User Guide: Email Delivery Optimizer (Web UI)

Harsh

July 15, 2025

Purpose

This guide walks users through using the Email Delivery Optimizer Web App to:

- Diagnose SPF, DKIM, and DMARC for any domain
- Compose and send emails with Gmail (App Passwords)
- Analyze inbound email headers for delivery/authentication issues

1 Getting Started

1.1 1. Setup Your Info

Navigate to `/setup` or click **Change Setup** on the homepage. Enter:

- Your domain name (e.g., `example.com`)
- DKIM selector (e.g., `default`, `20230601`)
- Gmail address (e.g., `you@gmail.com`)
- Gmail App Password (16-digit token from Google App Passwords)

1.2 2. Diagnose Domain

From homepage `/`, enter:

- Your domain
- DKIM selector

Then click **Run Checks**. The tool shows:

- **SPF Record** with pass/fail status
- **DKIM Record** value (if found)
- **DMARC Record** policy and report destination

1.3 3. Send Travel Email

Go to `/email`. Fill in:

- Sender Gmail + App Password
- Customer Name, Itinerary, Price
- Recipient Email + Subject

Click **Send Email** to generate and send. A preview appears below.

1.4 4. Analyze Received Emails

From `/analyze`:

- Input Gmail + App Password
- Provide subject line of received email

Output includes:

- SPF/DKIM/DMARC results
- Authentication headers
- Common issues and color-coded statuses

2 What the Results Mean

- **SPF**: Verifies if your domain's email was sent by an authorized server.
- **DKIM**: Validates message integrity and authenticity.
- **DMARC**: Tells receivers how to handle SPF/DKIM failures.
- **App Password**: Used to allow secure SMTP/IMAP access.

3 Security Notes

- Credentials are never stored server-side
- Session data is in-memory and flushed on browser close
- HTTPS should be used when deployed publicly

4 Credits

Developed by Harsh. GitHub repo: github.com/harsh-91/e-mail_optimizer.git