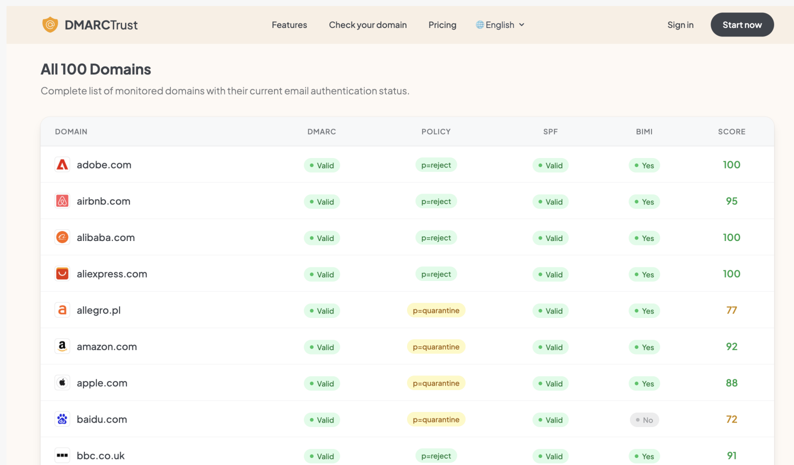
DMARCTrust Launches Live Email Security Tracker for America's Top 100 Websites

Leaderboard reveals 91% enforce DMARC, while major email providers use monitoring-only policies on consumer domains despite requiring enforcement from senders.



Top domains

HOUSTON, TX, UNITED STATES, January 13, 2026 /EINPresswire.com/ -- DMARCTrust today launched a live tracker analyzing the DMARC adoption status of the 100 most visited websites in the United States, revealing strong overall progress, but also notable inconsistencies among the world's largest email providers, including consumer email domains operated by both Microsoft and Google.

The findings follow a series of industry-wide policy changes. In 2024, Google and Yahoo mandated DMARC authentication for high-volume senders. In May 2025, Microsoft introduced similar requirements for all senders delivering email to Outlook.com, Hotmail.com, and Live.com.

> It is time to close this loophole and raise the security standard for every email user in the United States."
>
> *Marc Lelu*

The live tracker reveals a striking pattern: while major email providers strictly protect their corporate domains, they continue to apply monitoring-only DMARC policies to their consumer email domains (including gmail.com, live.com, and msn.com).

"When Google, Yahoo, and Microsoft announced their DMARC mandates, the industry responded quickly and decisively," said a DMARCTrust spokesperson. "But it is paradoxical that the same companies enforce strict protection for their enterprise domains while still using p=none on consumer email platforms used by hundreds of millions of people."

Key findings

DMARCTrust analyzed the DMARC and SPF configurations of 100 of the most-visited U.S. websites. The results paint a picture of an industry that has made significant progress, with notable exceptions. Overall Enforcement Rate: 91%

- 70 websites enforce the strictest policy (p=reject)
- 21 websites use partial enforcement (p=quarantine)
- 9 websites use monitoring-only policies (p=none)

Why this matters

DMARC is currently the most effective industry standard for preventing attackers from sending fraudulent emails that impersonate legitimate brands.
Domains configured with p=none merely collect reports about abuse but do not instruct receiving mail systems to block or quarantine forged messages. As a result, attackers can still send emails that appear to originate from these brands, increasing the risk of phishing, fraud, and malware distribution.

In contrast, domains using p=reject or p=quarantine enable automatic blocking or isolation of unauthorized messages. A DMARC policy of p=none means receiving mail servers are instructed to deliver messages even when authentication fails.

For users, the difference is simple: some brands block fake emails pretending to come from them, while others still allow those messages to reach people’s inboxes.

Major providers: Enterprise vs. Consumer domain policies

DMARCTrust’s analysis reveals a consistent pattern among major email providers: strict enforcement on enterprise domains and monitoring-only policies on consumer email domains.

Both Google and Microsoft follow the same approach:
- Enterprise domains (google.com, microsoft.com): p=reject, full enforcement
- Consumer email domains (gmail.com, live.com, msn.com): p=none with sp=quarantine for subdomains

This technical choice may be related to email forwarding. However, it also means that an address from these services could be spoofed to send fraudulent emails to other domains. It is time to close this loophole and raise the security standard for every email user in the United States.

Marc Lelu

DMARCTrust.com
+1 281-832-3696
press@dmarctrust.com
Visit us on social media:
LinkedIn
X
