



# You've Got Mail – Unless You Don't

Title: 20250507\_BIMI\_and\_DMARC/pdf  
Date: 7th May 2025 Version: 1.0



# You’ve Got Mail – Unless You Don’t (DMARC and BIMI: From Best Practice to Baseline)

Novalytics Gibraltar

**Abstract**—Recent enforcement actions by major email providers have shifted SPF, DKIM, and DMARC from recommended security measures to mandatory prerequisites for successful email delivery. At the same time, Brand Indicators for Message Identification (BIMI) has introduced a new layer of visual trust, allowing authenticated senders to display verified brand logos in recipients’ inboxes. This paper outlines the strategic importance of DMARC and BIMI not only as defences against spoofing and phishing, but as essential components for maintaining sender reputation, ensuring message visibility, and supporting brand integrity in modern email ecosystems. Drawing on current enforcement trends by Microsoft, Google, and Yahoo, it provides practical recommendations for organisations seeking to align their email infrastructure with emerging security and deliverability standards.

**Keywords**—email authentication, DMARC, BIMI, SPF, DKIM, Microsoft Outlook, Google Gmail, sender reputation, email deliverability, Verified Mark Certificate, phishing prevention, email branding

## 1. Introduction

Email remains a critical communication channel for organisations of all sizes, yet its continued utility depends on recipient trust and consistent deliverability. The last two years have seen major shifts in how leading mailbox providers handle bulk email traffic. These changes, spearheaded by Google, Yahoo, and most recently Microsoft, require strict enforcement of authentication protocols, specifically SPF, DKIM, and DMARC, as the foundation of modern sender reputation systems [3], [6], [7].

At the same time, the industry-wide adoption of Brand Indicators for Message Identification (BIMI) has transformed the display of the logo from a branding perk into a visibility asset [4]. BIMI builds upon DMARC compliance to provide a verified, standardised method for brands to display their logos in supported inboxes. When implemented correctly, BIMI signals legitimacy to users and inbox providers alike.

These developments are not just about best practice or defence-in-depth. As of May 20, 2025, Microsoft has begun routing non-compliant messages to the Junk folder for all Outlook.com, Hotmail.com, and Live.com addresses [7]. Google and Yahoo enacted similar enforcement in early 2024 [3], [6]. Failure to implement DMARC—and optionally BIMI—no longer means degraded deliverability: it increasingly means no deliverability at all.

This article outlines why DMARC and BIMI are now indispensable for bulk email senders, not just as security measures, but as prerequisites for being seen.

## 2. The New Baseline

Historically, email authentication protocols such as SPF and DKIM have been recommended as protective measures against phishing and spoofing. DMARC extended this framework by allowing domain owners to publish policies for handling unauthenticated mail. Until recently, the impact of failing to implement these standards was minimal for most legitimate senders [1].

This is no longer the case. In early 2024, Google and Yahoo began enforcing authentication at scale, requiring all high-volume senders (more than 5,000 emails per day) to implement SPF, DKIM, and DMARC. Microsoft followed suit with enforcement across its Outlook, Hotmail, and Live domains in May 2025 [7]. In practice, this means:

- Messages lacking SPF and DKIM authentication are more likely to be rejected or quarantined.
- Messages sent from domains without a DMARC policy are considered unauthenticated.

- Providers now require alignment between the visible “From” domain and the authenticated signing domains.

For organisations relying on mass communication, such as newsletters, transactional updates, or regulatory notices, this is a pivotal shift. Without proper authentication in place, even messages from legitimate sources may silently fail to reach the inbox.

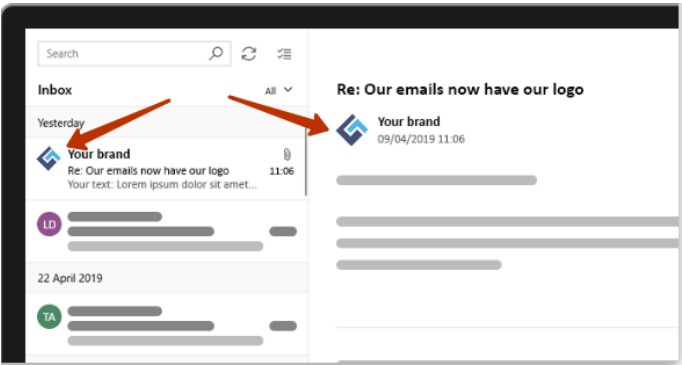
Crucially, a DMARC policy set to `p=none` is no longer sufficient to guarantee delivery. Google and Microsoft have both signaled that only enforcement policies (`p=quarantine` or `p=reject`) will be fully honoured for inbox placement and BIMI eligibility [3], [4].

This change effectively moves DMARC from a “should” to a “must”. The absence of a policy—or one configured incorrectly—places otherwise trusted communications in the same category as spam and phishing attempts.

## 3. BIMI: Security Meets Brand Visibility

Brand Indicators for Message Identification (BIMI) is a standard that leverages existing email authentication (specifically DMARC) to enable the display of verified brand logos in email clients that support it [4]. Though often discussed as a marketing enhancement, BIMI is fundamentally a security-linked visibility mechanism. Rewards properly authenticated email with increased prominence in the user interface.

So what does this mean? This means that when you get an email from someone, their respective logo is displayed within their email client, albeit Outlook, Gmail, Yahoo! or most other major provides. It means the customer knows it is from that established Brand (see Figure 1).



**Figure 1.** Example of BIMI in action: A verified brand logo is displayed next to authenticated email messages in the inbox and message pane, reinforcing brand trust and visual legitimacy.

At a technical level, BIMI relies on several components:

- A valid and enforced DMARC policy (`p=quarantine` or `p=reject`) with 100% alignment.
- An SVG Tiny PS version of the brand’s logo, hosted on an HTTPS-accessible endpoint.
- A published BIMI TXT record in DNS, referencing the logo and, optionally, a Verified Mark Certificate (VMC).

When configured correctly, email clients such as Gmail and Yahoo Mail display the sender’s logo alongside the message in the inbox. Microsoft Outlook has started limited support from 2025, with logo display contingent on the same authentication requirements [7].

Although the Verified Mark Certificate is not mandatory for all providers, it is currently required by Google and Microsoft for logo display in their clients. VMCs verify trademark ownership and prevent misuse of logos by unauthorised entities [5].

For users, this means clear visual cues about the authenticity of the message. For senders, the business case is equally compelling: increased open rates, reduced spoofing risk, and consistent brand representation across mailbox providers. In a crowded inbox, visibility is competitive real estate. BIMI, backed by robust DMARC enforcement, is the price of admission.

#### 4. The Cost of Inaction: Visibility, trust and delivery failure

Organisations that fail to implement DMARC and BIMI correctly now face tangible and measurable consequences. The days of deliverability being assumed are over; visibility in the inbox must now be earned through technical compliance and verified identity.

The first and most immediate consequence is the loss of inbox placement. Mail that does not pass authentication checks is routed to the Junk or Spam folder by default, or is silently rejected altogether. Microsoft's May 2025 enforcement milestone confirms this direction, with Outlook.com explicitly stating that unauthenticated bulk mail will be filtered or dropped [7]. Google and Yahoo have operated under similar rules since Q1 2024 [3], [6].

This has a knock-on effect on business operations. Transactional emails; password resets, purchase confirmations, regulatory updates may go unseen by users. Marketing and engagement campaigns may fail not because of content, but because recipients never receive the message. The volume of the help desk increases. User trust erodes. Revenue suffers.

In parallel, the absence of BIMI can signal a lack of legitimacy. In email clients that support it, BIMI adds a visual authentication layer. Messages without logos appear generic, less trustworthy, or even suspicious by comparison. Inboxes already use heuristics to prioritise familiar senders; BIMI enables the brand identity to function as part of that signal.

The damage compounds over time. Mailbox providers dynamically adjust the reputations of senders. High bounce rates, frequent spam reports, and unauthenticated messages feed into long-term reputation metrics. Reversing a damaged domain reputation is expensive and slow - often requiring changes to infrastructure, IP rotation, and rewarming of sender domains [2].

In summary, failure to act on authentication standards is no longer a passive oversight. It is an active decision to lose control over the delivery, branding, and reputation.

#### 5. Recommendations: What to Do Now

Organisations that rely on email for customer communication, security notifications, or operational updates must act decisively. The authentication landscape has shifted from advisory to mandatory, and compliance is now a condition of access to the major inbox providers.

The following steps are recommended for all high-volume senders:

- 1. Implement SPF and DKIM.** Publish valid SPF records to specify the IPs allowed to send. Configure DKIM to sign outbound messages with domain-aligned keys. Both are required for DMARC to function correctly [1].
- 2. Enforce DMARC.** Deploy a DMARC policy with either `p=quarantine` or `p=reject`, and ensure alignment 100% across all mail streams. Policies set to `p=none` are no longer honoured for BIMI or inbox trust [3], [7].
- 3. Monitor with DMARC Reports.** Use Aggregate (RUA) and Forensic (RUF) reports to track unauthenticated traffic and correct misconfigurations. This is essential before moving from monitoring to enforcement.
- 4. Prepare and Publish BIMI Records.** Create a square, SVG Tiny PS version of your brand logo. Host it over

HTTPS and reference it in a DNS TXT record under `default._bimi.yourdomain.com` [4].

- 5. Obtain a Verified Mark Certificate (VMC).** Acquire a VMC from a recognised certificate authority such as Entrust or DigiCert. A VMC is required for the display of BIMI in Gmail and Outlook [5].
- 6. Validate and Test.** Use BIMI inspection tools and DMARC analysers to validate the configuration. These tools help identify misalignments before enforcement begins.
- 7. Audit All Sending Domains.** Ensure all domains—whether used for marketing, transactional, or system email - are compliant. DMARC and BIMI must be configured across the entire mail ecosystem.

Compliance should not be viewed as a one-off project. DMARC and BIMI require ongoing operational oversight to remain effective, especially in organisations with multiple departments, vendors, or third-party mail platforms.

#### 6. Conclusion

The email ecosystem has undergone a structural redesign. What was once optional, DMARC enforcement and BIMI implementation, is now foundational. Mailbox providers have codified these standards into the delivery path, with non-compliance leading to reduced visibility, impaired deliverability, and long-term reputational damage.

This is not merely a security issue. It is a brand integrity and operational continuity issue. Messages that are unseen cannot inform, engage, or convert. Organisations that invest in correct authentication, robust policy enforcement, and visual branding via BIMI stand to benefit not only from improved inbox placement, but also from enhanced trust, user engagement, and reduced abuse.

'You've got mail' is no longer a certainty. But with DMARC and BIMI in place, your emails will be seen and trusted.

#### 7. Contact Novalytics for More Information

We work with small and medium enterprises, particularly those in regulated or high-risk sectors, to ensure that email systems are resilient against phishing, spoofing, and data leakage, and that marketing email platforms actually work.

Our expertise covers the implementation of standards such as SPF, DKIM, DMARC, and BIMI, as well as the design of a broader security architecture to support regulatory compliance, incident response, and operational continuity.

To discuss your organisation's email security posture, authentication strategy, or broader cybersecurity requirements, contact us at:

- Website: <https://www.novalytics.com>
- Email: [contact@novalytics.com](mailto:contact@novalytics.com)

#### References

- [1] DMARC.org, *Domain-based message authentication, reporting and conformance (dmarc)*, <https://dmarc.org/overview/>, Accessed: 2025-05-07, 2015.
- [2] M. I. Ashiq, W. Li, T. Fiebig, and T. Chung, *You've got report: Measurement and security implications of {dmarc} reporting*, 2023.
- [3] N. Kumaran, *New Gmail protections for a safer, less spammy inbox*, Oct. 2023. [Online]. Available: <https://blog.google/products/gmail/gmail-security-authentication-spam-protection>.
- [4] BIMI Group, *Bimi implementation guide*, <https://bimigroup.org/implementation-guide/>, Accessed: 2025-05-07, 2024.

- [5] Entrust Corporation and DigiCert, *Verified mark certificates for bimi*, <https://bimigroup.org/verified-mark-certificates/>, Accessed: 2025-05-07, 2024.
- [6] *Bulk Email FAQs*, [Online; accessed 7. May 2025], Apr. 2025. [Online]. Available: <https://senders.yahooinc.com/faqs/>.
- [7] Microsoft Corporation, *Outlook is changing how it filters bulk emails*, <https://www.okoone.com/spark/technology-innovation/outlook-is-changing-how-it-filters-bulk-emails/>, Accessed: 2025-05-07, 2025.



