TWILIO SendGrid × VALIMAIL
TRUST YOUR EMAIL

Uplevel Your Email SenderOps

Table of Contents

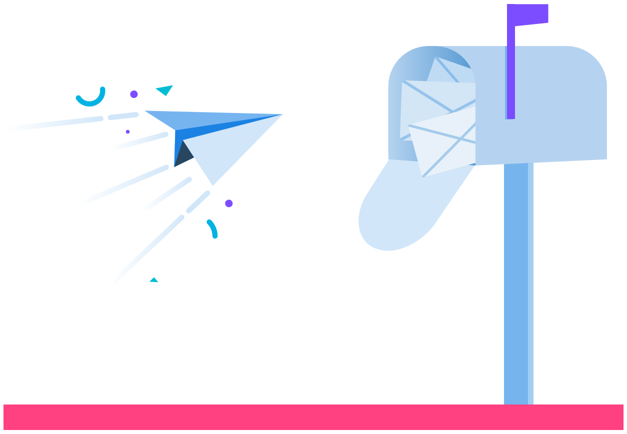
Introduction

We no longer send email from a single mail server or even a handful of servers. Instead, most of us use cloud-based systems (like Twilio SendGrid or Salesforce). This provides us with so much more flexibility—we can send email from anywhere in the world! But without the necessary precautions in place, this flexibility puts your brand at greater risk of phishing scams.

In fact, you've probably opened a phishing scam without even realizing it (see how seamless these phishing attempts can be in the example on the next page). **Research from Barracuda** showed that a whopping 82% of organizations faced an email-based security threat in 2019. These threats are costly to organizations, causing 25% to lose $100,000 or more. But it's more than money—a phishing scam can also damage a sender's reputation, identity, and brand, making it a lot harder to reach your customers in the inbox.

Twilio SendGrid and **Valimail** are tackling this conundrum together to help you reduce phishing, secure your domain, and boost your email performance. Together, we've simplified the best practices into one program for your teams: Sender Operations (SenderOps).

In this guide, we will cover the two core components of SenderOps: identity and reputation. Learn how to optimize your sending practices and offer mailbox providers reliable cues to determine the legitimacy of your email. You'll strengthen your sender identity and reputation so that your email is secure—no matter where it comes from.



WE USE THESE TERMS A LOT. WHAT DO THEY MEAN?

SenderOps: A program focused on the best practices for maintaining a trusted sender profile, securing and elevating the sender and their brand through email; this includes maintaining sending reputation and sender identity.

Sending reputation: Sending reputation is how mailbox providers evaluate you as a sender. Every time you send an email campaign, mailbox providers collect valuable data that says whether or not you follow proper sending practices. Your sender reputation is determined by a wide variety of factors, including recipient engagement, email content, spam complaints, spam traps, invalid email addresses, deny lists, and domain reputation.

Sender identity: Your sender identity is the mail sender information in the "From" field that includes server domain name, email username, and sometimes the name of the person or generic account that the sender ties to the account (e.g. "John Smith" or "Amazon Tech Support").

Want to fake an email? It's surprisingly easy

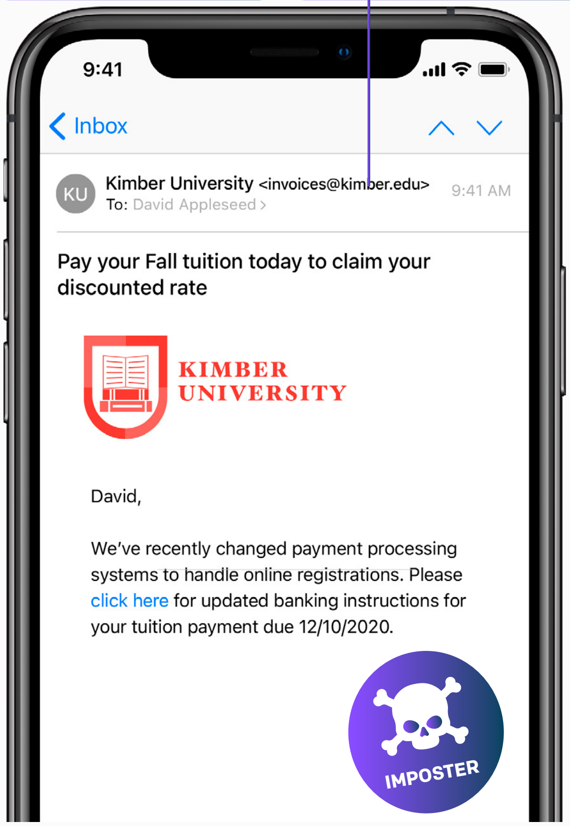
At the time of their creation, the Internet and email were only accessible to a handful of people, so there was no room for impersonation. The **inventors of email** didn't know how popular and central to business email would become, so they didn't include any way to verify an email sender's identity. Because of this oversight, email headers, including the "From:" and "Reply-to:" fields, are remarkably easy to fake.

This has resulted in a prominent and highly convincing type of email impersonation that is referred to as exact-domain spoofing.

REAL OR FAKE? CAN YOU SPOT THE DIFFERENCE?

Sent from a [kimber.edu] address to customers and partners.

Currently allowed because the domain does not have a DMARC policy.



Kimber University <invoices@kimber.edu> 9:41 AM
To: David Appleseed >

Pay your Fall tuition today to claim your discounted rate

KIMBER UNIVERSITY

David,

We've recently changed payment processing systems to handle online registrations. Please click here for updated banking instructions for your tuition payment due 12/10/2020.

Read on to see how this type of impersonation is possible.

With exact-domain spoofing, attackers appear as legitimate senders coming directly from the company's email servers. In other words, they can put an actual company email address in the "From" field of the phishing message. And for many domains, this will be delivered in exactly the same way a legitimate message is, regardless of where it was actually sent from.

These exact-domain attacks can have a disastrous impact on a company's brand when attackers use the organization's domain for faking sender identity in "*outbound" messages that they send to the company's business partners, customers, or random members of the public.

**Note*: these emails don't actually originate from the company's infrastructure—the company's servers or authorized cloud services are not used, but the email can still appear legitimate.

IMPERSONATION REMAINS A LEADER OF PHISHING SCAMS

83% of all email attacks focus on **brand** impersonation, and another 6% of attacks impersonate **people**, like your CEO, instead of the brand itself. (**Barracuda, 2019**)

How is it that hackers can so easily manipulate the sender to appear to come from any brand they want? Until 2015, there was no mechanism in place to verify the "From" address. This allows any sender to put whatever email in the "From" address, even if it doesn't match the actual sender.

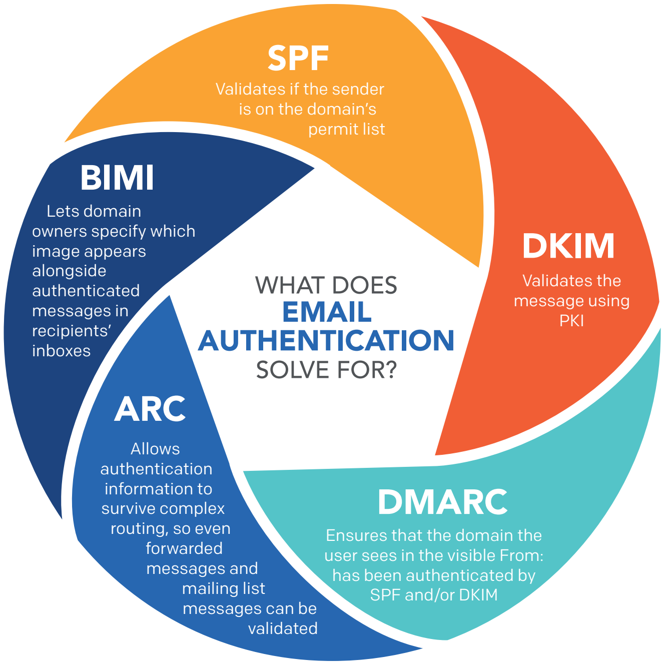
From the perspective of your sending reputation, this can cause a lot of damage. Imagine a large number of recipients receive an email from this unauthorized sender using your domain and have never heard of your company. The email is immediately deleted or marked as spam by the recipients. With enough spam complaints, your brand could be blocked (yikes!).

However, this isn't all bad. This setup is what allows us to use third-party cloud services, like payroll and marketing automation tools, and have emails sent by that platform appear as if they were sent directly from your company. Luckily, a solution now exists. And it puts the domain owner in control of who can and cannot use their sender identity to send email.

Protect your sender identity with email authentication

By implementing email authentication, you enable only those senders that you explicitly authorize, thereby blocking everyone else who attempts to send in your name—spammers, phishers, and "shadow email" senders that may be legitimate but have not been vetted or authorized. This protects your sender identity from being abused by impersonators and prevents damage to your sending reputation.

> "The five key standards solve a fundamental flaw of email—it can't be trusted. Each standard restores trust in a different way.


SPF
Validates if the sender is on the domain's permit list
DKIM
Validates the message using PKI
DMARC
Ensures that the domain the user sees in the visible From: has been authenticated by SPF and/or DKIM
ARC
Allows authentication information to survive complex routing, so even forwarded messages and mailing list messages can be validated
BIMI
Lets domain owners specify which image appears alongside authenticated messages in recipients' inboxes
WHAT DOES EMAIL AUTHENTICATION SOLVE FOR?

AN OVERVIEW OF EMAIL AUTHENTICATION PROTOCOLS

Email authentication collectively refers to the open Internet standards that validate email senders. Here's a high-level overview:

SPF (Sender Policy Framework) is the standard that pioneered the concept of domain-based email authentication. SPF lets domain owners publish a list of approved IP addresses. If a mail server with an IP address that's not on the list tries to send email using that domain, it won't pass SPF authentication.

DKIM (DomainKeys Identified Mail) uses public-key cryptography to authenticate individual email messages. If the contents of the signed headers and message are not altered, the DKIM signature will still work. With proper implementation, DKIM ensures that messages are not tampered with in transit.

DMARC (Domain-based Message Authentication, Reporting and Conformance) builds on SPF and DKIM to stop exact-domain email spoofing by matching what is checked by SPF and DKIM with what the end-user actually sees—the "From" header field.

BIMI (Brand Indicators for Message Identification) allows brands to provide brand-specific imagery that appears alongside messages they send. However, In order to use BIMI, senders must be using DMARC with an enforcement policy.

ARC (Authenticated Received Chain) is a small percentage of messages that will still fail authentication after being forwarded or passed through a mailing list. This problem is addressed by implementing ARC. The Authenticated Received Chain protocol provides an authenticated "chain of custody" for a message. In simple terms: ARC allows receivers to make delivery decisions for email that has been complexly routed.

Each of the standards have their own complexities for implementation, so if you want a deeper dive, check out the **Email authentication handbook**—a 44-page deeper dive into the standards.

Email authentication and in particular, DMARC, provides a variety of benefits to your sending reputation and identity. While SPF and DKIM are necessary email authentication measures, DMARC offers the strongest method for protecting users from exact domain spoofing attacks. What this means is you'll have full control over the "from" address that appears in a recipient's inbox. DMARC ensures that the DKIM key's domain (or the SPF verified sender) and the domain shown in the "from" address match. This prevents phishers from using a false domain in the "from" address while sending the message with an unrelated domain that they control.

DMARC Enforcement

A key part of the DMARC standard is that it gives domain owners the ability to specify a policy for how they'd like receivers to handle email messages that fail authentication.

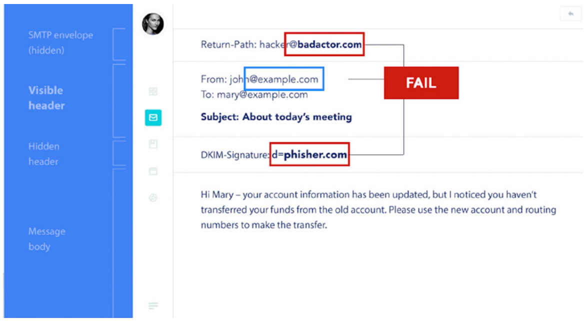
DMARC policy is spelled out with the "p" parameter, for which there are three options:

- **p=none**: No enforcement; mail that fails authentication is delivered normally. This setting is intended as a "test" mode, so domain owners have a way to troubleshoot their authentication settings without the risk of legitimate messages getting blocked.
- **p=quarantine**: Messages that fail authentication should be quarantined. Usually this means that the messages are delivered to a user's spam folder.
- **p=reject**: Messages that fail authentication should be discarded, not delivered at all. Some receivers honor this request, while others just mark failing messages as spam.

If your goal is to stop phishing and impersonation attacks, you need to get to enforcement with a policy of quarantine or reject. Then you will begin to see the anti-impersonation and anti-phishing benefits of DMARC.

EXAMPLE WITHOUT DMARC AT ENFORCEMENT

This fake email would be delivered on behalf of the brand, even though the sender is not aligned with the brand.



Return-Path: hacker@**badactor.com**

From: john@example.com
To: mary@example.com

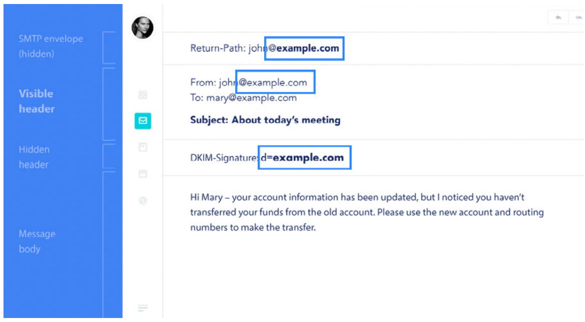
Subject: About today's meeting

DKIM-Signature: d=**phisher.com**

Hi Mary – your account information has been updated, but I noticed you haven't transferred your funds from the old account. Please use the new account and routing numbers to make the transfer.

EXAMPLE WITH DMARC AT ENFORCEMENT

Only aligned messages (authorized messages) will be delivered.



Return-Path: john@**example.com**

From: john@example.com
To: mary@example.com

Subject: About today's meeting

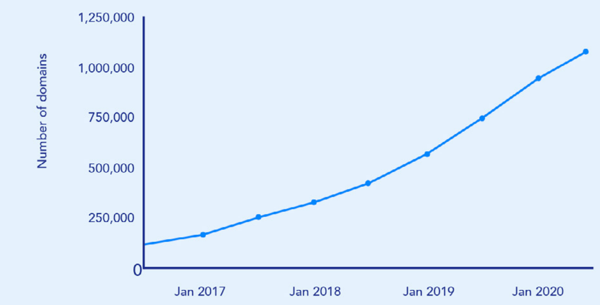
DKIM-Signature: d=**example.com**

Hi Mary – your account information has been updated, but I noticed you haven't transferred your funds from the old account. Please use the new account and routing numbers to make the transfer.

DMARC ADOPTION IS ON THE UP AND UP

According to the latest **Valimail research**, 1 million+ domains now use DMARC, which is almost 2.5X growth in under 3 years. Plus, it's widely accepted by mailbox providers. About 80% of the world's inboxes (including virtually all U.S.-based email providers) do DMARC checks on inbound email messages, enforcing the domain owner's stated policies.

TOTAL DOMAINS WITH DMARC



NOTE: VALIMAIL'S ANALYSIS COUNTS ORGANIZATIONAL DOMAINS ONLY. WE ARE NOT INCLUDING SUBDOMAINS IN THESE TOTALS.

SOURCE: VALIMAIL

Email authentication benefits

One of the biggest benefits of DMARC is that the number of attempts to spoof a domain typically drops to zero or near zero within a few months after that domain moves to DMARC enforcement. Would-be impersonators give up and move on to other targets or adopt other techniques.

The issue is that getting to enforcement is notoriously difficult, but you only get the anti-spoofing benefits when you reach that level of implementation. And of the 1 million+ DMARC records, only **13.9%** have enforcement policies.

Improvements in email deliverability

Added security isn't the only benefit. Inbox providers, like Google and Yahoo, are more likely to deliver email from authenticated senders.

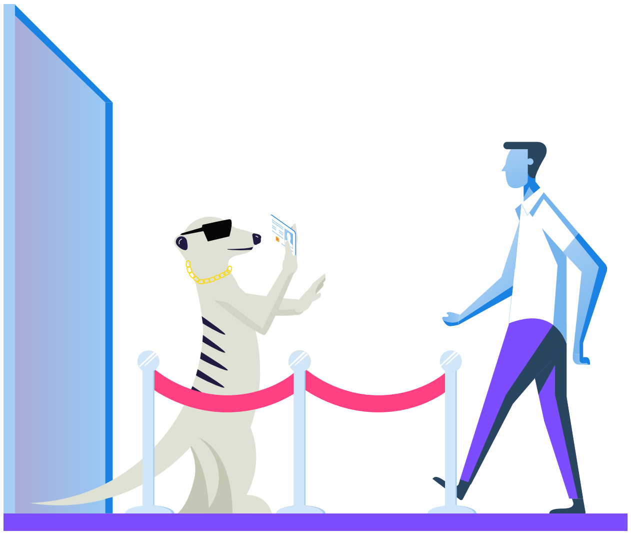
Research from Valimail shows that when a domain deploys a DMARC enforcement policy, **deliverability increases on average by 10%**. And, if the domain starts off with an especially bad sending reputation, the delivery rate can be even higher. Email already has a high ROI, bringing in **$42 for every dollar spent**. But to make the most of that ROI, your mail has to make it to the inbox. Small improvements, even a 1% increase in your delivery rate, can make a big difference to your email program. Imagine what a 10% increase could do.

For more information on email deliverability, check out Twilio SendGrid's annually published **Email Deliverability Guide.**

More benefits with BIMI

BIMI allows brands to add a logo next to their email, making their emails easily recognizable and improving a users' experience with the brand. In fact, Verizon Media found that it makes a difference in more than just visual appeal. **Their research** showed that companies using BIMI saw a 10% increase in open rates compared to brands that did not have a logo next to the email.

In addition to improving brand recognition and increasing open rates (yes, there's more!), it also promotes the use of email authentication and prevents phishing attacks. In order to use BIMI, senders must have a DMARC enforcement policy in place. The policy ensures that only the sender can send email from the domain, the sender has full visibility into who is using the domain, and any unauthorized senders are blocked. By motivating senders to authenticate their email to the highest degree, BIMI will help create herd immunity against exact-domain spoofing attacks.



For more information on BIMI, its benefits, and how to implement it, check out Valimail's article: **The benefits of BIMI—and how to get ready for it.**

Take control of your sender identity

We've talked about the dangers of phishing and the importance of email authentication.

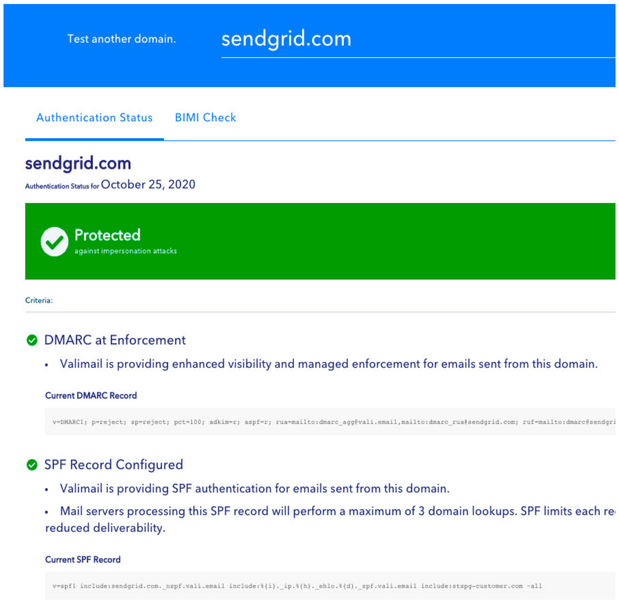
> So, how do you take control of your sender identity? It actually might be simpler than you think.

Valimail provides a free domain checking tool that verifies your domain's authentication status. If you're at square 1 wondering how many of the authentication protocols are set up for your domain, this is where you need to start.

Want to check the status of your domain? Find out with Valimail's **Domain Status Checker**.

Here's an example report when Twilio SendGrid's website is entered into Valimail's domain checker. In the image below, you can see that SendGrid meets Valimail's standards for DMARC at enforcement and SPF.

TWILIO SENDGRID'S DOMAIN STATUS REPORT



sendgrid.com

Authentication Status for October 25, 2020

Protected

against impersonation attacks

Criteria:

✓ DMARC at Enforcement

- Valimail is providing enhanced visibility and managed enforcement for emails sent from this domain.

Current DMARC Record

```
v=DMARC1; p=reject; sp=reject; pct=100; adkim=r; aspf=r; rua=mailto:dmarc_agg@vali.email,mailto:dmarc_rua@sendgrid.com; ruf=mailto:dmarc@sendgri
```

✓ SPF Record Configured

- Valimail is providing SPF authentication for emails sent from this domain.
- Mail servers processing this SPF record will perform a maximum of 3 domain lookups. SPF limits each re reduced deliverability.

Current SPF Record

```
v=spf1 include:sendgrid.com._nspf.vali.email include:%{i}._ip.%{h}._ehlo.%{d}._spf.vali.email include:stspg-customer.com ~all
```

The next step towards protection

Once you know your domain's status, you need to know who is sending from your domain and identify the legitimate vs. fraudulent senders.

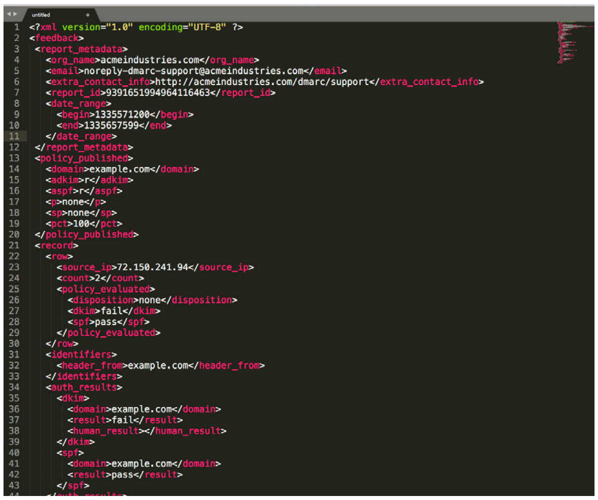
When you set up your DMARC record, you can provide an email address to receive DMARC reports.

Check out how to build your DMARC record with Valimail's **Making Sense of DMARC Records and Tags**.

To set up DMARC for your Twilio SendGrid account, here is your step-by-step **guide to DMARC implementation**.

All of the data you need to maintain a DMARC program and identify senders is available in these reports, but that doesn't mean they are easy to interpret. The raw DMARC reports are simply XML data dumps with lines of detail about the IP addresses and authentication status of each email.

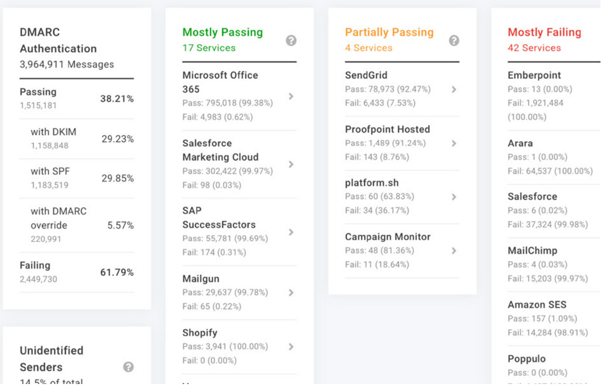
EXAMPLE XML REPORT



```xml
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
    <org_name>acmeindustries.com</org_name>
    <email>noreply-dmarc-support@acmeindustries.com</email>
    <extra_contact_info>http://acmeindustries.com/dmarc/support</extra_contact_info>
    <report_id>9391651994964116463</report_id>
    <date_range>
      <begin>1335571200</begin>
      <end>1335657599</end>
    </date_range>
  </report_metadata>
  <policy_published>
    <domain>example.com</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>none</p>
    <sp>none</sp>
    <pct>100</pct>
  </policy_published>
  <record>
    <row>
      <source_ip>72.150.241.94</source_ip>
      <count>2</count>
      <policy_evaluated>
        <disposition>none</disposition>
        <dkim>fail</dkim>
        <spf>pass</spf>
      </policy_evaluated>
    </row>
    <identifiers>
      <header_from>example.com</header_from>
    </identifiers>
    <auth_results>
      <dkim>
        <domain>example.com</domain>
        <result>fail</result>
        <human_result></human_result>
      </dkim>
      <spf>
        <domain>example.com</domain>
        <result>pass</result>
      </spf>
```

Instead, you can get access to **DMARC Monitor™** for free. With DMARC Monitor, maintenance goes from parsing through large volumes of XML data to a single sign in to the dashboard where you can see the names of your services (instead of IP addresses), with a clear view of their authentication status.

DMARC MONITOR DASHBOARD



DMARC Authentication
3,964,911 Messages

Passing 1,515,181 38.21%
with DKIM 1,158,848 29.23%
with SPF 1,183,519 29.85%
with DMARC override 220,991 5.57%
Failing 2,449,730 61.79%

Unidentified Senders
14.5% of total

Mostly Passing
17 Services

Microsoft Office 365
Pass: 795,018 (99.38%)
Fail: 4,983 (0.62%)

Salesforce Marketing Cloud
Pass: 302,422 (99.97%)
Fail: 98 (0.03%)

SAP SuccessFactors
Pass: 55,781 (99.69%)
Fail: 174 (0.31%)

Mailgun
Pass: 29,637 (99.78%)
Fail: 65 (0.22%)

Shopify
Pass: 3,941 (100.00%)
Fail: 0 (0.00%)

Partially Passing
4 Services

SendGrid
Pass: 78,973 (92.47%)
Fail: 6,433 (7.53%)

Proofpoint Hosted
Pass: 1,489 (91.24%)
Fail: 143 (8.76%)

platform.sh
Pass: 60 (63.83%)
Fail: 34 (36.17%)

Campaign Monitor
Pass: 48 (81.36%)
Fail: 11 (18.64%)

Mostly Failing
42 Services

Emberpoint
Pass: 13 (0.00%)
Fail: 1,921,484 (100.00%)

Arara
Pass: 1 (0.00%)
Fail: 64,537 (100.00%)

Salesforce
Pass: 6 (0.02%)
Fail: 37,324 (99.98%)

MailChimp
Pass: 4 (0.03%)
Fail: 15,203 (99.97%)

Amazon SES
Pass: 157 (1.09%)
Fail: 14,284 (98.91%)

Poppulo
Pass: 0 (0.00%)

This gives you the information needed to configure SPF and DKIM for each approved sender.

Valimail Enforce® can automate this process for you, but if you're interested in implementing SPF, DKIM, and DMARC yourself, here is a quick visual of the steps you need to take: **Six steps for operationalizing email authentication**.

Maintaining a secure sender identity

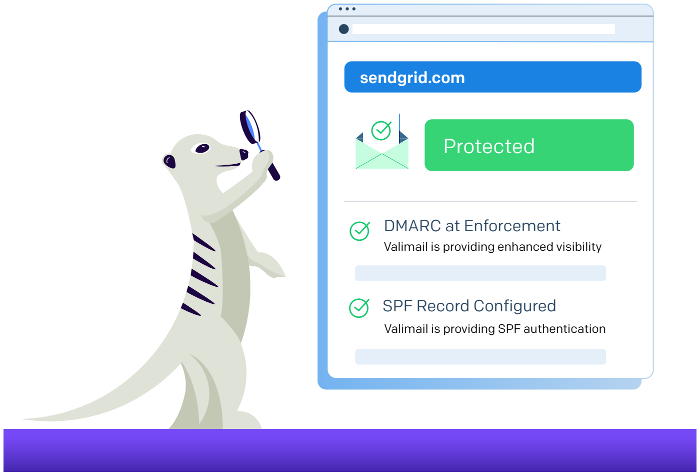
The authentication program doesn't stop when you reach enforcement. As your organization grows and evolves, you will likely add new cloud services and retire the out-of-date services. If you do not keep up with this ongoing process, good emails can end up blocked by the receiver. For instance, if you authorize a service to send email on your behalf, and then switch to Twilio SendGrid without updating your DMARC configuration, all emails would fail authentication. This is just one example, but there are many other reasons that services will come and go throughout your time at an organization.

And your organization is not the only one that will experience changes.

> “Third-party cloud services also change their underlying configuaration—sometimes without notice—which could lead to critical email workflows breaking.

If you do experience a change in your sending services, whether from internal factors or the services themselves changing, you must have a system in place to monitor for these changes. This can be done by monitoring the daily DMARC reports to verify the authentication status of your approved services and identify any new services that may pop up on these reports.

Once you notice a service that is failing authentication, you'll need to follow the previous steps to update or add the appropriate SPF record and DKIM key for the authorized services. You'll also need to remove the SPF or DKIM specifications for services that are no longer valid.


sendgrid.com
Protected
DMARC at Enforcement
Valimail is providing enhanced visibility
SPF Record Configured
Valimail is providing SPF authentication

Managing your sender reputation

By implementing DMARC at enforcement, mailbox providers know who should be sending your email. This helps the mailbox providers verify your identity as a sender and trust your email, ultimately improving your sender reputation.

To better understand how you are being perceived as a sender, it's valuable to regularly check your sending reputation. A poor score could be indicative of a phishing scam, poor engagement rates, or a deny list. Twilio SendGrid's article, **5 Ways to Check Your Sending Reputation**, lists 5 tools like Google Postmaster Tools, SenderScore, and TrustedSource to help you better understand your sending reputation.

While these tools provide insight into how inbox providers view you as a sender, the reputation scores are not the full picture. Use the scores in conjunction with other factors, like how recipients are engaging with your emails and your list collection practices, to truly understand your sending reputation. Here are a few factors to keep in mind.

Keep an eye on your benchmarks

Each mailbox provider evaluates a sender's reputation a bit differently, so one of the best ways to determine how your sender reputation is performing across providers is to understand if you are reaching or under/overperforming on your email benchmarks. If you see your open rates decrease or your spam complaints increase, it's likely that your sender reputation will be affected negatively. On the flip side, a higher open rate or click-through rate signals to the mailbox provider that you're sending valuable content, which is likely to improve your sender score.

In 2019, **the global aggregate open rate was 14.5% and the click-through rate was 1.6%**. If you are new to sending and don't have an idea of what is a good (or bad) engagement rate, use these stats as jumping-off points. From there, you can fine-tune the benchmarks you'd like to reach by evaluating what a successful campaign means for your business. Use the scores in conjunction with other factors, like how recipients are engaging with your emails and your list collection practices, to truly understand your sending reputation.

Follow contact list best practices

To help your sender engagement rates and your sending reputation, follow **list collection and cleaning best practices**. This means never purchasing lists. The contacts that are on purchased lists don't know your brand, so they're unlikely to engage with your content.

These lists are also much more likely to have **spam traps** (also known as honey pots). Spam traps are email addresses that mailbox providers, corporations, and deny list organizations use to identify and catch spammers. You can also fall into spam traps if you haven't cleaned your list in a while. Think about the last time you cleaned out your contact list. Was it a year ago? 2 years? Never...? Many spam traps are converted from old, unused email addresses making an uncleaned list a minefield for these traps. And, the more spam traps you hit, the more likely you are to ding your sending reputation or even be deny listed.

WHAT IS CLUSTERING?

Clustering is a mailbox providers' way of grouping multiple data points to better understand your sending reputation. For example, by clustering your campaign's from address, email authentication, and IP address, the mailbox provider can create a fingerprint of you as a sender. This helps the mailbox provider evaluate whether or not you're sending wanted or unwanted email. And, it helps you strategically divide your sending by informing decisions like separating mail streams. **Learn more here**.

IP and domain deny lists

If you're receiving a number of spam complaints or you're frequently landing in spam traps, the next natural step is that your IP address or domain is deny listed. Being added to a deny list greatly affects your email deliverability, but it's also a sign that your sending reputation is suffering.

Could you be on a deny list? We recommend regularly checking whether or not you've been added to a deny list **with this free tool**.

If you are deny listed, don't swap your IPs or domains. You may see a small improvement in the short term, but it will have negative long term effects. Instead, work with delivery experts, like **SendGrid's Expert Services**, to help you navigate the murky waters of the deny list world.

Building and maintaining successful sender operations

Ultimately, establishing a secure sender identity and sender reputation builds trust with your mailbox provider. This trust carries on throughout the sending process, improving your email deliverability and engagement metrics. While phishing and bad actors can pose a threat to your SenderOps program, if you have the right balances and checks in place, you'll protect your sender identity and reputation from harm. Rely on sending best practices like email authentication, organic email address collection, and the continuous monitoring of your sender reputation to secure your sender profile.

Take the first step towards protecting your domains and brand—sign up for your free **DMARC Monitor** for Twilio SendGrid account. Know who is sending from your domain and uncover fraudulent senders posing as your brand. If you don't have a Twilio SendGrid account, **sign up for a free trial** and access Valimail's DMARC Monitor tool alongside your email platform.

ABOUT TWILIO SENDGRID

Twilio SendGrid helps you focus on your business without the cost and complexity of owning and maintaining an email infrastructure. We help with all technical details (from sender reputation to email authentication) and offer world-class deliverability expertise to help your emails reach the inbox. With a full-featured marketing email service that offers an intuitive workflow, effortless list segmentation, and actionable analytics, all of your email needs are met in one simple platform. Learn more about **Twilio SendGrid**.

ABOUT VALIMAIL

Valimail is the global leader in zero-trust email security. The company's full line of cloud-native solutions authenticate sender identity to stop phishing, protect brands, and ensure compliance; they are used by organizations ranging from neighborhood shops to some of the world's largest organizations, including Uber, Splunk, Yelp, Fannie Mae, Mercedes Benz USA, and the U.S. Federal Aviation Administration. Valimail is the fastest growing DMARC solution, with the most domains at DMARC enforcement, and is the premier DMARC partner for Microsoft 365 environments. For more information visit **www.valimail.com**.

TWILIO SendGrid