warmy
Email Channel. Reliable.

February 2025

DNS Record Impact on Email Deliverability

This research explores how DNS records—particularly SPF, DKIM, and DMARC—affect email deliverability across diverse domains.

We examined both newly registered and established domains, assessing whether correctly configured DNS records translate to higher inbox placement rates. Additionally, we investigated how email template types (HTML vs. text-based) influence the likelihood of messages being flagged as spam.

About Warmy and the Research Team

Warmy is the leading email deliverability technology, helping businesses improve their inbox placement, sender reputation, and overall email performance. Powered by AI-driven strategies.

The Warmy Research Team is a dedicated group of email deliverability-certified experts focused on analyzing and optimizing email-sending practices.

Through continuous testing, data-driven insights, and innovative methodologies, they uncover factors that impact deliverability and translate findings into actionable improvements for Warmy's platform. Their expertise helps businesses navigate the complexities of email deliverability with confidence.

Daniel Shnaider

Deliverability Expert

Alexandr Panchenko

Technical Deliverability Expert

Vahagn Shirinyan

Senior Deliverability Expert

Oleksiy Lutskin

Deliverability Expert

Bohdan Tsapenko

Head of Research Team

warmy

The Warmy.io team

Key findings

- **DMARC** is the most critical record for maximizing inbox rates. Misconfigured or absent DMARC policies often lead to higher spam classification.
- **DKIM** provides essential authentication, but requires alignment with DMARC for full effectiveness.
- **SPF** is beneficial but offers limited impact in isolation; it is best combined with DKIM and DMARC.
- **Newly registered domains,** even when configured, tend to face more scrutiny from email service providers, resulting in lower initial inbox rates.
- **Text-based emails** typically outperform HTML emails, especially in stricter filtering environments such as MS365 and Outlook.

Research Technical Details

- **Data Sources:** The study utilized four distinct datasets, each representing different domain configurations and ages:
    - **New Domains (Configured DNS)** – Domains with correctly set SPF, DKIM, and DMARC.
    - **New Domains (Misconfigured DNS)** – Domains with partial or incorrect DNS configurations.
    - **Old Domains (Configured DNS)** – Older domains with properly configured DNS records.
    - **Old Domains (Misconfigured DNS)** – Older domains with misconfigurations in SPF, DKIM, or DMARC.

Each dataset captured real-world email-sending scenarios to multiple providers, including Google, Gsuite, Outlook, MS365, Zoho, and SMTP. The sender mailboxes were exclusively Gsuite.

- **Data Entries:** Included fields for domain name, DNS record status (SPF, DKIM, DMARC), sender/receiver info, email template type, and average inbox/spam rates.

- **Tools & Analysis:**
    - Aggregated data to compare configured vs. misconfigured DNS outcomes.
    - Correlation analysis to determine the relative influence of SPF, DKIM, and DMARC.
    - Chart visualizations (bar charts, scatter plots) to illustrate trends in deliverability and DNS record configurations.

Methodology

- **Domain Categorization**
  - **New Domains (Configured vs. Misconfigured) and Old Domains (Configured vs. Misconfigured)** were selected to represent varying reputations and DNS setups.

- **Email Dispatch**
  - A series of emails (ranging from 5 to 15 per test batch) was sent from each domain category to multiple providers.
  - Template Types included HTML, text-based, and variations marked as “spam” or “inbox” to gauge filter sensitivity.

- **DNS Validation**
  - **SPF, DKIM, and DMARC** settings were verified for each domain, noting any mismatches between recorded and expected configurations.

- **Data Collection & Analysis**
  - Inbox vs. Spam outcomes were aggregated per domain, per provider, and per template type.
  - Charts and correlation analyses were used to identify which DNS record or template format best predicted inbox success.

Results

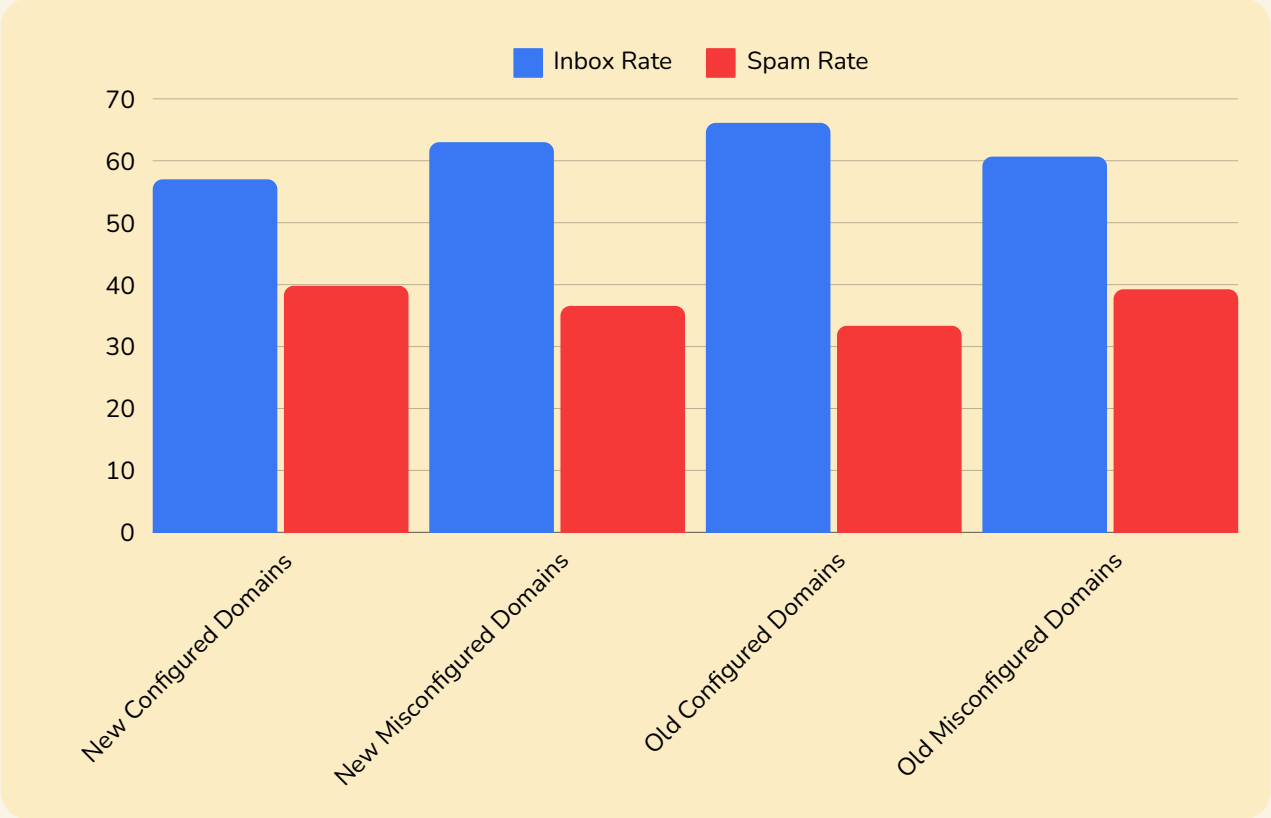
- **DNS Configurations**
  - **Properly configured SPF, DKIM, and DMARC** domains typically achieved 70%+ inbox rates.
  - **Misconfigured domains** frequently saw spam rates above 50%, with DMARC misalignment causing the steepest drop.
  - **New configured domains** showed lower deliverability despite correct DNS records, suggesting heightened scrutiny for newly registered domains.

- **Template Types**
  - **Text-based emails** consistently outperformed HTML.
  - **MS365/Outlook** displayed the most stringent filtering, while Yahoo also frequently flagged misconfigured domains as spam.

- **Provider-Specific Observations**
  - **Gsuite/Gmail:** More lenient when it comes to various template types, but still penalizes absent DMARC.
  - **MS365:** Prefers text-based emails; DNS misconfigurations lead to substantial spam placement.
  - **Outlook:** Often flags HTML content as spam unless DNS is fully aligned.

Below are the charts presented from some of the control/focus groups.

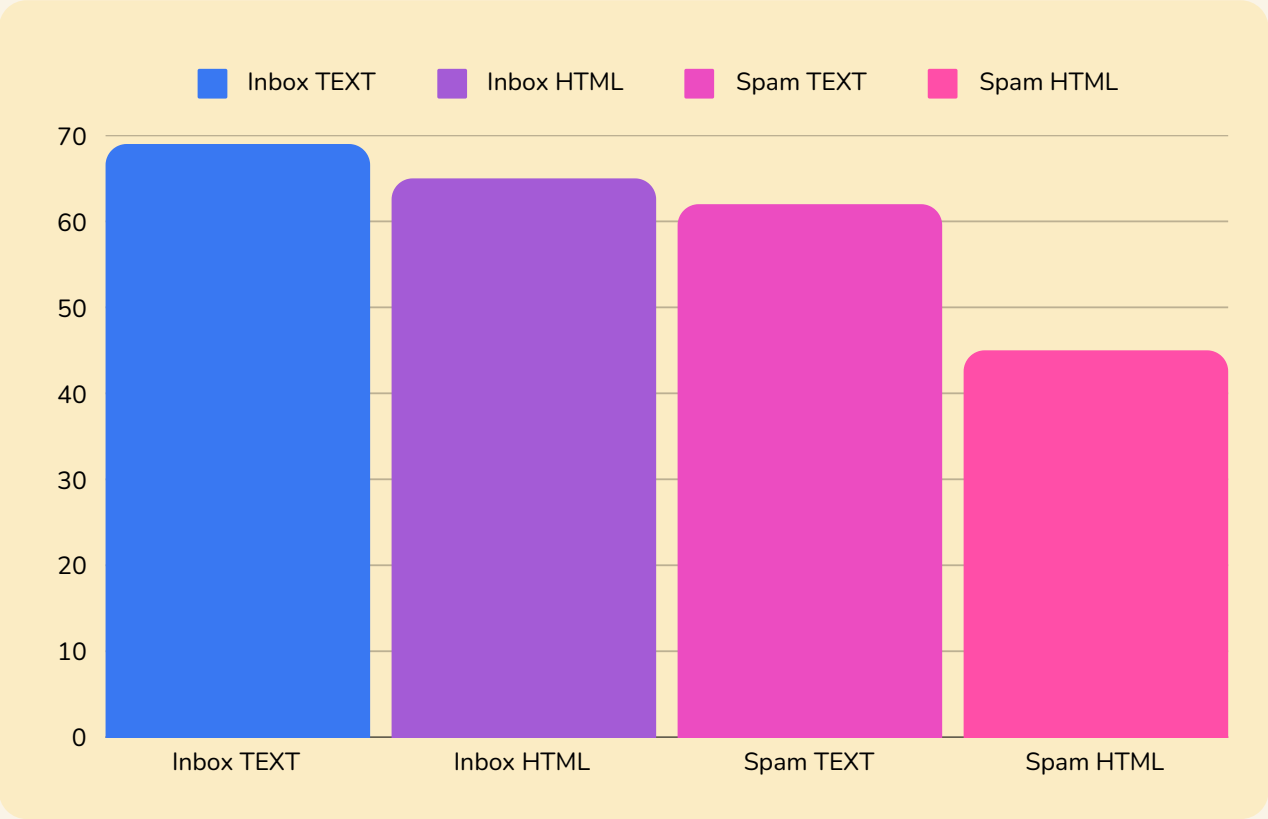
Inbox Rate Comparison Between Configured and Misconfigured DNS Domains



The chart reflects how DNS configurations and domain age influence deliverability. Configured domains, especially older ones, show higher inbox rates, while new or misconfigured domains struggle, often landing in spam.

Misconfigured DNS settings, particularly missing or weak DMARC policies, contribute to increased spam classification. Additionally, text-based emails tend to perform better than HTML emails, particularly with providers like MS365 and Outlook.

Inbox Rate Comparison Between Text and HTML Email Templates



The chart illustrates the impact of email template type on deliverability, aligning with the research findings. Text-based emails have the highest inbox rate, with Inbox TEXT leading, followed closely by Inbox HTML. However, HTML emails see a slightly lower inbox rate, which reflects the study's conclusion that providers like MS365 and Outlook prefer text-based emails.

Spam rates also show a clear pattern: Spam TEXT has a higher inbox rate than Spam HTML, reinforcing the idea that HTML-based emails are more likely to be filtered as spam. This aligns with the research, which found that HTML emails, especially from misconfigured domains, tend to struggle with deliverability.

Overall, the findings confirm that proper DNS configurations improve inbox placement, but email content type remains a critical factor. Text-based emails consistently outperform HTML emails, making them a more reliable choice, especially when sending from newer domains or to stricter providers like MS365 and Outlook.

Conclusion

Proper DNS record configuration (SPF, DKIM, DMARC) is central to achieving high email deliverability.

Among these, DMARC is the most influential; without it, even valid SPF and DKIM may not prevent spam filtering.

New domains, despite correct records, remain under heightened scrutiny, emphasizing the need for ongoing domain warming and reputation building.

Finally, plain-text emails consistently show stronger performance, particularly under strict filtering conditions.

For maximum effectiveness, organizations should keep all DNS records current, enforce stricter DMARC policies (quarantine or reject) after a warm-up period, and favor simpler email formats to reduce the likelihood of being flagged as spam.

Auto All-In-One Tool For Email Deliverability To Make Your Email Channel Reliable

We are passionate about solving email deliverability challenges and making email a reliable channel for every business

325+
Years Of Combined Email Deliverability Expertise

9 countries
Home To Our Talented Team

95+
Countries Have Daily Active Users In Warmy