Securing your email—by understanding DMARC and BIMI

These two email protocols help authenticate legitimate communications and prevent delivery of potentially malicious messages.

Due to the prevalence of business email compromise (BEC), phishing and spoofing, email remains one of the primary vectors for cyber crime. Many criminals are adept at creating messages that appear to come from legitimate email domains, which can trick recipients into thinking that they're opening an email from someone they know.

Domain-based Message Authentication, Reporting and Conformance, or DMARC, is a protocol designed to give email administrators greater visibility into who is using their email domains while simultaneously preventing potentially malicious emails from reaching the recipient's inbox.

Brand Indicators for Messaging Identification—BIMI—builds on the foundation of DMARC and enables an independently verified logo—which represents the domain owner's company or brand to be displayed in the consumer's inbox. BIMI can help protect senders' domains by making legitimate emails easier to recognize, while also promoting a brand.

Below are essential details about how DMARC and BIMI work, and how they may create more transparency in email systems while mitigating cyber crime.

→ How DMARC works

DMARC controls can **improve the effectiveness of email filters** by providing a clear path for determining an email's legitimacy.

DMARC relies on two underlying email authentication methods: DKIM (Domain Keys Identified Email) and SPF (Sender Policy Framework). **Email authentication systems should implement DKIM and SPF for DMARC to work efficiently.**

An email system will check SPF and DKIM on every piece of email that appears to originate from an organization's domain. **A message that fails SPF and DKIM can be quarantined or rejected based on the domain's DMARC policy.**

A DMARC record is published in the Domain Name System (DNS). Domain owners can then receive automated reports on messages attempting to leverage the domain. **This provides visibility into exactly who is sending emails—**possibly including legitimate senders whose emails may have been rejected by DMARC due to improper configuration. It also can help detect illegitimate emails.

Starting in February 2024, it is reported that major Email Service Providers[1] will begin **requiring DMARC compliance for all bulk email senders.**

→ DMARC benefits and challenges

Benefits

DMARC can help reduce the number of spoofing and phishing emails that avoid detection, thereby reducing the direct and indirect losses related to cyber crime.

Email recipients are in a **better position to trust emails** that come from an organization that applies DMARC, DKIM and SPF authentication.

DMARC can help organizations **detect legitimate emails that are misconfigured or experiencing authentication issues,** as well as emails that illegitimately use their domains.

The protocol helps establish a consistent policy for legitimizing email and **can enhance the trustworthiness of communication between partner organizations.**

Challenges

A domain's DMARC policy does not protect against spoofing or phishing emails that do not directly replicate a domain name. If an email's address varies by a single character- but still looks very much like a known sender's address - DMARC policy has no means to flag it. For example:

- DMARC reporting will register every email sent from the domain **xycorporation.org.**
- DMARC reporting will NOT register email sent from **xyZcorporation.org** (unless you also own that domain and apply DMARC)**.**

While DMARC can instruct recipients to quarantine or reject email that from a domain that is not authenticated, **implementing and monitoring DMARC requires some technical knowledge.** Some organizations may need outside expertise to adopt DMARC or properly scale the policies that prevent delivery of illegitimate emails. Resources for understanding DMARC's details and implementation process are available from the National Institute of Standards and Technology (NIST) and DMARC.org.

→ What BIMI does

BIMI **generates a company-defined, verified and authenticated logo** for every email that is validated by the DMARC protocol**.**

The logo appears next to the email in the recipient's inbox of participating email providers.

BIMI provides an additional layer of email authentication that **helps build users' trust** in the communications they receive.

By controlling the use of a distinctive logo, BIMI also **helps increase brand recognition** and marketing effectiveness.

→ How BIMI works

To use BIMI, email owners **must enable DMARC.**

The domain owner must set their DMARC policy to "quarantine" or "reject." With either protocol, any email associated with the domain that **fails DMARC authentication will be sent to spam or sent back as nondelivered mail.**

Organizations or brands create and trademark a logo image that will appear on every legitimate email associated with their domain.

✓ **An independent certification authority reviews the logo and issues a Verified Mark Certificate,** which acts as evidence that the logo belongs to a specific domain or organization.

When a recipient's email server receives a message, it is authenticated by the sender's DMARC system. The DNS name server of a DMARC authenticated message is then inspected for a BIMI record and, if one is found, the sender's logo will display in the recipient's inbox.

BIMI's value to cyber

While email domains are often spoofed by cyber criminals, the combination of DMARC and BIMI **makes any legitimate mail from a domain much easier to identify and trust.**

Since BIMI only operates within strict DMARC policies, **it has the added value of encouraging full DMARC adoption among organizations that deploy it.** Currently, most DMARC users set DMARC at a lower threshold that does not instruct recipients to quarantine or reject nonauthenticated messages. This threshold, known as monitor mode, is good for identifying mail leveraging a domain, but does not prevent or disrupt the delivery of unauthenticated messages.

While BIMI is often described in terms of its value to brand recognition and marketing objectives, **many organizations have recognized its potential contribution to a higher standard of email security** based on trust logos that are easy to view and be verified by the company.

To learn more

Information about BIMI implementation, logo verification requirements and issuers, how to generate reports, DMARC and other aspects of this emerging protocol can be found on the website of the BIMI working group: *bimigroup.org*

[1] https://blog.google/products/gmail/gmail-security-authentication-spam-protection/

IMPORTANT INFORMATION

Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC are members of the NFA.

Investment products offered by Investment Banking Affiliates:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value