How Your “From” Address Affects Email Deliverability

Last Modified on 10/09/2025 1:20 pm MST

This article applies to:

Max Classic

The email address you send from — known as your **“From” address** — plays a critical role in whether your messages are delivered successfully or rejected by mailbox providers.

Using a **free, public domain email address** (like Gmail, Yahoo, AOL, or Outlook.com) when sending through Keap or any other email marketing platform can cause your emails to **bounce, go to spam, or be rejected outright**.

This issue is not unique to Keap — it affects all senders who use third-party email systems.

Why Free Email Addresses Cause Deliverability Issues

Mailbox providers (like Gmail, Yahoo, and Microsoft) have implemented strict **DMARC** policies to protect their users from phishing and spoofing.

DMARC (Domain-based Message Authentication, Reporting & Conformance) allows domain owners to tell receiving mail servers what to do if an email fails authentication (for example, reject or quarantine it).

Free email services such as **Gmail**, **Yahoo**, and **AOL** publish DMARC policies that **reject emails sent from their domains unless sent directly through their own servers**.

Example:

If you send an email through Keap using `yourname@yahoo.com`, that message appears to come “from” Yahoo — but it’s actually being sent by Keap’s servers.
Since Keap isn’t authorized to send on behalf of Yahoo, the receiving mail server will reject it based on Yahoo’s DMARC policy.

Keap Policy on “From” Addresses

To ensure compliance with current authentication standards and maintain strong deliverability across all major mailbox providers, **Keap does not allow users to send email from free, public domain addresses** (such as Gmail, Yahoo, AOL, or Outlook.com).

All email sent through Keap must use a **custom or personal domain that you own and can manage** — meaning you must have the ability to add DNS records for authentication (SPF, DKIM, and DMARC).

Using a managed domain ensures that:

- You can verify ownership of your sending domain.

- Keap can authenticate your emails correctly.
- Your messages comply with modern DMARC enforcement policies.
- You build and maintain your own sender reputation over time.

Updated Bulk Sender Requirements (2024–2025)

Starting in 2024, **Google (Gmail)**, **Yahoo Inc.**, and **Microsoft (Outlook/Hotmail)** implemented new requirements for bulk senders (those sending 5,000+ emails per day to their domains).

Even if you send below that volume, following these best practices is critical for consistent inbox placement.

All senders must:

- **Send from a custom domain you own and control** — not from a free email service.
- **Authenticate** all outgoing email with **SPF**, **DKIM**, and **DMARC**.
- **Publish a valid DMARC record** aligned with your domain.
- **Include a visible one-click unsubscribe link** and honor opt-outs within two days.
- **Maintain a complaint rate below 0.3%** to preserve reputation and deliverability.

How to Fix “From” Address Rejections

Use a Custom Business Domain

The best practice — and Keap’s requirement — is to send from a **custom business domain**, for example:

- `alex@greenmarketing.com`
- `alex@gmail.com`

If you don’t have a domain yet, you can purchase one through registrars like Google Domains, GoDaddy, or Namecheap, then create a business email address associated with it.

Learn how to create a custom business email for Gmail Here

Set Up Domain Authentication

To ensure successful delivery and compliance with DMARC enforcement, your domain must be properly authenticated:

- **SPF (Sender Policy Framework):** Authorizes which servers can send mail for your domain.
- **DKIM (DomainKeys Identified Mail):** Confirms that the message hasn’t been altered and is sent from an authorized source.
- **DMARC:** Instructs receiving servers how to handle messages that fail SPF or DKIM checks.

Learn more: Setting up DKIM for your domain

Key Takeaways

- Keap **does not allow sending from free email domains** such as Gmail, Yahoo, AOL, or Outlook.com.
- You must use a **custom or personal domain** that you control and can manage DNS records for.
- Authenticate your domain with **SPF**, **DKIM**, and **DMARC** to meet deliverability and compliance requirements.
- Adhering to **Google**, **Yahoo**, **and Microsoft's bulk sender requirements** ensures inbox placement and strong sender reputation.

Looking for extra help?

If you'd like professional guidance with your email practices or recommended tools to improve your email practices and deliverability, check out these trusted partners:

- **Email Deliverability specialist training, consulting and software**
  - **EmailSmart**
- **List Cleaning**
  - **SpamClean**
  - **ListDefender**
  - **Klean13**
  - **EmailSmart Pro Tools**
- **Form Security**
  - **Spamkill**
  - **ListDefender**