Why Email Authentication Matters

How to Control and Protect Your Brand and Reputation with DMARC

SPARKPOST

dmarcian

Table of Contents

The Case for Email Authentication

Email is an excellent and arguably irreplaceable communication channel for businesses. But maintaining visibility and best practices for multiple external email resources like your email service provider (ESP), customer relationship management (CRM) application and help desk platform is no easy feat. Even with improved efficiencies in the email channel, a typical small to medium-sized organization will use between four and nine services to send email on their behalf. It isn't uncommon for large enterprises to use between seven and 20 services to send email, and often some IT teams aren't even aware of some of these services being used.

Having many different tools and services exposes organizations to security risks, making it incredibly easy for bad actors to blend in and launch malicious campaigns. This leads to successful phishing attempts, eroded brand reputation and diminished email performance.

For marketers or mail operations teams responsible for deliverability, brand reputation and inbox rates, these unauthorized mailings can upend successes gained by adhering to best practices, observance of which is another major resource investment. Legitimate campaigns launched outside of your CRM or ESP of record run the risk of re-mailing to previously unsubscribed, hard bounced or spam complainant addresses, further eroding your collective domain reputation.

The Challenge of Shadow IT

By using unauthorized services to send mail on your organization's behalf, good actors or well-intentioned internal parties can also be at fault for diminished email performance. Think of the rogue group who circumvented the vendor approval process running a campaign, or the sales rep who signed up for a service that sends mail to customers from his work email address. Initially, this general lack of governance was believed to be a pain point at only very large organizations where overlapping efforts of distributed teams are more commonplace. We now know that it's a common problem plaguing businesses of all sizes. Today, the term "Shadow IT" has been welcomed into the normal, everyday vernacular among IT and security professionals and is recognized as a contributing factor to poor economies of scale, unnecessary risks and vendor noncompliance.

Shadow IT is defined as the use of IT-related hardware or software products within an organization without the knowledge of the internal IT or security group. It has grown exponentially in recent years, driven by the quality of consumer applications in the cloud such as file sharing apps, social media and collaboration tools. Shadow IT also exposes your organization to additional vectors for data leaks and other security problems.[1]

Research by Microsoft shows that on average, enterprise IT departments are unaware of more than 60% of applications used.[2]

What You Think Your Email Program Looks Like

Corporate Mail (B2B Communications) • Marketing Cloud (Promotions) • Transactional Mail (PW Reset, Purchase Receipts)

What Your Email Program Actually Looks Like

Corporate Mail (B2B Communications) • Marketing Cloud (Promotions) • Transactional Mail (PW Reset, Purchase Receipts) • **Helpdesk** • **Billing Platform** • **CRM** • **Survey/CSAT** • **Adhoc Marketing** • **Event Registration** • **Disaster Recovery and Legacy Infrastructure** • **HR Platform** • **Product Management** • **Recruitment Software** • **More?**

1. https://dmarcian.com/understanding-shadow-it/
2. https://www.microsoft.com/security/blog/2020/08/24/microsoft-corrata-integrate-extend-cloud-security-mobile-endpoints/

Techniques to Combat Shadow IT

There are a few steps that organizations can take to combat this growing problem and maintain control:

1. **Establish a DMARC Initiative:** DMARC (Domain-based Message Authentication, Reporting and Conformance) is an industry initiative and standard developed specifically to combat many of the problems outlined above. It provides a way for organizations to declare which mail is authorized, and what to do with mail that isn't. DMARC builds on well established email authentication specifications SPF and DKIM and introduces a robust reporting mechanism. The datasets generated from DMARC afford an opportunity to observe a complete accounting of resources sending mail on behalf of a domain, misconfigured authentication (SPF/DKIM), sub-domain detection and more.

2. **Consolidate Vendors by Using a Reputable ESP:** Many reliable email delivery platforms are able to send your different types of messages (marketing, transactional, etc) all under one roof.

3. **Take Advantage of Current-Gen Reputation Solutions:** Employing a solution that provides actionable insights and real-time alerting for domain reputation, engagement trends, message efficacy will keep your organization apprised of any issues before or as they are happening to mitigate risk.

DMARC Adoption Trends and Getting Started

The number of valid DMARC policies observed in the domain name system (DNS), increased by roughly 300% over the course of 2019.

> **DNS** is a database that connects domain names to Internet addresses and contains records that play a crucial role in enabling email authentication.

At the end of 2018 there were roughly 630,000 valid DMARC policies published, and at the end of 2019 this figure was 1.89 million.[3] Though this adoption rate indicates widespread acceptance of the specification, of the 2,000 listed publicly traded companies, approximately 50% have yet to establish a DMARC record. Though DMARC is recognized globally as an industry standard, there is a misnomer that establishing a DMARC record and management is just too difficult.

There are several solutions armed to help you when it comes to implementing DMARC or employing DMARC best practices in your own mailings.

dmarcian is dedicated to upgrading the entire world's email by making DMARC accessible to all via education and advocacy. Their SaaS platform translates email data into a data-rich display and provides domain abuse alerts. Complementing the platform, dmarcian's AIM deployment model addresses how employing DMARC affects the different aspects of an organization; in addition, a dedicated support system helps people manage and maintain DMARC compliance in the long-term. DMARC is the foundation to protect and control your email domains and as part of a layered, comprehensive approach to phishing protection.

SparkPost believes DMARC is so valuable that it's integrated directly into their platform. Inbox Tracker Premier, SparkPost's deliverability solution, uses the most accurate data sources in the market to empower marketers to maximize their email revenue and improve the critical success of their email program. Message authentication is a large part of that critical success. Powered by dmarcian, SparkPost offers DMARC and authentication reporting through the Brand Protection feature in the Inbox Tracker Premier edition.

3. https://dmarc.org/2020/02/dmarc-policies-increase-300-over-2019/

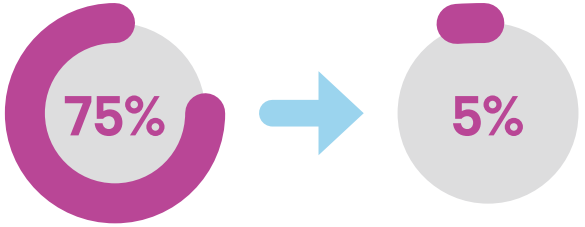
Case Study: Maintaining Brand Integrity with dmarcian

A leading agricultural and food distribution company began experiencing heavy attacks from successful spoofing and phishing efforts on a domain catalog that recently came under their control through acquisition. The food purveyor themselves had recently completed their own DMARC project, leaving them confident in the work that needed to be accomplished.

Because the domains in question were without a DMARC policy at the time of acquisition, the company had insufficient visibility into the unforeseen dangers that came along with the purchase. Immediately after DNS control was delegated, the company's IT team applied DMARC and gained invaluable insights in a matter of days. The challenges of understanding each email solution's capabilities, necessary configuration steps and tactical guidance were supplied by the dmarcian application and staff.

"Our IT department recognizes the benefit of DMARC; by using the dmarcian dashboard, it was easy to highlight the progress in protecting our domain. I don't know how we would have proven it otherwise," the company's DMARC project manager said.

The DMARC project concluded with all newly acquired domains reaching a restrictive policy of "reject." As a result, **the total outbound mail volume went from 75% unauthorized mail/abuse to less than 5%**. Though the road to domain and brand reputation recovery had only just begun, the attackers deemed their efforts fruitless and moved on to other susceptible targets.



Now, before this company purchases or acquires a domain, they require DMARC to be enabled to afford both management and email teams clear insights into how domains are being used (or abused) as well as visibility into their active email vendors. The result is a progressive, interdepartmental domain management process to identify, evaluate and understand all hosted and external services at play. This allows for informed decisions that significantly reduce risk and poor economies of scale.

DMARC Benefits at Your Organization

DMARC helps legitimize email by giving feedback to the domain owner about the email itself, including if SPF and/or DKIM are properly aligned. DMARC also tells email receivers like Gmail and Yahoo how to handle messages that fail to align with those protocols.

Here are four main benefits of implementing DMARC:

Visibility

DMARC provides you with detailed insight on all emails sent on behalf of your domain.

Security

With DMARC you can monitor your email flow for threats and unknown senders and prevent spoofing and phishing emails from being sent from your domain.

Identity

DMARC makes your email easy to identify across the huge and growing footprint of DMARC-capable receivers.

Deliverability

Using DMARC helps ensure your emails are delivered using the same technology that large companies use to deliver their email.

You've Convinced Me, What's Next?

How to Publish a DMARC Record

To start generating DMARC data, you must first publish a DMARC record for each of your domains. dmarcian's DMARC Record Wizard makes it easy to create a DMARC record in just a few simple steps:

1. Navigate to your domain's DNS settings. (These are typically located in the product settings where your domain was registered)
2. Locate the "Add a Record" option in your domain's settings
3. Set record type to TXT
4. Set host/target to _dmarc (note underscore!)
5. The Value is the DMARC record you would like to publish

Example

DMARC Record: v=DMARC1; p=none; rua=mailto:dmarc-reports@example.com;

This tells providers to take no action on email that fails the DMARC check[4] and to send aggregate XML reports to dmarc-reports@example.com.

Once you've published DMARC records, DMARC data will typically begin to generate within a day or two in the form of reports that give you insight into the way your domains are handling email.

These reports are XML-based and can be difficult to read and make sense of, especially when they can number in the thousands. There are services available to help interpret these reports (more on that below), which we help to maximize the effectiveness of the data you're reporting on.

With DMARC data flowing, you can then begin examining what sources are sending email on behalf of your domain and if those sources are legitimate. From there, it's a matter of compliance, making each legitimate email source DMARC compliant by deploying SPF and DKIM technologies, as well as learning more about the importance of SPF and domain management[5], and having a process around it in your organization.

Note: For SparkPost's Inbox Tracker users, the DMARC set-up protocol is fully integral to the platform through its DMARC Policy Manager.

4. https://dmarcian.com/start-dmarc/#DMARCpolicy
5. https://dmarcian.com/spf-management-challenge/

DMARC Policy

Part of the DMARC record, a DMARC policy[6] allows a sender to indicate that their messages are protected by SPF and/or DKIM and tells the receiving server what to do if neither of these are verified, such as marking the email as junk mail or denying its delivery.

A DMARC enforcement policy removes the responsibility of the management of these messages, thus limiting the exposure to potentially fraudulent or malicious messages. DMARC also provides a way for the email receiver (like Google and Microsoft) to report back to the sender about messages that pass or fail DMARC evaluation.

Senders can set their DMARC policy (referred to as "p=") to determine what happens to non-compliant email:

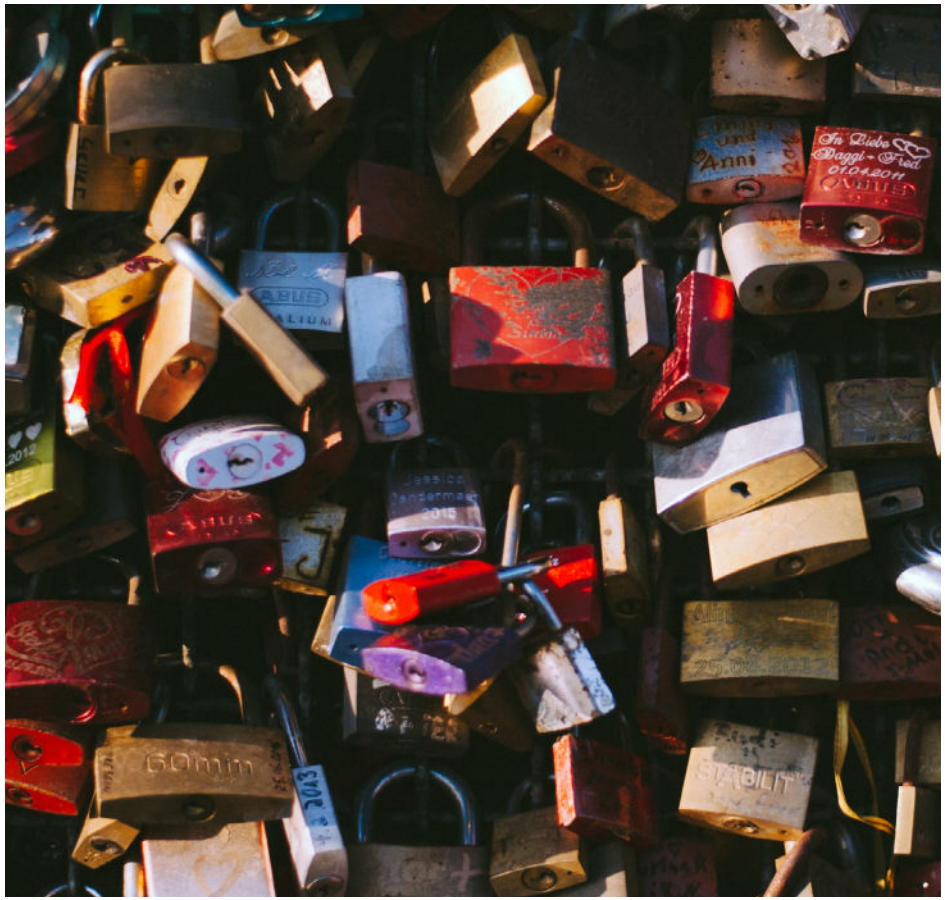
Monitoring (p=none) - no impact on mail flows

Quarantine (p=quarantine) - messages that fail DMARC are moved to spam folder

Reject (p=reject) - messages that fail DMARC aren't delivered at all

In addition to protection from spoofing, DMARC gives organizations visibility over their email domain and the ability to identify and audit all usage by third-party platforms. The IT organization may know and condone some shadow IT platforms that use their email domain as part of the FROM address, but they also may be ignorant of many other platforms that also do.

In an era when cybersecurity is always on the agenda (especially at the company board level), DMARC helps eliminate threats like spoofing while giving visibility into how people in the organization are using third party platforms to better enforce security policies.



6. https://dmarcian.com/policy-modes-quarantine-vs-reject/

Next Steps to Protect Your Brand

Email is a very powerful tool for businesses. Unfortunately, both the good guys and the bad guys know this—those in the latter category take advantage of that fact every day. That's why it's so critical to not only be aware of but understand and implement DMARC best practices to defend your brand's integrity and overall security posture. Starting small by first communicating the importance of DMARC to stakeholders and explaining how it works will help build a foundation of understanding and respect for authentication across the landscape of executives.

Then, by employing a service like dmarcian, who specializes in processing DMARC data and reports, you can begin to develop a holistic view of your organization's security footprint, and develop processes for bringing on new domains, acquiring domains already in use, and overall develop a more streamlined plan to align with all stakeholders in emails who have an impact on your brand's reputation and organization's overall security. dmarcian's platform categorizes sources of email and presents you with DMARC compliance status (based on email source, DKIM and SPF) and alerts you if there are any potential threats to or abuse on your domains. All of this information will arm you to make better business and process decisions.

Additional reading and resources on DMARC:

1. Department of Homeland Security Binding Operational Directive 18-01
2. Google Postmaster recommends DMARC
3. M3AAWG Statement on email authentication for COVID-19 Mailings
4. DMARC Explained
5. Global Cyber Alliance
6. APWG Phishing Activity Trends Report