" with other authenticated domain names. If either SPF or DKIM alignment checks pass, then the DMARC alignment test passes.

JUSTDMARC ADVANTAGES

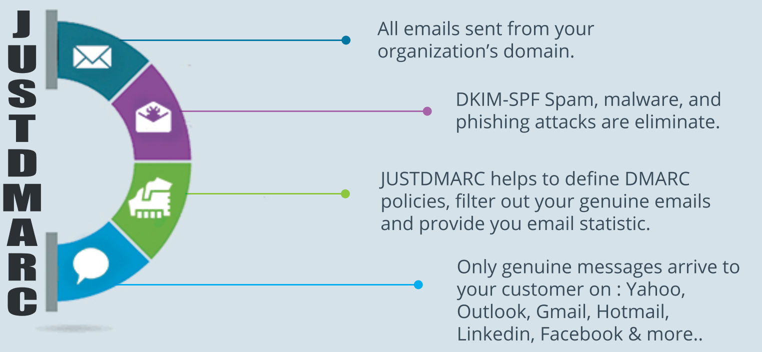
- It protects your company brand by preventing unauthenticated parties from sending mail from your domain.
- The systems inbuilt reports provide information about who is sending mail from your domain. This gives you more visibility about your email program.
- It has capability to view / observe the IP address with geo-graphical location from where the email is generated.
- The system helps to see sender IP Reputation.
- It provides the email statistics category-wise / department-wise etc.
- JUSTDMARC helps email community and email ecosystem as a whole become more secure and more trustworthy.

JUSTDMARC Policy Settings

✓ **None :** The entire email authentication ecosystem is monitored to map out legitimate traff.

🗑 **Quarantine :** Messages that fail JUSTDMARC move to the spam folder.

✗ **Reject :** Messages that fail JUSTDMARC do not get delivered at all.



All emails sent from your organization's domain.

DKIM-SPF Spam, malware, and phishing attacks are eliminate.

JUSTDMARC helps to define DMARC policies, filter out your genuine emails and provide you email statistic.

Only genuine messages arrive to your customer on : Yahoo, Outlook, Gmail, Hotmail, Linkedin, Facebook & more..

BHANU TECH PRODUCTS PVT. LTD.

225, Link Way Estate, Andheri Malad Link Road,
Malad (West), **Mumbai** - 400 064
Email : kaushikk@bhanu-tech.com, **Website :** www.bhanu-tech.com

CALL US NOW!

+91- 9869 159 034