Be cyber secure: automated protocols for email security

DMARC and BIMI can help authenticate legitimate communications and flag ones that have been compromised.

Below are essential details about how domain-based authentication reporting and conformance (DMARC) and brand indicators for message identification (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 must implement DKIM and SPF for DMARC to work efficiently.

An email system will run SPF and DKIM on every piece of email that appears to originate with an organization's domain. A message that passes SPF and DKIM will then receive DMARC authentication.

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. It also can help detect illegitimate emails.

How BIMI works

To use BIMI, email domain 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. This logo also appears next to the email in a recipient's inbox.

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

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 that the recipient's server reads, and the sender's logo will display in the recipient's inbox.

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

BIMI's value to cyber security

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 in 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*.

Visit www.business.bofa.com/managingfraudrisk to learn how to help protect yourself and those closest to you.

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" is the marketing name used by certain Global Banking and Global Markets businesses 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.