A Buyers Guide

A buyers guide to DMARC - godmarc.com

WHAT IS DMARC ?

DMARC (Domain-based Message Authentication Reporting & Conformance) is the first & only email authentication technology that can make the From address that users see in their email clients trustworthy.

DMARC ensures that legitimate email is properly authenticating against established DKIM & SPF standards, & that fraudulent activity spoofing domains under your company's control is blocked

GoDMARC eliminates email phishing by blocking unauthorized emails before they reach company employees, partners, & consumers. Simultaneously, GoDMARC facilitates higher corporate email deliverability because mail providers will easily distinguish between phishing message & valid marketing campaigns.

Block Email Phishing in Real Time

Email authentication policies identify valid corporate email & block the remaining corporate & consumer phishing. Our customers control whether identifiers phishing & fraudulent email is sent to an end user's spam box, or not delivered at all.

Improve Email Deliverability

An email provider may well refuse to deliver an email to a user's inbox if it does not have an SPF and/or DKIM signature, or if the user has previously marked the sender's emails as "junk". With DMARC, emails are reliably authenticated, thereby improving deliverability of legitimate emails to a user's inbox.

Protect Brand Reputation

Organizations that are subject to regular email spoofing suffer considerable reputational damage. Phishing scams often attract negative press, with liability often attributed to the organization which has been impersonated.

Improve Marketing Campaign Open Rate

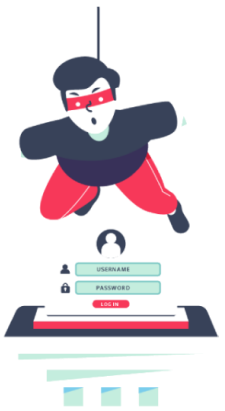
Use GoDMARC to identify and whitelist marketing, billing, and customer service email senders. Tune email security policies to increase third party deliverability.

Simulation Attack

Simulation attacks help you in safeguarding your business against phishing and other email security threats by training your employees to identify attacks.

As we have already mentioned earlier your employees are vulnerable to cyber-attacks and even the smartest of the members in your team can inadvertently trigger a major chain reaction that harms your business interest and brand equity.

From installing malware into your system to breaching your security system, cyber criminals can go to any length to hurt your business operations and dent your brand reputation.



Look A Like Domain

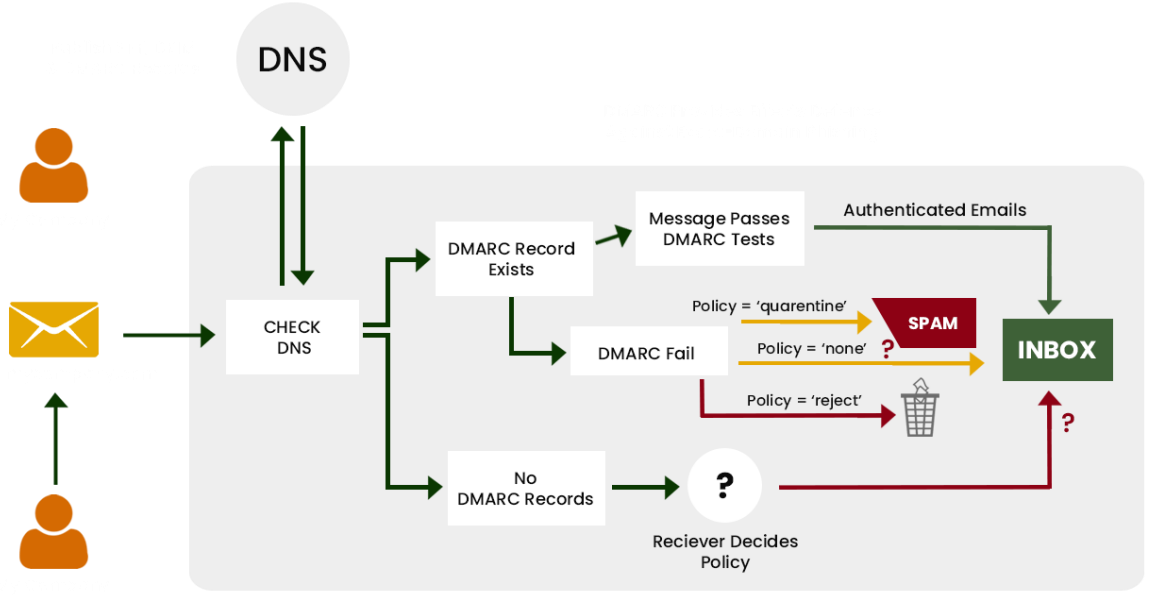
A look-alike domain is a nearly identical, slightly altered domain name, registered with intent to deceive.

Cybercriminals register hundreds of thousands of look-alike domains each year with the goal of impersonating legitimate brands and making money, usually by committing fraud.

HOW DMARC WORKS ?

We deploy DMARC for your emails in five easy steps -

1. We start by deploying DKIM and SPF. This is the first and most important step on the process
2. We define appropriate identifiers to make sure your mailers aligning align to them
3. Publish your unique DMARC record with “p=none” flag set for your email policies.
4. Monitor the data constantly and modify your mail streams whenever required.
5. Modify your DMARC policy flags from “p=none” to “p=quarantine” to “p=reject” when needed.



HOW TO IMPLEMENT DMARC ?

STEP 1: Visit godmarc.com

STEP 2: Enter you Email ID/Address

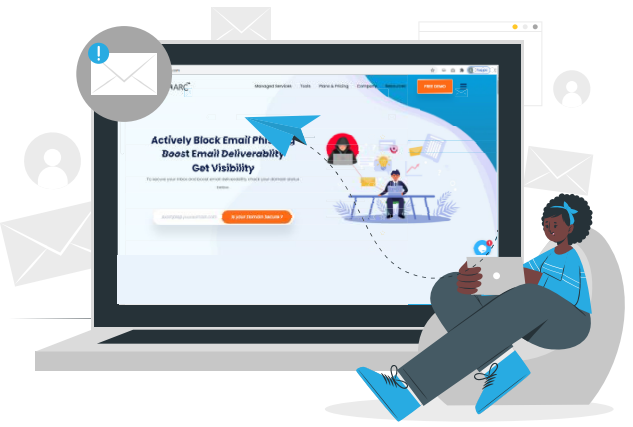
STEP 3: Your record should look something like this:

v=DMARC1; p=none;
rua=mailto:rua@godmarc.io;
ruf=mailto:ruf@godmarc.io; fo=0; adkim=r;
aspf=r; pct=100; rf=afrf;

STEP 4: Send record on your Email

Congratulations! You have created your DMARC record. The next step is implementation.

STEP 5: Implement your DMARC record into DNS Work with your DNS server administrator to add your DMARC record to DNS



FAQs

1. Why should we pay for an open standard protocol?

You can deploy DMARC at no cost by configuring your own reports, interpreting the results and then adjusting your SPF and DKIM configurations accordingly. However, DMARC XML reports are very lengthy and require staff resourcing to interpret the data and make adjustments. DMARC providers, such as GoDMARC, provide support in interpreting these reports and guidance on the appropriate DMARC configuration to get to the stage of being able to implement p=quarantine or p=reject policies more quickly.

2. We haven't deployed SPF and/or DKIM yet - don't we have to do that first?

You don't need to have deployed SPF and/or DKIM to get up and running with DMARC. In fact, the insight from your DMARC reports will help you to correctly deploy and configure SPF and DKIM.

3. I'm concerned that implementing DMARC is going to affect our current email deliverability.

DMARC will improve your email deliverability significantly providing that it is correctly configured. A DMARC expert, such as GoDMARC, will help you reach full protection mode far more quickly, minimizing day to day email operational issues and helping your organization achieve a far higher level of email deliverability.

4. We already have Firewall/DLP - doesn't that do this job?

Most of the email security solutions currently available do not give organizations total protection against email impersonation. This is because they focus on preventing security breaches which result in spam emails being sent from within an organization's network boundary. They do not prevent attacks which originate outside the organization's network and which will not cross the network boundary. The DMARC protocol is the only way to close this loophole by ring fencing an organization's domain and preventing spammers from impersonating it.