VALIMAIL

THE EMAIL MARKETER'S Guide TO DMARC

Email marketing campaigns aren't just about captivating content and eye-catching designs. Behind the scenes, standards and protocols influence whether your messages are received, opened, or banished to the spam folder.

At the forefront of this is DMARC: Domain-based Message Authentication, Reporting, and Conformance. DMARC is perhaps the most important standard for email authentication, and it's a key player in the integrity and effectiveness of all your email communication.

It acts as the security guard to all your recipients' inboxes, ensuring only legitimate, verified emails make it through.

> **DMARC is not going away, and the best thing a company can do is understand the potential exposure without it.**
>
> **Alexander Garcia-Tobar, Valimail CEO**

As an email marketer, you'll be excited to know that effective DMARC implementation can significantly boost your email deliverability rates (by as much as 10%). However, the benefits go far beyond that. DMARC also shields your business against email fraud, protecting your brand's reputation and building trust with your audience.

And in today's digital age, with email scams at an all-time high, safeguarding your email campaigns has never been more important.

To combat rising cyber criminals and phishing attacks, Google and Yahoo have taken a stand to make DMARC compliance a critical requirement for all bulk email senders. This changes Yahoo! and Google's previous advice, evolving DMARC from a best practice recommendation to a must-have requirement.

This new standard will start in February 2024, and if you don't adopt DMARC before then, your messages won't be delivered to Gmail or Yahoo inboxes.

It's time to get ahead of the curve.

Fortunately, understanding and implementing DMARC isn't rocket science. This guide is your comprehensive resource on DMARC, from its fundamental concepts to its strategic importance and practical implementation steps for your email marketing initiatives.

What is DMARC?

DMARC stands for Domain-based Message Authentication, Reporting, and Conformance. Now, that's quite a mouthful (we know), so let's break it down further. DMARC is a way of verifying that an email claiming to be from your domain (e.g., xyz@yourcompany.com) is actually from you.

It acts as a secret handshake or VIP pass to tell email providers like Gmail and Yahoo that your email is legitimate and not a fraudulent message trying to fool your customers.

DMARC works closely with three other email authentication protocols:

DKIM (DomainKeys Identified Mail)

SPF (Sender Policy Framework)

BIMI (Brand Indicators for Message Identification)

Resource: Curious how all of these authentication protocols work together? Check out DMARC, DKIM, & SPF Explained (Email Authentication 101).

These technologies work in tandem to create a robust framework for email authenticity, but they all revolve around DMARC implementation. None of these authentication protocols alone will ultimately protect your brand—you need to use them all in combination with DMARC to ensure 360-degree email protection.

DMARC is more than just a technical requirement. It's a cornerstone piece of any modern email marketing strategy. It helps your email reach their intended destination and protect your brand (and customers) in the process.

Resource: Need more help on your journey to DMARC? Avoid the common pitfalls and obstacles with the help of our Journey to DMARC Guide. Download your free copy here.

How Does DMARC Work?

DMARC isn't just a set-it-and-forget-it tool—it's a dynamic system that actively manages your email's journey from sender to receiver. Understanding the entire end-to-end DMARC process will help you make informed decisions about your email policies and how they impact your marketing campaigns.

01

The Authentication Checkpoint

When you send an email, the receiving email server performs a background check. It looks at the SPF and DKIM records associated with your domain. SPF verifies if the server sending the email is permitted to do so, while DKIM checks if the email content remains untampered from its original state.

These checks are the first line of defense in ensuring the email's authenticity.

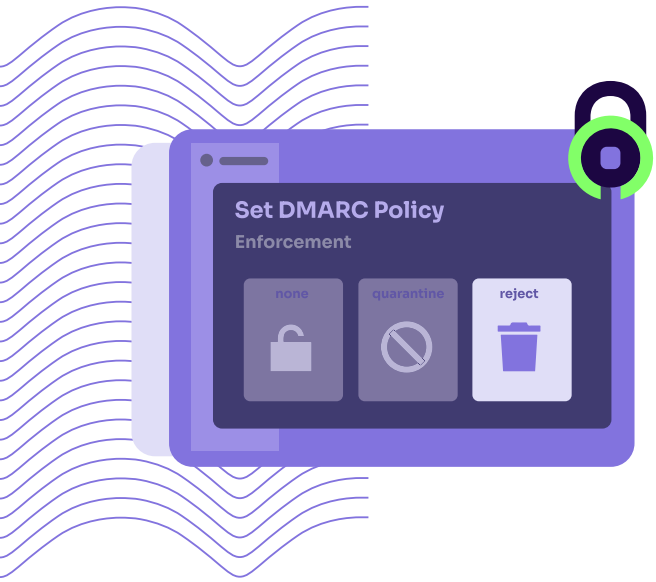
02

DMARC's Role as the Decision Maker

After SPF and DKIM have done their part, DMARC steps in as the decision maker. It checks its policy set for your domain to see how it should handle emails that pass or fail the SPF and DKIM checks.

Think of DMARC as the strategy behind your email's defense, dictating how strictly the rules should be enforced.

03 Policy Actions: Three Choices



DMARC offers three policy choices on how to treat emails that fail the authentication checks:

- **None:** This policy is essentially a monitoring mode. It tells receiving servers to report back on the emails but not take any action against them. It's a great starting point to understand how your emails perform without affecting their delivery, but it doesn't actually protect your brand.
- **Quarantine:** A step up in security, this policy advises servers to treat failing emails with suspicion. Typically, this means diverting them to the spam folder instead of the inbox.
- **Reject:** The strictest policy. Here, DMARC advises servers to outright reject emails that fail SPF and DKIM checks. This ensures that only authenticated emails reach the inbox, but it requires confidence in your email setup to avoid rejecting legitimate emails.

04 The Feedback Loop

One of the most valuable features of DMARC is its reporting capability. You receive reports on your emails' authentication status, giving insights into delivery success, potential security issues, and opportunities to improve email authentication practices.

These reports can be inherently hard to read and understand, and that's why tools like Valimail Monitor exist to interpret the raw data and help you identify and authorize all senders, find bad actors, and make the steps toward a reject or quarantine DMARC policy.

> **Valimail has proven itself to be future-proof because it has scaled to protect us from startup to global corporation. Their solution is easy to set up, and we've maintained our DMARC enforcement status since we onboarded.**
>
> **Kip Borie, IT Manager, Reputation**

Do You Really Need DMARC?

In today's digital marketing world, where every email counts, the question isn't just whether you need DMARC, but rather, can you afford not to have it? Email is a crucial touchpoint for communicating with your customers—from email marketing campaigns to transactional messages, it's the primary point of contact for staying in touch.

Before, most brands treated DMARC as a recommendation or a best practice. Fortunately, that's evolving now to become a must-have requirement. Here's why DMARC is becoming an essential tool for email marketers:

The Upcoming Google/Yahoo Changes:

The email landscape is undergoing a significant shift. Google and Yahoo, two of the biggest names in email, are gearing up to make DMARC compliance a requirement. This change is set to redefine the standards for email delivery and authentication. For a detailed understanding of these updates and where your sending status stands, check out this page: Google and Yahoo Compliance Check.

> **Your email should be trusted and safe. Everyone's email should be. This is Valimail's mission: restore trust to email. We believe that authentication is foundational, and doing it the right way is critical. Google and Yahoo are elevating best practices – having strong authentication – into requirements.**
>
> **Seth Blank, CTO of Valimail**

DMARC is about being proactive in a landscape where email authenticity is appreciated and increasingly required. Integrating DMARC into your email strategy is a forward-thinking move that aligns with the evolving requirements of major email service providers and the expectations of your audience.

Benefits of DMARC

DMARC might be becoming a requirement, but let's not overlook its many benefits to your brand. From enhancing the deliverability of your emails to fortifying your brand's digital presence, DMARC plays a pivotal role in shaping the effectiveness and security of your email campaigns.

Let's explore these benefits in greater detail, showcasing how DMARC isn't just about keeping your emails secure—it's about elevating your brand in the modern-day digital marketplace.

ENHANCED DELIVERABILITY:

Ensuring Your Emails Land Where They Should

Improved deliverability is perhaps the most direct benefit of implementing DMARC. DMARC is like a trusted courier, ensuring your messages are delivered straight to your audience's inbox.

By verifying that an email is genuinely from your domain, DMARC significantly reduces the likelihood of your emails being wrongfully flagged as spam. This authentication process ensures higher inbox placement rates, improving the visibility and engagement of your marketing campaigns.

ROBUST SECURITY:

Fortifying Your Email Defenses

DMARC protects against the rising tide of phishing attacks and email spoofing. These fraudulent activities can tarnish your brand's reputation and compromise your audience's trust.

Implementing DMARC establishes a line of defense that prevents malicious actors from misusing your domain to send harmful emails. This protects your recipients from potential security threats and upholds your reputation as a safe and secure communicator in the digital space.

BRAND PROTECTION:

Safeguarding Your Reputation

Your brand's reputation is invaluable, and email fraud can significantly damage it. DMARC acts like a brand bodyguard, ensuring that every email sent under your domain's name is authentic and genuine.

This protection maintains the integrity of your brand in your customers' eyes. It prevents fraudsters from eroding the trust you've built with your audience, assuring that your brand remains synonymous with reliability and credibility.

BUILDING CONSUMER TRUST:

Establishing Credibility with Your Audience

Trust is fundamental in a world where customers are increasingly aware of and concerned about digital security. When your emails are consistently authenticated, customers gain confidence that the communications they receive are genuinely from you.

This transparency and reliability go a long way in strengthening the relationship between your brand and your audience, fostering loyalty and trust that are essential in today's competitive market.

PREPARATION FOR BIMI:

Enhancing Brand Visibility and Recall

With DMARC in place, you set the stage for implementing Brand Indicators for Message Identification (BIMI), which allows you to display your brand's logo next to your email in customers' inboxes. This enhances brand visibility and also aids in brand recall.

DMARC is a BIMI requirement—without it, you can't display your brand's logo in the inbox.

Your BIMI logo is a powerful way to stand out in a crowded inbox, making your emails instantly recognizable. BIMI is a testament to your commitment to security and brand presence, adding a layer of professionalism and distinction to your email communications.

However, the impact of BIMI extends beyond your email campaigns. It's part of a broader strategy to ensure cohesive branding across all communication channels—be it email, social media, or your website. Consistent branding strengthens brand identity, fosters customer loyalty, and enhances the overall perception of your brand.

Additionally, if you have BIMI enabled, you'll be eligible for Google's new Blue Verified Checkmark, to further signal to audiences that they can trust your email.

BIMI boosts your brand's impact by offering prominent inbox visibility, reinforcing identity with consistent branding, and assuring email authenticity through DMARC compliance.

Resource: Haven't heard of BIMI before or not sure what it does? Download our comprehensive guide to become a BIMI expert.

How to Set Up DMARC

Implementing DMARC might seem daunting, but it's a relatively straightforward process when you break it down into manageable steps. As a marketer, you'll play an important role in pushing for and coordinating this setup.

Here's how you can spearhead the DMARC implementation in your organization.

01

Start the Conversation With IT

The first step is to establish a collaborative effort with your IT department. DMARC involves technical configurations that require IT expertise. Initiate a conversation with your IT team, explaining the marketing benefits and the necessity of DMARC for email deliverability and security.

For help communicating this need and securing resources from your IT team, use our pre-written email template!

Get your copy here>>

02 Identify and Record Email Sending Sources

Before diving into DMARC, you'll need to understand every source that sends emails on behalf of your domain. This step involves a comprehensive audit of your email-sending sources.

Collaborate with your IT team to list all the platforms and tools used for email communication. This includes marketing automation platforms, CRM systems, customer service tools, and even individual email servers within your organization. Accurate identification of these sources is essential for setting up effective SPF and DKIM records (which are foundational to DMARC).

03 Support Your IT Team

While IT team will be doing a large portion of the heavy lifting to implementing DMARC, it can still be helpful to be aware of. They will be managing tasks like these:

- Set up SPF and DKIM records
- Configure the DMARC record
- Monitor and analyze reports
- Adjust the DMARC policy as needed
- Continuously monitor and adjust

A DIY approach to these tasks can take years. However, solutions like Valimail Enforce can accelerate and automate this process to ensure you can keep sending email.

Common Challenges (and Solutions) to Implementing DMARC

Implementing DMARC is an essential step toward securing your email communications, but it has its roadblocks and obstacles. Here's a look at some common obstacles organizations face and practical solutions to overcome them:

CONFIGURATION MISTAKES

Problem:

One of the most common issues in DMARC implementation is the incorrect configuration of DNS records. This can lead to legitimate emails being marked as spam or not delivered at all.

Solution:

Double-check your DNS records for accuracy. Work closely with your IT team or seek assistance from DMARC service providers like Valimail.

LEGACY SYSTEMS

Problem:

Older email systems or legacy technology can complicate DMARC implementation, as they may not support modern authentication standards.

Solution:

Identify and upgrade legacy systems not compliant with SPF, DKIM, or DMARC standards. In cases where immediate upgrades aren't feasible, consider using email gateways that can add DMARC compatibility to your existing setup. Engage with vendors who specialize in integrating DMARC with legacy systems.

Use DMARC record check tools available online to validate your setup.

TRANSITION TO STRICTER POLICIES

Problem:

Moving from a DMARC policy of "none" to "quarantine" or "reject" can be challenging. There's a risk of legitimate emails being blocked if the setup isn't finely tuned.

Solution:

Gradually transition to stricter policies. Regularly analyze DMARC reports to understand your email flow and authentication success rates. Adjust SPF and DKIM records as needed to improve authentication rates before tightening your DMARC policy.

OVERLOOKING SUBDOMAINS

Problem:

Many organizations overlook the need to secure subdomains with DMARC. This is doubly important if you use a separate domain for your marketing communications—you'll need to ensure the marketing subdomain (and your email service provider) has the correct DMARC policy in place. Attackers can exploit unprotected subdomains for phishing attacks, damaging the organization's reputation.

Solution:

Ensure all active subdomains are included in your DMARC implementation plan. In cases where subdomains aren't used for sending emails, apply a DMARC policy of "reject" to these subdomains to prevent misuse.

MISINTERPRETATION OF DMARC RECORDS

Problem:

DMARC reports can be complex and difficult to interpret, leading to misinformed decisions or overlooked security issues.

Solution:

Use DMARC reporting tools that provide simplified and actionable insights. Consider partnering with DMARC solution providers who offer report analysis services.

MAINTAINING COMPLIANCE

Problem:

Once DMARC is set up, some organizations fail to maintain it, leading to issues as email-sending practices evolve.

Solution:

Treat DMARC as an ongoing process rather than a one-time setup. Regularly review and update your DMARC, SPF, and DKIM records to reflect changes in email-sending practices. Schedule periodic audits to ensure ongoing compliance and effectiveness.

Get Started with DMARC

DMARC is a strategic move towards more secure, reliable, and effective email marketing. It's the safeguard to protect your brand's reputation and ensure that only trusted emails reach your customers' inboxes.

Plus, it's becoming a Google and Yahoo requirement in February 2024, so it's no longer an option to ignore it.

> **Currently, there are said to be 140 million email-sending domains in the world, but only 5 million of them use DMARC. Furthermore, among them, only a few domains allow automatic authentication, and it is said that 60% set up DMARC on their own. We have a long way to go to reach 140 million.**
>
> **Alexander Garcia-Tobar, Valimail CEO**

Enabling DMARC helps differentiate your email program and gives you a competitive advantage.

QUICK RECAP:

- **DMARC is essential** for safeguarding your email communications against fraud and ensuring they land in your audience's inbox.
- **Collaboration with IT** and securing budget approval are critical first steps in the DMARC implementation process.
- **A step-by-step approach**, including setting up SPF and DKIM, configuring the DMARC record, monitoring reports, and adjusting policies, is required for successful implementation.
- **The benefits of DMARC** extend beyond security, enhancing email deliverability, brand protection, and readiness for BIMI.
- **Google and Yahoo sender requirements** mean all bulk senders must have a DMARC policy in place by February 2024 to send messages to Gmail and Yahoo inboxes.

NEXT STEPS:

01 Assess Your Email Strategy

Evaluate how DMARC can integrate into and enhance your email marketing efforts.

02 Initiate the Conversation

Talk with your IT team and leadership about the importance of DMARC and its role in the evolving digital landscape.

03 Start the Implementation Process

Follow the outlined steps to implement DMARC in your organization.

You'll need the right tools and expertise to get the most out of DMARC. This is where Valimail Monitor, our free service, can help. Monitor provides you with the insights and guidance needed to manage your DMARC policy effectively, ensuring optimal email deliverability and security. With our tool, you can even take the first step to get to DMARC enforcement and set up your p=none policy.

Sign up for Valimail Monitor for free today and take the first step towards a more secure, effective, and future-proof email marketing strategy.

Secure your brand, build trust with your audience, and stay ahead in the ever-evolving world of email marketing.