# **Web UI Walkthrough: Email Delivery Optimizer**

## **Purpose**

This guide is for users interacting with the **Web Interface** of the Email Delivery Optimizer. It explains what each section of the app does and **why** it's important for your email deliverability and security.

## **Accessing the Web App**

Launch the app by running:  
  
 python run.py

Open a browser and navigate to:  
  
 http://localhost:5000

## **Home Page (/)**

### **What You See:**

* Input for your **domain** (e.g., example.com)
* Input for your **DKIM selector** (e.g., default, 20230601)
* Button to **Run Diagnosis**

### **What It Does:**

* Fetches and displays:  
  + **SPF Record**: Shows who can send emails from your domain
  + **DKIM Record**: Verifies email integrity and authenticity
  + **DMARC Record**: Tells inboxes how to handle unauthenticated mail

### **Why It Matters:**

* Helps prevent your emails from going to spam
* Avoids your domain being spoofed by scammers
* Improves sender reputation and delivery rates

## **Send Email Page (/email)**

### **What You See:**

* Input fields:  
  + Your **Gmail address** and **App Password**
  + Recipient email
  + Subject, Itinerary, Price, Name
* Submit button

### **What It Does:**

* Builds a visually branded HTML email using your input
* Authenticates using Gmail’s SMTP with App Password
* Sends the email to the recipient securely

### **Why It Matters:**

* Ensures travel itineraries, invoices, or important docs are delivered cleanly
* Avoids formatting or spam filter issues caused by plain text

## **Analyze Email Page (/analyze)**

### **What You See:**

* Input fields:  
  + Your **Gmail address** and **App Password**
  + Optional: Subject filter for finding specific email

### **What It Does:**

* Connects to your inbox securely (IMAP)
* Retrieves headers of the latest matching email
* Parses:  
  + SPF pass/fail result
  + DKIM-Signature status
  + DMARC policy outcomes

### **Why It Matters:**

* Lets you check if a real-world email was delivered securely
* Helps debug why an email might have landed in spam
* Useful for testing sent emails or replies

## **Instructions Sidebar (Visible on All Pages)**

The app provides inline definitions and examples:

* SPF: “Who can send on behalf of your domain”
* DKIM: “Digital signature added to outgoing mail”
* DMARC: “Tells inboxes what to do when SPF/DKIM fails”
* App Password: “Generated from your Gmail settings → Security → App Passwords”

## **Security Tips**

* Never reuse passwords. Only use App Passwords.
* Data is not stored. It’s used only for real-time analysis.
* Your credentials are not saved anywhere.

## **Final Recommendations**

* Always verify your domain’s SPF/DKIM/DMARC setup after DNS changes
* Send yourself a test email, then analyze it using the tool
* Share screenshots with your domain/email provider if you find issues

Need help? open a GitHub issue.