DMARC REPORT

Win the War on Email Spoofing With DMARC

A Guide for Brands That Want to Be Trusted

www.dmarcreport.com

TABLE OF CONTENTS

Phishing Emails Are Getting Harder to Detect

There was a time when you could spot a phishing email from afar. Emails riddled with spelling errors, an apparent low-key imitation of style and logo, or lucrative offers that were too good to be true. But now attackers have become smarter, and they execute a phishing attack like a brand campaign— well-curated, polished, and persuasive.

New-age technologies, such as AI, are further changing the game for these attackers. What used to take time and effort, like drafting convincing emails or mimicking a company's tone, can now be done in minutes with generative AI tools. That's one of the reasons why phishing emails today have become more refined than ever, and your customers can't tell what's legit anymore.

Lesson 1: DMARC Doesn't Work Alone – It's Built on SPF and DKIM

> "But to 2025 and beyond, as successful exfiltrations occur, the data feeding AI will almost certainly improve, enabling faster, more precise cyber operations."- NCSC

If you're serious about protecting your domain from spoofing, you can't rely on DMARC alone. It needs the support of SPF and DKIM to work effectively. Together, these three protocols check who's sending the email and whether the message was tampered with along the way.

Win the War on Email Spoofing With DMARC: A Guide for Brands That Want to Be Trusted

- **SPF** authorizes which IP addresses are allowed to send emails on your behalf.
- **DKIM** attaches a cryptographic signature to ensure the message content hasn't been altered.
- **DMARC** is like a watchdog that not just looks out for suspicious emails but also acts on those failing SPF and DKIM authentication based on the policy you have enforced.

With this layered approach, you can build stronger protection against impersonation attacks before they ever reach your customer's inbox. Because once these emails reach their inbox, the chances of them falling prey to them significantly increase.

Lesson 2: DMARC Reporting Tools Save Time, Sanity, and Sales

> "Research from agari.com indicates that adopting DMARC can reduce spam and phishing attacks by up to 75%."

Enforcement is only one aspect of DMARC. The real value comes from the reporting feature of DMARC that tells you what's going on with your sending domain and how receiving servers are handling emails that claim to be from you.

Why You Can't Read Aggregate XML Reports Manually

The problem is that aggregate reports are delivered in XML format, which can be very difficult to decipher without specialized tools. Manually going through them takes too much time, and you'll likely miss critical warning signs, especially if you're going through a large volume of emails.

Forensic Reports Can Be Useful When Handled Right

As for the forensic reports, they provide more detailed insights into specific authentication failures, such as who attempted to spoof your domain and what exactly went wrong. But they often contain sensitive information and need to be handled with care to avoid privacy or compliance issues.

This is where DMARC reporting tools come in. They turn all that raw, complex data into clear, easy-to-read dashboards and alerts so that you don't waste time and resources decoding them. Instead, you can focus on what matters most—growing your business while protecting your brand.

With this layered approach, you can build stronger protection against impersonation attacks before they ever reach your customer's inbox. Because once these emails reach their inbox, the chances of them falling prey to them significantly increase.

Lesson 3: Quarantine or Reject– Which One Is Right for You?

> "The DMARC reporting system is crucial for the operation of email systems: if email receivers do not provide suitable feedback, domain owners cannot properly identify and fix problems in their configurations."
>
> -Hureau, Duda & Korczyński, Stress Testing the DMARC Reporting System: Compliance with Standards and Ways of Improvement

The basic paradigm of DMARC is to decide what happens to the emails that fail authentication. To make this happen, it relies on three policies: none, quarantine, and reject. Out of the three, quarantine and reject are the ones that actively stop suspicious emails from entering your inbox.

Understand What Each Policy Does

Quarantine tells receiving servers to treat failed emails as suspicious, usually moving them to the spam folder. Reject, on the other hand, instructs servers to outright block the email from being delivered. Both policies serve to protect your domain, but they work at different levels of strictness.

Balance Between Deliverability and Protection

You cannot choose and enforce these policies arbitrarily. Striking the right balance between deliverability and protection is key.

Before you implement "p=reject", which is the strictest policy, all your legitimate email sources are properly authenticated with SPF, DKIM, and domain alignment. Otherwise, you risk blocking genuine emails that fail DMARC checks due to misconfigurations.

This is why it is recommended that you start DMARC enforcement with p=quarantine. Starting with this policy lets you safeguard your domain while monitoring for any gaps in authentication.

Once you're confident that everything is aligned and functioning, you can safely advance to p=reject for maximum protection against spoofing and impersonation.

Lesson 4: Domain Alignment Is Critical for DMARC Success

When you implement DMARC, it doesn't just look at whether an email passes SPF or DKIM; it also checks if the domain in those checks aligns with the visible "From" address your users see. That's the most important part, because without alignment, even a legitimate email that passes SPF or DKIM might still fail DMARC.

This applies to even SPF and DKIM. With these authentication protocols, it's not enough for the checks to simply pass; they need to be tied back to the same domain that appears in the "From" address. That's because DMARC doesn't just care if authentication passes; what matters is if the authenticated domain matches the one your recipients see. Without that alignment, your emails can still fail DMARC even if SPF or DKIM are technically valid.

SPF vs DKIM Alignment – Know the Difference

But the alignment works a bit differently for each protocol. SPF alignment compares the domain in the Return-Path (the technical sender) to the domain in the "From" address. If they match, SPF is considered aligned. DKIM alignment, on the other hand, checks if the domain that signed the email (the d= tag in the DKIM signature) matches the "From" domain.

Strict vs Relaxed – Choose Based on Your Email Setup

When you implement DMARC, you get to decide how strict this alignment needs to be. You can choose between 2 alignment modes— strict and relaxed. In strict alignment, the domain in SPF or DKIM must match the "From" domain exactly. In relaxed alignment, the domain just needs to share the same organizational domain. For instance, "news.brand.com" aligns with "brand.com".

Relaxed alignment is useful when you have multiple subdomains sending emails on your behalf. However, strict alignment gives you a tighter grip on your domain, ensuring that only emails from your exact domain pass alignment. This reduces the risk of subdomain abuse but requires consistent domain usage across all your email sources.

Lesson 5: Not Every Failure Is Your Fault

When you review DMARC reports, you'll see some authentication failures. But not every failure means you've misconfigured something or that your domain is under attack. In fact, there are several technical reasons why legitimate emails might fail DMARC checks, even when your SPF, DKIM, and alignment are set up correctly. Understanding these reasons can save you from chasing false alarms and help you interpret reports with better judgment.

DNS Timeouts and Network Issues Happen

Sometimes, authentication failures happen because of factors beyond your control. One of them is DNS timeouts. When a receiving server tries to validate SPF, DKIM, or DMARC, it queries your domain's DNS records. If the DNS server is slow, unreachable, or is experiencing some lag due to network congestion, the lookup can fail. In this situation, even if your records are correct, the receiving server may not get a response in time, causing the authentication check to fail. These timeouts don't mean your setup is wrong; it just means the network wasn't responsive at that moment.

The silver lining is that these issues are temporary and resolve on their own, but that does not mean you should ignore them completely.

Mail Servers Can Misbehave Too

Another common reason for your email to fail authentication is that mail servers don't handle emails the way you expect. This happens when an email is auto-forwarded or passes through intermediary servers that modify the message, such as adding footers, disclaimers, or altering headers. Although these are not significant changes, they can still break the DKIM signature, as it analyzes the content of the email for **integrity and expects** it to remain exactly as it was when signed.

When DKIM fails, the only fallback is SPF. But if SPF isn't properly aligned or, even worse, if the forwarding server replaces the Return-Path, then SPF fails too, ultimately causing DMARC to fail. This can happen even if the original email was fully authenticated when it was first sent.

This doesn't mean your DMARC setup is wrong. It's just the nature of how some mail servers handle emails along the way.

Lesson 6: But Most Errors Can Be Fixed on Your Side

Now, coming to factors that are actually in your control. Most DMARC errors happen because of misconfigurations in SPF, DKIM, or **domain alignment**. Let's say you added a new marketing platform that sends emails on your behalf, but forgot to include its sending IPs in your SPF record. Any email they send will fail SPF.

Common Misconfigurations in DNS

An incomplete SPF record is one such mistake that most organizations make, which causes DMARC to fail. If you don't include all your authorized senders, like marketing platforms, CRMs, or third-party tools, in your SPF record, any emails they send will fail SPF checks.

Another issue is exceeding the SPF 10 DNS lookup limit. If your record includes too many mechanisms that require lookups, SPF can return a permerror, causing the authentication to fail even when the listed servers are correct.

For DKIM, the reason for failure is different. It happens when DKIM signing isn't enabled across all your sending sources, or when you have not updated the public DKIM key, or it is incorrectly published in DNS.

Wrong Policy Settings

DMARC also fails if your policy is not enforced properly. Proper policy enforcement does not mean that you jump to "p=reject", just because you need maximum protection, it means choosing a policy that matches your domain's readiness.

If your SPF, DKIM, and alignment aren't fully configured across all email sources, enforcing p=reject too soon can block legitimate emails. That's why DMARC enforcement is a gradual process. You start with p=none to monitor and collect data, then move to p=quarantine as you resolve issues, and finally to p=reject once you're confident everything is properly set up.

Ignoring DMARC Reports

Checking your DMARC reports is as important as enforcing DMARC, and one of the biggest mistakes you can make is not paying attention to them. DMARC reports give you a clear view of who is sending emails on your behalf, which ones are passing or failing authentication, and whether there are any attempts to spoof your domain.

If you ignore these reports, you risk missing critical insights, like misconfigurations, unauthorized senders, or alignment issues, that can impact your email deliverability and security.

Lesson 7: Email Security Doesn't Have to Be Expensive

> According to research, less than half (47%) of 150 banks incorporated in the UK implement the strictest and recommended level of DMARC.

Most organizations feel that email security is a tedious and expensive endeavor, which is perhaps why they are apprehensive about it. But in reality, email security is not at all expensive, especially when compared to the cost of a successful phishing attack or brand impersonation.

In fact, implementing SPF, DKIM, and DMARC costs nothing at the DNS level; all it takes is time and effort to configure them correctly and monitor the reports they generate. You can also use DMARC reporting tools that automate this process and make it easier to catch issues early. For most businesses, especially small and medium-sized ones, this is a cost-effective way to strengthen email security and protect brand reputation.

Free Tools That Work Well

The good part is that DMARCReport now offers free tools, which make DMARC implementation and monitoring easy and efficient.

- The **DMARC Lookup Too**l lets you check and analyze DMARC records for any domain to ensure proper configuration.
- The **SPF Lookup Tool** allows you to verify and analyze SPF records to confirm all authorized senders are included.
- The **MTA-STS Lookup Tool** checks your domain's MTA-STS records to ensure secure email transmission.
- The **BIMI Lookup Tool** lets you verify BIMI records so your brand logo displays correctly in supported email clients.
- The **TLS-RPT Lookup Tool** helps you check TLS-RPT records, which provide reports on email transport layer security.

Affordable Hosted DMARC Solutions for SMBs

For SMBs (small and medium-sized businesses), managing DMARC, SPF, and DKIM manually can be a bit tricky, especially because they don't have a dedicated security team. That's why they need hosted DMARC solutions, which will make the entire process simpler and more manageable.

So, instead of handling everything on your own, you can rely on a hosted solution that automates the heavy lifting. These services help you monitor DMARC reports, identify problems, and fix authentication issues without needing deep technical skills. And the best part is, they don't cost a fortune. Most hosted DMARC solutions are built to be budget-friendly for SMBs, offering essential features like report dashboards, alerts, and guided fixes at a reasonable price. It's a simple, affordable way to stay secure and build trust with every email you send.

Free Tools

- DMARC Lookup Tool
- SPF Lookup Tool
- MTA-STS Lookup Tool
- BIMI Lookup Tool
- TLS-RPT Lookup Tool

DMARC REPORT

Contact Us

www.dmarcreport.com

support@dmarcreport.com

(+1)-855-700-1386

Reach us on Social Media