E-BOOK

DMARC: The Key to Email Deliverability

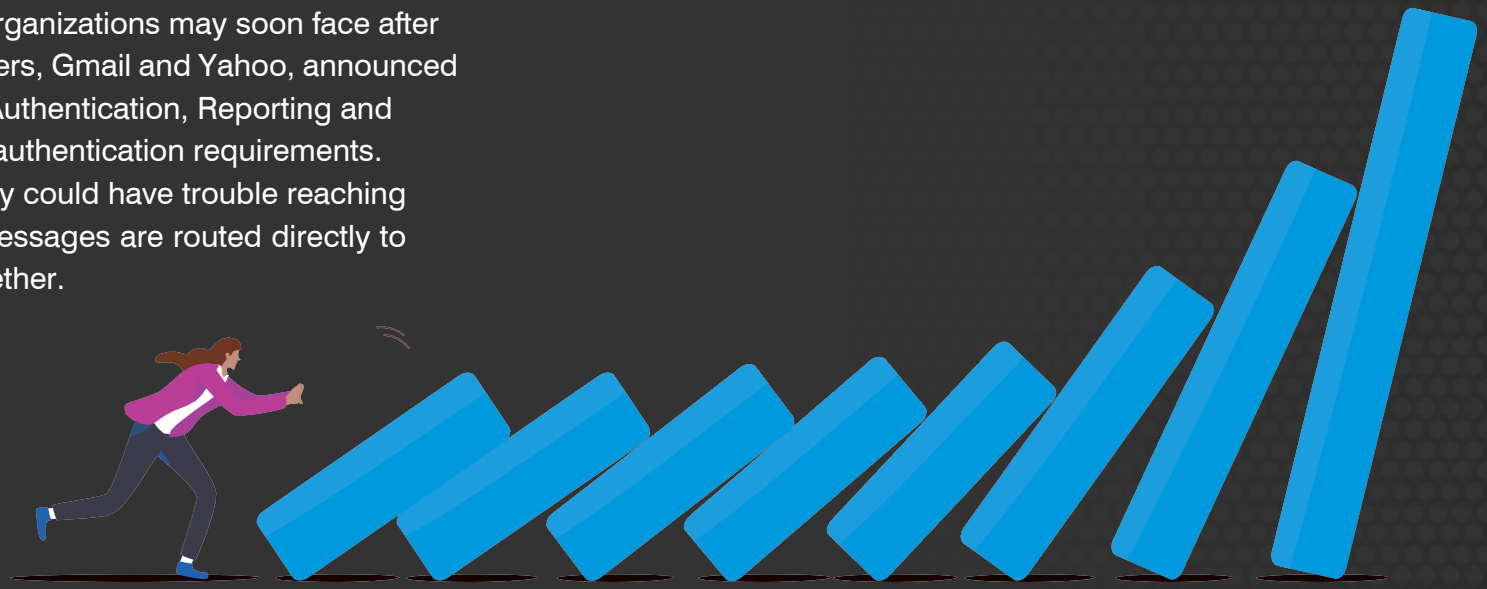
Why email authentication is no longer optional for reaching prospects, serving your customers and protecting your brand

proofpoint.

Introduction: D-Day for DMARC

Imagine what would happen if your customers simply stopped getting your company's emails. Suddenly, your fastest and most effective marketing channel is gone. Customers can't log in to verify their identity or reset their passwords. Customer support comes to a halt.

That's precisely the scenario organizations may soon face after two of the biggest email providers, Gmail and Yahoo, announced new Domain-based Message Authentication, Reporting and Conformance (DMARC) email authentication requirements. Organizations that don't comply could have trouble reaching customers through email as messages are routed directly to spam folders or rejected altogether.



The goal

Email is one of the most widely used and effective communication channels in the modern world. But it also faces many challenges and threats from cybercriminals who exploit this channel to launch phishing, spoofing and spamming attacks.

By requiring DMARC for senders who send more than 5,000 emails per day to Gmail or Yahoo Mail addresses, the internet giants aim to protect their users from malicious emails that impersonate trusted senders or domains. These include business email compromise (BEC) scams that cost organizations billions of dollars every year. The companies also hope to spur better email practices and standards across the industry. These norms include enabling easy unsubscribe options and staying under a reported spam threshold.

Together, the measures aim to help reduce the amount of unwanted and fraudulent emails that clutter users' inboxes and lower their trust in email.

The challenge

But setting up DMARC correctly is not a trivial task. It requires careful configuration and monitoring of Domain Name System (DNS) records, alignment of Send Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) identifiers, testing of various DMARC policies and analysis of DMARC reports.

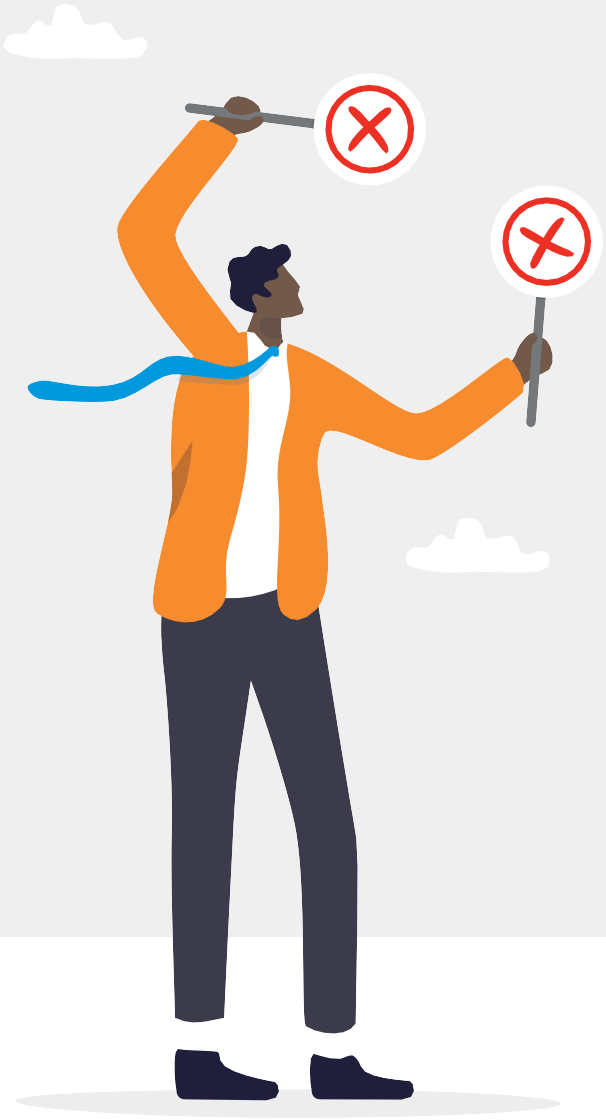
Failing to do so can result in legitimate emails being blocked or marked as spam, which can hurt email deliverability and performance. That's why it is essential for organizations that rely on email communication to understand the benefits and challenges of DMARC and how to implement it properly before the new requirements take effect.

This e-book explains how DMARC works, explores DMARC's impact on email deliverability and offers some best practices and advice for achieving the best DMARC results.

SECTION 1

Email: Essential to Modern Business

In today's fast-paced digital world, email has become the lifeblood of the modern economy. To say that organizations depend on it to keep their operations running smoothly is an understatement. From marketing strategies to customer service, the daily exchange of millions of emails supports almost every aspect of business.



A mandatory marketing tool

Marketing teams rely heavily on email as the main vehicle for their campaigns, using it to reach out to potential and existing customers with offers, news and content to drive engagement and sales.

A traffic route for transactions

For customers, the ability to reset passwords or receive one-time login codes via email is vital. Without this transactional email, they couldn't access services or do business with your organization.

A key to customer service

The post-purchase experience is greatly enhanced by order confirmations, digital receipts and follow-up surveys sent through email. These emails aren't just expected—they're demanded by customers as a baseline aspect of customer service.

And today's top target

Without trustworthy email, many aspects of business would come to a standstill. Unfortunately, email has also become a prime target of cybercriminals who seek to exploit your domain and your users' trust.

SECTION 2

Why DMARC?

One of the most common and costly forms of email fraud is business email compromise (BEC). (In these attacks, fraudsters impersonate trusted senders with spoofed or lookalike email addresses.) According to the FBI, BEC scams cost organizations $51 billion between 2013 and 2022.[1] And Proofpoint research has found that more than 3 in every 4 organizations faced at least one BEC attempt in 2022.[2]

As email fraud became a growing threat, a consortium of 20 companies—including Google, Yahoo, Microsoft, and Facebook—agreed on the DMARC standard in 2012. DMARC is an open email authentication protocol that enables domain-level protection of email. It builds on existing standards SPF and DKIM, which are used to verify the sender's identity and the integrity of the email message.

1 FBI. "Business Email Compromise: The $50 Billion Scam." June 2023.
2 Proofpoint. "State of the Phish." March 2023.

BEC scams cost organizations $51B

between 2013 and 2022.

More than 3 in every 4

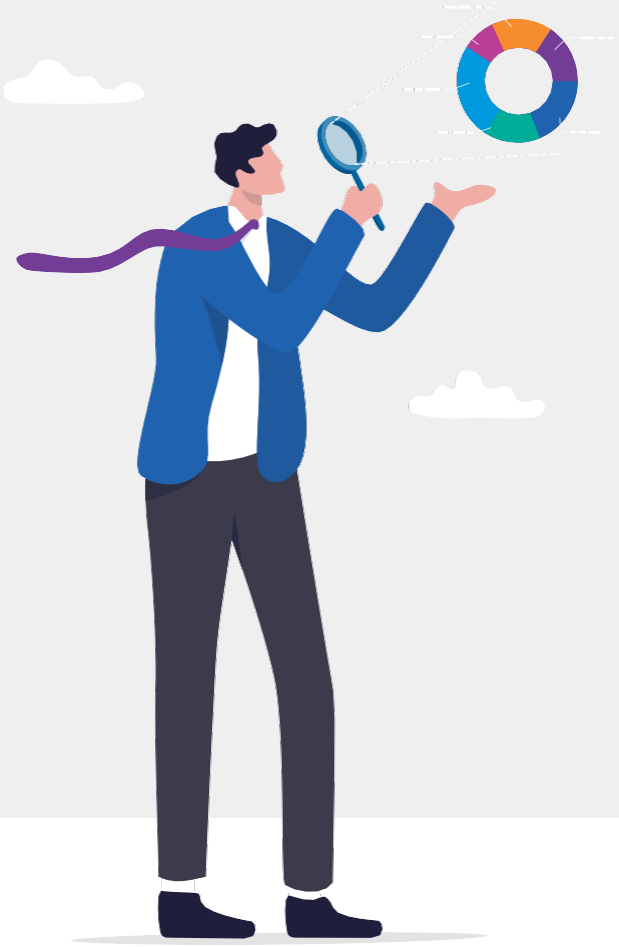
organizations faced at least one BEC attempt in 2022.

Here are the main features and benefits of SPF, DKIM and DMARC:

	Description	Benefit
SPF	A DNS record that specifies which IP addresses are authorized to send email from a domain.	Prevents unauthorized use of a domain by spammers or spoofers.
DKIM	A digital signature embedded in the email header that proves the message was sent by the domain owner and was not tampered with in transit.	Ensures the authenticity and integrity of the email message.
DMARC	A DNS record that defines how SPF and DKIM results should be interpreted and what actions should be taken if an email fails authentication checks.	Enables domain owners to monitor and control how their domains are used in email communication.

DMARC is the first and only widely deployed technology that can make the “From:” header domain (what users see in their email clients) trustworthy. By using DMARC, domain owners can prevent their domains from being used in phishing or spoofing attacks that target their customers, employees and partners.

But DMARC adoption has been slow and uneven. To speed up adoption of DMARC and improve email security, Google and Yahoo announced in late 2023 that emails that don’t meet certain SPF, DKIM and DMARC standards could be blocked or sent straight to users’ spam folders. The standards are strictest with senders of more than 5,000 emails per day to Gmail or Yahoo Mail addresses.



Beyond these market-driven incentives, new rules are ratcheting up the pressure for implementing DMARC. Starting in early 2025, PCI DSS V4.0 will require anti-phishing mechanisms to be in place, which means auditors could fail companies that have not implemented DMARC.

Regional mandates will further increase the demand for DMARC compliance. Japan's United Security Standards, for instance, sets a July 2024 target date for all government agencies to implement a DMARC reject policy. Japanese authorities are also pushing for all credit card companies to also implement DMARC reject policy by February 2024.

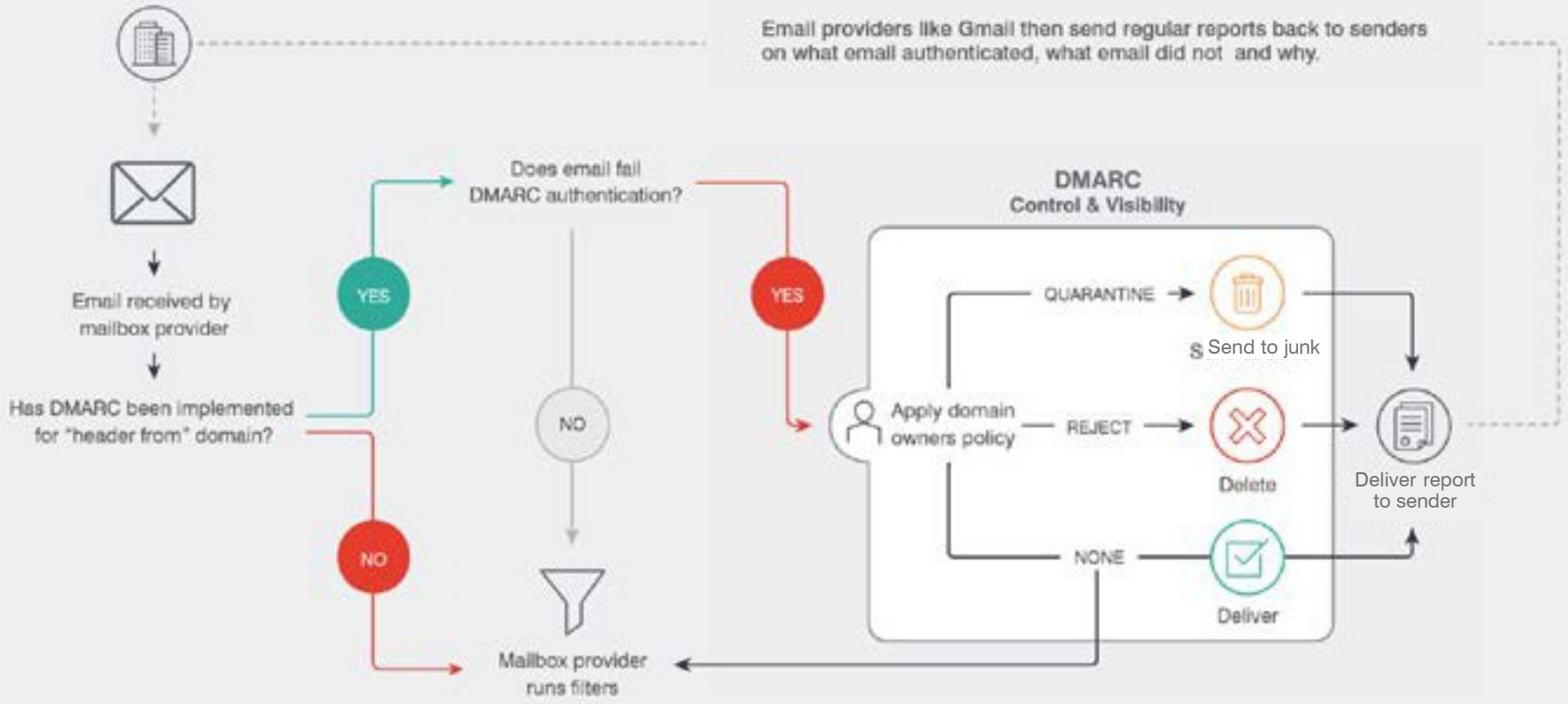
How DMARC works

Any organization that uses email as a vital communication channel must understand DMARC and how to implement it correctly.

DMARC works by authenticating legitimate email messages for their email-sending domains. It does this by checking whether the email message passes two existing standards: SPF and DKIM.

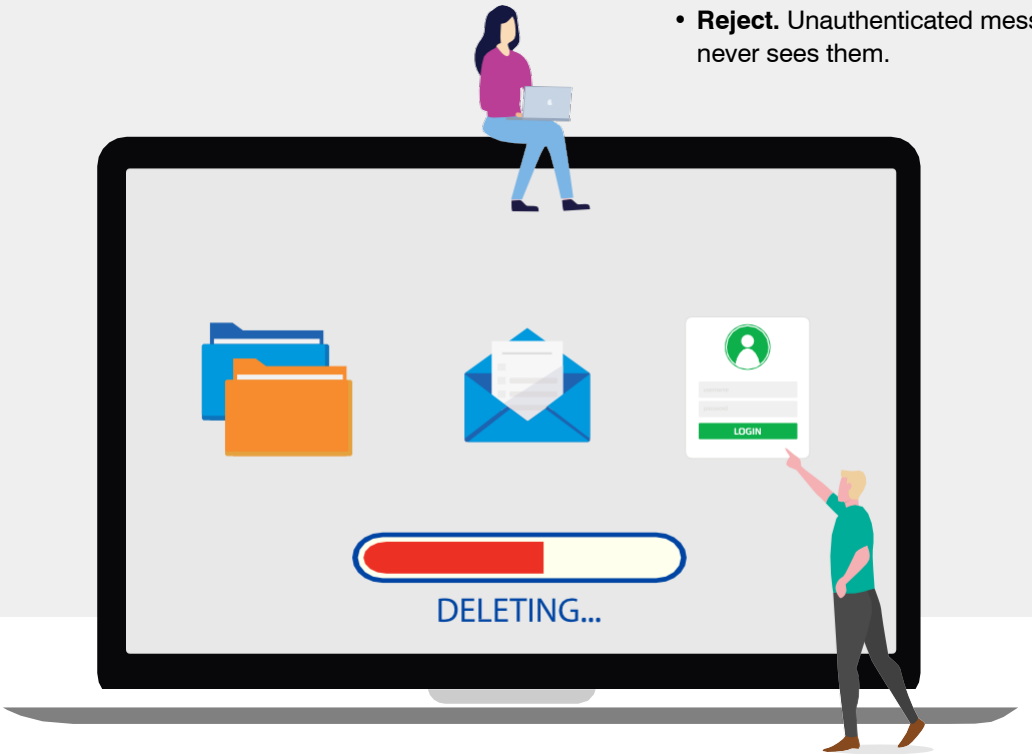
SPF verifies that the email message comes from an IP address that is authorized by the domain owner; DKIM verifies that the email message has a valid digital signature that matches the domain owner's public key.

If either of these checks fails, the email message is considered unauthenticated—and potentially fraudulent.


Email providers like Gmail then send regular reports back to senders on what email authenticated, what email did not and why.
Email received by mailbox provider
Has DMARC been implemented for "header from" domain?
YES
NO
Does email fail DMARC authentication?
NO
YES
DMARC
Control & Visibility
Apply domain owners policy
QUARANTINE
Send to junk
REJECT
Delete
NONE
Deliver
Deliver report to sender
Mailbox provider runs filters

Using an explicit policy setting, DMARC also instructs mailbox providers on how to treat messages that fail authentication. These messages can either be sent to a junk folder or rejected outright. The policy setting can be one of three options:

- **None.** No action is taken on unauthenticated messages. The domain owner can still receive reports on how their domain is being used in email.
- **Quarantine.** Unauthenticated messages are marked as spam and sent to a junk folder. Recipients can review spam messages, but rarely do.
- **Reject.** Unauthenticated messages are blocked and bounced back to the sender. The intended recipient never sees them.



SECTION 3

Benefits of DMARC

DMARC offers many benefits for organizations that use email as a vital communication channel. Here are just a few.

Better email deliverability and engagement

By ensuring that only legitimate and authenticated emails from your domain reach the recipient's inbox, DMARC reduces the chances of your email being marked as spam or filtered out by email providers. This improves your email reputation and performance—increasing the likelihood of your email being opened, read and acted upon by your target audience.

This DMARC benefit is especially critical for transactional email. It ensures that your business isn't disrupted because of undelivered or deprioritized email.

Safer employees, business partners, consumers and brands

DMARC ends an entire class of fraudulent email before it reaches your employees, partners and customers. By preventing phishing and spoofing attacks that use your domain to trick or harm your stakeholders, DMARC enhances your brand trust and loyalty. It also reduces the risk of data breaches, financial losses and other legal issues.

Insight into the email threat landscape

You can't control what you can't see. DMARC gives you instant visibility into the threats targeting your company. In essence, it shines a light on domain phishing and spoofing attacks that put your customers and brand reputation at risk. By receiving regular reports on the sources and volumes of unauthenticated emails using your domain, you can identify and mitigate potential vulnerabilities and bad actors.

Reduced customer service costs

By blocking fraudulent emails that impersonate your domain, DMARC reduces the number of customer complaints, inquiries and disputes that you have to deal with. This saves you time and money on customer service operations and improves customer satisfaction and retention.

Lower phishing remediation costs

Phishing costs brands $6.9 billion in 2021, according to the FBI's Internet Crime Complaint Center (IC3).[3] DMARC reduces the spend on fraud, reimbursement and phishing remediation costs. By preventing BEC attacks that use spoofed email addresses to trick your employees or partners into transferring funds or disclosing sensitive information, DMARC saves you from the financial and reputational damage caused by these scams.

3 FBI. "Internet Crime Report 2021." April 2022.

SECTION 4

How to Ensure That Your Email Gets Delivered to Customers' Inbox

Many factors can affect whether your email lands in the inbox or the spam folder. But here's a list of minimum requirements to ensure that your business-critical email does not end up in the spam folder.

Have a DMARC policy in place.

By definition, this also requires having SPF or DKIM authentication methods implemented. To pass the DMARC check, your email's "From:" header must be aligned with either the SPF domain or the DKIM domain. (In other words, your header must match or share the same organizational domain.) Also, you must not impersonate Gmail in the "From:" header; any email that pretends to be from Gmail will automatically be marked as spam or rejected.

Ensure valid forward and reverse DNS records.

DNS records are used to map domain names to IP addresses and vice versa. Forward DNS records, such as A or CNAME records; resolve domain names to IP addresses; reverse DNS records, such as PTR records; and resolve IP addresses to domain names. Having valid forward and reverse DNS records helps email providers verify the identity and reputation of your email server to prevent spoofing and phishing attacks.

Keep reported spam rates reported below 0.3%

Gmail Postmaster Tools let you monitor and analyze your email performance and deliverability on Gmail. One of the metrics that the service reports is the spam rate, which is the percentage of your email that users mark as spam. Having a high spam rate can not only damage your email reputation but cause your email to be filtered out by Gmail. A report rate of 0.3% is the threshold for Gmail to consider email "spammy."

Ensure that the message format adheres to RFC 5322

RFC 5322 is a document that defines the standard format and syntax for email messages. It spells out the rules and conventions for the structure and content of email headers and bodies, such as the date, subject, sender, recipient and message-id fields.

Adhering to the RFC 5322 standard ensures that your email is compliant with the email protocols and can be properly processed and displayed by email providers and clients.

Provide one-click unsubscribe

To comply with the email marketing laws and regulations such as the CAN-SPAM Act or the GDPR, you must provide an easy and clear way for your subscribers to opt out or unsubscribe from your email list.

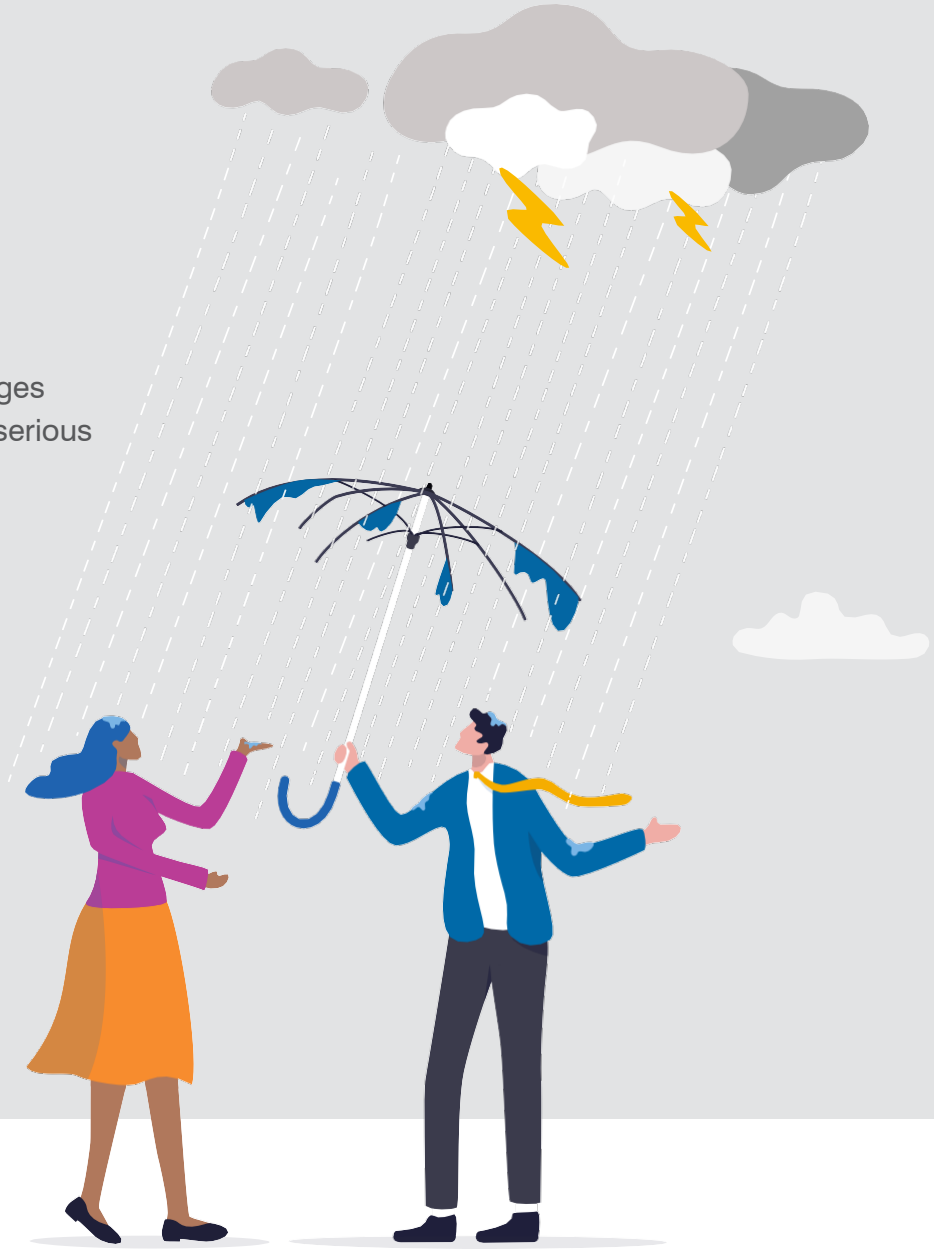
One of the best practices for this is to include a one-click unsubscribe link or button in your email footer, which allows your subscribers to unsubscribe from your email list without having to enter their email address or log in to your website. This not only respects your subscribers' preferences and privacy, but also reduces the chances of your email being marked as spam or reported as abuse.

SECTION 5

What Happens if You Don't Comply?

Email authentication is not only a matter of security, but also of business performance and customer satisfaction. If you don't meet the email authentication requirements set by Google and Yahoo, your email messages could be blocked or sent directly to the spam folder. And that could have serious consequences for your business.

Here are just a few of the potential business outcomes.



Your marketing becomes less effective

If your email campaigns are not authenticated, they could be filtered out by Gmail or Yahoo Mail. That means your target audience may never see your offers, news or content. The upshot: lower open rates, click-through rates, conversions and sales from your email marketing efforts.

Business disruption and loss

If your customers aren't receiving critical communications from you, they can't do business with you. They may not be able to log in, reset passwords, confirm orders, receive receipts or access support. That leads to confused, frustrated and unhappy customers. Many of them may abandon your services or switch to your competitors.

Reduced customer satisfaction and brand goodwill

Today's consumers expect follow-up emails, order confirmations, delivery notifications and more as a minimum level of customer service in the digital era.

If your email messages are not authenticated, they could be missed or ignored by your customers. People may perceive your brand as unprofessional, unreliable or untrustworthy. Any of these outcomes could damage your brand image and increase customer churn.

How Proofpoint Can Help

Meeting the new email authentication requirements can help bolster your digital marketing efforts, keep customers happy and protect your brand. Here are just a few of the ways Proofpoint can help you deploy DMARC to ensure that your business-critical emails reach customers and prospects.

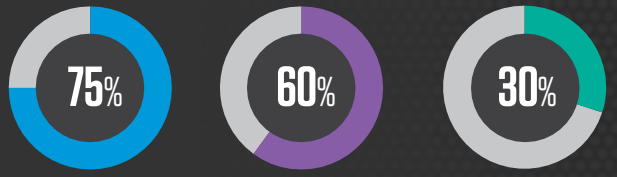
- **Proofpoint Email Fraud Defense (EFD)** provides access to highly experienced consultants who can guide you through each step of your DMARC journey, helping you to achieve optimal email deliverability and security.
- **Hosted SPF, Hosted DKIM and Hosted DMARC services** can streamline your configuration and maintenance to ensure that your email messages pass the authentication checks. These services can also help you overcome limitations such as the 10 DNS lookup limit for SPF or the key rotation requirement for DKIM.
- **Proofpoint Secure Email Relay** can ensure that transactional emails (those sent from applications or third-party partners on your behalf) are DKIM signed for faster DMARC alignment. This service can also provide you with granular visibility and control over your transactional email traffic to help identify and resolve any issues that may affect your email deliverability or performance.

Why Proofpoint

Every day, we analyze more than:

2.6B EMAILS	**49B** URLS	**1.9B** ATTACHMENTS
1.7B MOBILE MESSAGES	**430M** WEB DOMAINS	**143,000** SOCIAL MEDIA ACCOUNTS

We are trusted by more than:



OF THE FORTUNE 100 | OF THE FORTUNE 1000 | OF THE FORTUNE GLOBAL 2000

8,000 ENTERPRISES

200,000 SMALL BUSINESSES

LEARN MORE

For more information, visit proofpoint.com

ABOUT PROOFPOINT

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media and the web. More information is available at www.proofpoint.com.

proofpoint.