What is BIMI?

BIMI (Brand Indicators for Message Identification) Explained

Brand Indicators for Message Identification (BIMI) is a relatively new email authentication standard that aims to enhance email security and improve brand recognition in the inbox. BIMI allows organizations to display their brand logos and other identifiers alongside authenticated emails in the recipient's inbox. This is accomplished by associating a verified logo with the sender's domain through DNS records, which are then fetched and displayed by email clients that support BIMI. Some email providers or email apps also offer checkmarks or other visual "OK" type indicators on BIMI compliant emails.

One of the primary benefits of BIMI is its ability to increase brand visibility and recognition in the inbox. By displaying brand logos alongside authenticated emails, recipients can quickly identify emails from trusted senders and distinguish them from phishing attempts or fraudulent emails. This helps build trust between organizations and their customers while also reinforcing brand identity.

BIMI incentivizes organizations to adopt email authentication standards like **SPF, DKIM, and DMARC**, because BIMI requires these protocols to be implemented and properly configured. By encouraging widespread adoption of these authentication mechanisms, BIMI helps improve email security and reduce the prevalence of email spoofing and phishing attacks. BIMI can also have a positive impact on email engagement metrics. Research has shown that emails with recognizable brand logos are more likely to be opened and clicked by recipients. By prominently displaying brand logos or other visual indicators in the inbox, BIMI can attract the attention of recipients and increase the likelihood of engagement with marketing or promotional emails.

Here's how BIMI works within the DMARC framework:

1. **DMARC**: DMARC (Domain-based Message Authentication, Reporting, and Conformance) is an email authentication protocol that helps protect email senders and recipients from spam, spoofing, and phishing attacks. It allows domain owners to send instructions to a recipient mail server on how it should handle email delivery sent on behalf of their domain, and works in tandem with **SPF** and **DKIM**.
2. **BIMI Record**: In addition to SPF, DKIM, and DMARC records, organizations can publish a BIMI record in their DNS settings. This record contains information about the location of the organization's brand logo image and any additional specifications for displaying the logo.
3. **Email Authentication**: When an email is sent from a domain that has a BIMI record published, the receiving email server can verify the authenticity of the email using SPF, DKIM, and DMARC. If the email passes these authentication checks, the recipient's email client, app or web mail service may display the organization's brand logo alongside the email in the inbox.
4. **Improved Brand Visibility**: BIMI helps improve brand visibility and recognition by providing a visual indicator of authenticity alongside authenticated emails. This can help recipients quickly identify legitimate emails from trusted organizations and reduce the likelihood of falling victim to phishing attacks.

Overall, BIMI enhances email authentication efforts by providing an additional layer of visual verification, reinforcing the authenticity of authenticated emails and improving brand recognition for organizations. It also incentivizes and rewards domain owners by encouraging them to adopt a more rigorous email security policy.

For those seeking to deploy a full-blown **DMARC** (Domain-based Message Authentication, Reporting, and Conformance) policy combined with BIMI for their sending domains, the DMARC + BIMI compliance process does take some time and technical knowledge to achieve. BIMI is not available without several key components.

- BIMI relies on DMARC authentication. The domain must have a DMARC policy in place, and is typically required to be set to "**p=reject**".
- Since BIMI also relies on DMARC, this means that valid SPF and DKIM records also exist in the domain's DNS record. (SPF and DKIM are required for DMARC).
- BIMI requires a valid **VMC Certificate**. The certificate must be installed on the web server hosting the BIMI logo. This can be hosted on your current server, or most VMC vendors allow you to host it with them.
- The BIMI record itself. The domain must publish a BIMI record in the DNS of the domain. The BIMI record specifies the location of the brand's logo image and provides additional metadata related to the logo file.
- The BIMI logo needs to be a registered trademark. In the United States, it would be registered with the **USPTO**. Other regions would use their local registration authority to certify the trademark.

You can **learn more about how DMARC, BIMI, SPF and DKIM** work together as we have created an entire section that tackles these topics from start to finish within this knowledge base. GlowHost also offers Managed DMARC and Managed BIMI Services for those that would prefer a "done for you" hands-off DMARC + BIMI approach. Our managed service is also suitable for those organizations that prefer to entirely outsource or simply supplement their own IT department's management of their DMARC and BIMI policy. GlowHost's **Managed DMARC and Managed BIMI Service** combine experienced DMARC and BIMI technicians and advisors with a Software as a Service DMARC dashboard complete with graphs, robust reporting and BIMI management facility.

Related Topics:

- What is a VMC?
- DMARC, DKIM, SPF and BIMI Info
