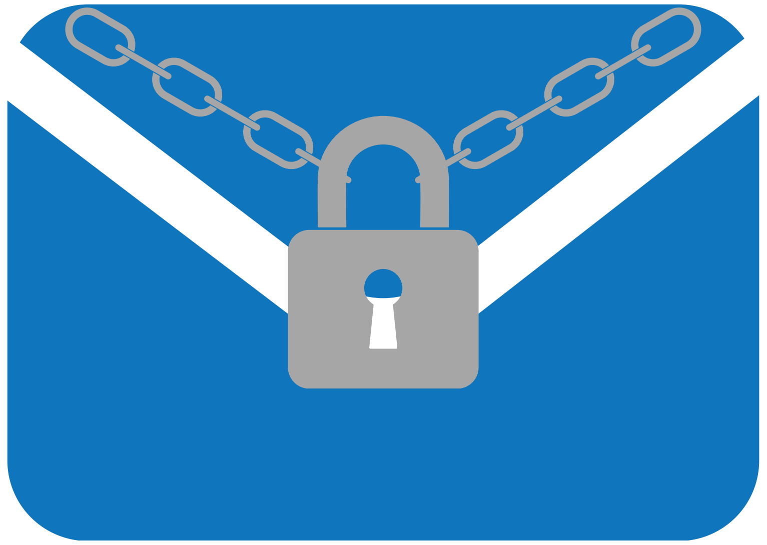
CORP INFO TECH / Guide
CORPORATE INFORMATION TECHNOLOGIES

DMARC

Ensuring Secure Email Authentication



WHAT IS DMARC AUTHENTICATION?

Email is an essential tool for communication that every organization uses to collaborate and share files or resources with peers across the country or even the world. Unfortunately, cyber criminals find this to be the easiest and most lucrative way to breach an organization.

Through the use of phishing and social engineering, threat actors will attempt to manipulate users into downloading a file or following a malicious link. To make their charade even more convincing, attackers will employ a tactic called “domain spoofing’ in which they use an organization’s domain to impersonate employees.

Domain-based Message Authentication Reporting & Conformance, or DMARC, is a security protocol that verifies the sender of an email and blocks domain spoofing attempts. As an email security protocol, DMARC builds off of the foundation of several other important security protocols including SPF, DKIM, and DNS.

Using these processes, DMARC is able to make decisions on how it should respond to incoming emails claiming to be from your domain.

CORP INFO TECH
CORPORATE INFORMATION TECHNOLOGIES

CORPORATE INFORMATION TECHNOLOGIES

Key Features of DMARC Authentication

DNS

Domain Name System

DNS is used to store SPF, DKIM, and DMARC records. These records ensure that emails originate from a legitimate source, mapping an email address to an IP address located within a DNS server.

DKIM

Domainkeys Identified Mail

DKIM provides a digital signature within the email header to prove authenticity. This signature also proves the message was not edited or tampered with during transit.

SPF

Sender Policy Framework

SPF provides a DNS record that states what IP addresses are permitted to send an email from a domain.

HOW DOES DMARC AUTHENTICATION WORK?

DMARC uses both SPF and DKIM as tests to determine whether or not an email is legitimate in relation to their email-sending domain. SPF verifies that an email comes from a legitimate domain by looking at the IP address. On the other hand, DKIM looks at the email's digital signature and verifies that is corresponds with the domain's public key. Once these checks are complete, DMARC decides whether or not the email is legitimate. If either fail, then the email will not be considered authenticated.

If an email is deemed unauthenticated, DMARC uses explicitly defined policies to determine where the email is sent. **One of three policies will take effect:**

- None - No action is taken toward the unauthenticated email.
- Quarantine - The email is either marked spam or sent to your junk folder. These emails are less likely to appear within your main inbox.
- Reject - The email is block/bounced and is sent back to the sender.

CORP INFO TECH
CORPORATE INFORMATION TECHNOLOGIES

Benefits of DMARC

1

Increased Email Delivery

DMARC helps authenticate your legitimate emails while filtering out illegitimate ones. This will help reduce the amount of time your emails spend in a junk folder or reported as spam.

2

Greater Security

By implementing DMARC, your employees, customers, and partners will benefit from greater security and protection from fraudulent emails.

3

Protect Your Reputation

Your organization can protect its reputation by preventing third parties or bad actors from spoofing your domain. This helps you look more trustworthy over email.

CORP INFO TECH
CORPORATE INFORMATION TECHNOLOGIES

WHY DMARC IS REQUIRED

Implementing DMARC authentication is not only highly recommended but for many organizations it is now a requirement. In the past several months, Gmail and Yahoo have begun requiring DMARC for senders that push out more than 5,000 emails a day. This change represents an effort to reduce spam and domain spoofing which in turn would protect users from online threat actors.

Gmail and Yahoo’s new email authentication requirements:

- You must have DMARC policies in place.
- Make sure that both SPF and DKIM are implemented.
- You must make it easy for users to unsubscribe from your emails.

CORP INFO TECH
CORPORATE INFORMATION TECHNOLOGIES

How Can CorpInfoTech Assist You?

A Trusted Partner

Corporate Information Technologies (CorpInfoTech) is a managed service provider (MSP) that offers IT and security solutions to SMBs. Our services equip businesses with the tools to protect their private data and secure their customers.

Through our services we can offer end to end email authentication and protection. We are able to configure the necessary email authentication protocols to prevent domain spoofing and provide email filtering services to prevent phishing and social engineering attempts.

Our Services Include...

- Firewall Management (xDEFENSE)
- Vulnerability Management (v360)
- Security/Risk Assessments
- Managed Compliance
- Managed IT

Contact Us

☎ 704-392-3031

✉ hello@corp-infotech.com

🌐 www.corp-infotech.com

in f X @corpinfotech

CORPORATE INFORMATION TECHNOLOGIES