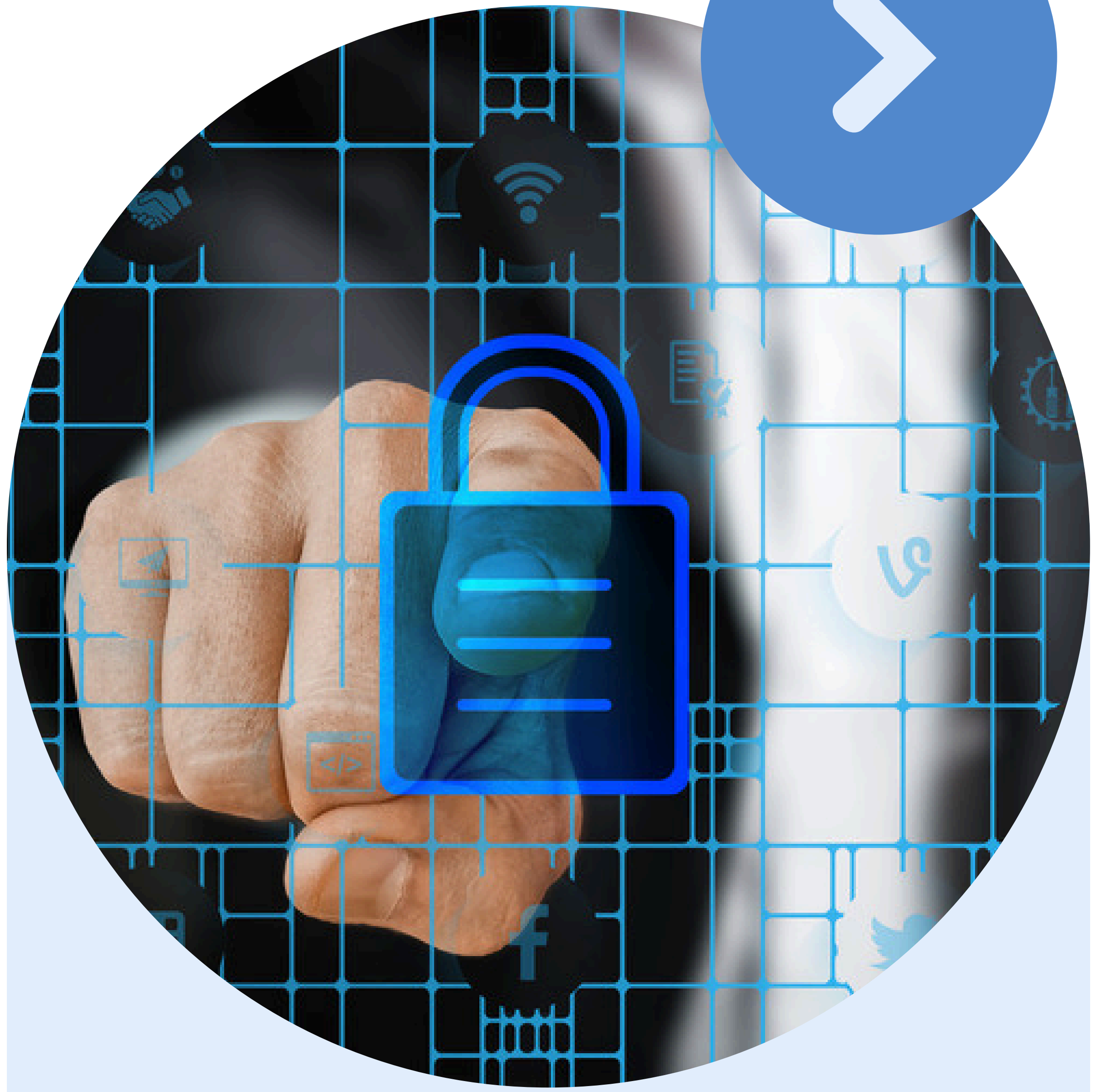
FILE GUARD

FILE GUARD

Safeguarding Gmail Transfers with Seamless Protection



Introduction

FileGuard aims to develop a lightweight, user-friendly extension that ensures the safety of files shared via Gmail. The tool will automatically validate files to detect any potential malware, viruses, or harmful content without requiring manual uploads or downloads.

FILE GUARD

How Does the Tool Work?

Email Received

A user receives an email with an attachment in Gmail.

Attachment Detected

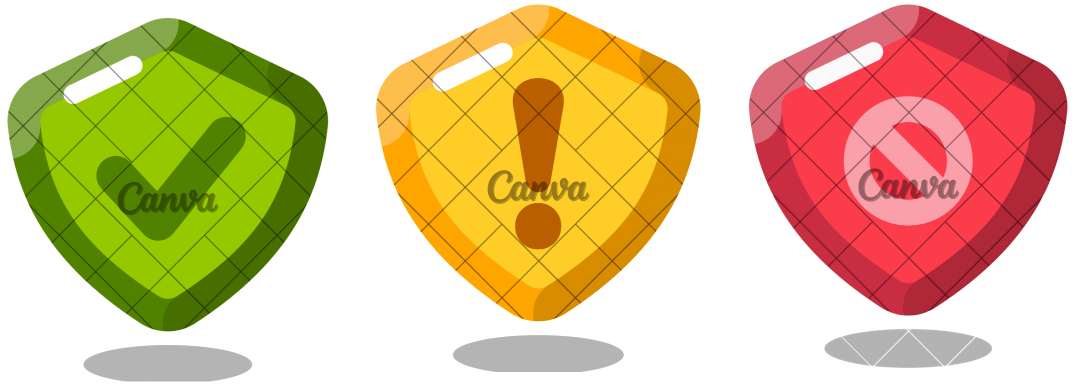
The tool automatically identifies that the email has an attachment. A "Scan File" button appears next to the attachment.

Scanning

The user clicks the "Scan File" button without downloading the file.

File is Analysed

The tool sends the file to a secure scanning system (e.g., VirusTotal API). It checks the file against databases of known viruses and malware.



Scan Results Displayed

The tool shows the user a report:

- SAFE: The file has no threats and is safe to download.
- MALICIOUS: The file contains harmful content and should not be downloaded.
- UNCERTAIN: The tool couldn’t determine if the file is safe (rare cases).

User Action

Based on the results, the user decides whether to download the file or ignore it.

PROCEDURE

Folder Creation

Create a folder called gmail_file_scanner.

VirusTotal API Key

Get VirusTotal API Key by creating a free account in VirusTotal. THis API key will authenticate the request.

Interaction with API

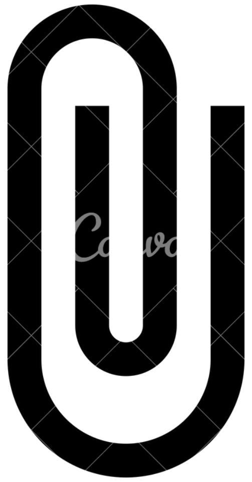
Create code to interact with VirusTotal API to scan file.

Setup Gmail API

Gmail API is needed to access gmail in the program

Authenticate and Authorize Gmail Access

OAuth 2.0 is an industry-standard protocol for authorization. With OAuth 2.0, file guard can request access to a user’s Gmail account without needing their credentials.

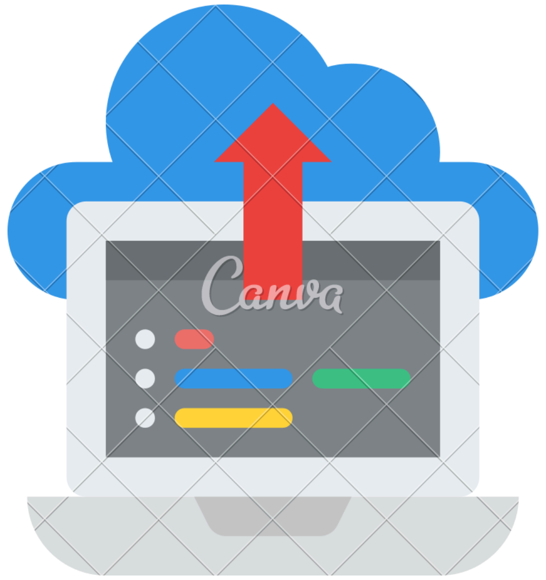


Access Emails and Attachments

Use the Gmail API to retrieve emails and attachment metadata.

Implement the "Scan" Button

Use a browser extension to add a "Scan" button next to email attachments in Gmail. This extension will send the attachment metadata or ID to your backend service when clicked.

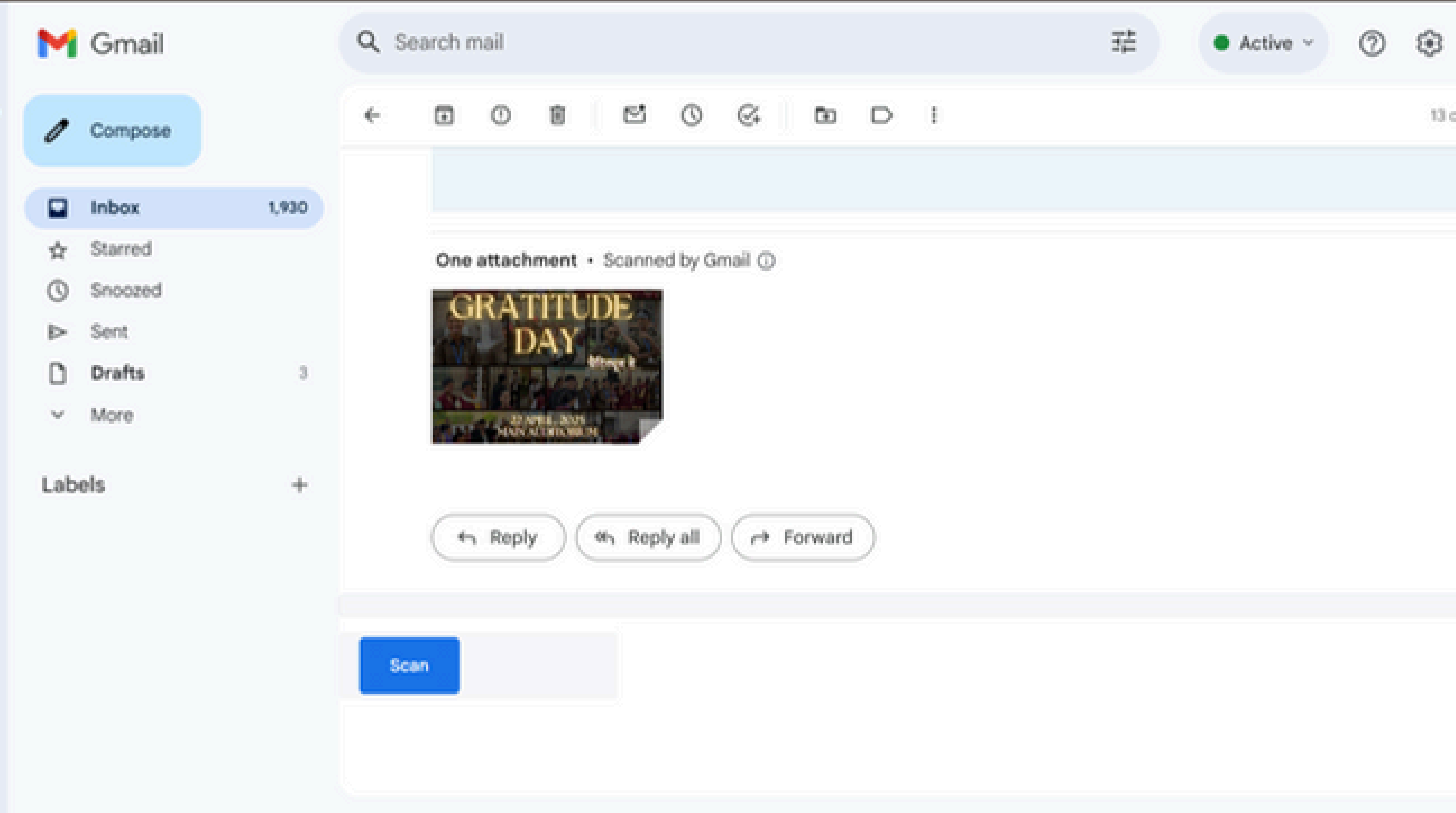


Deployment

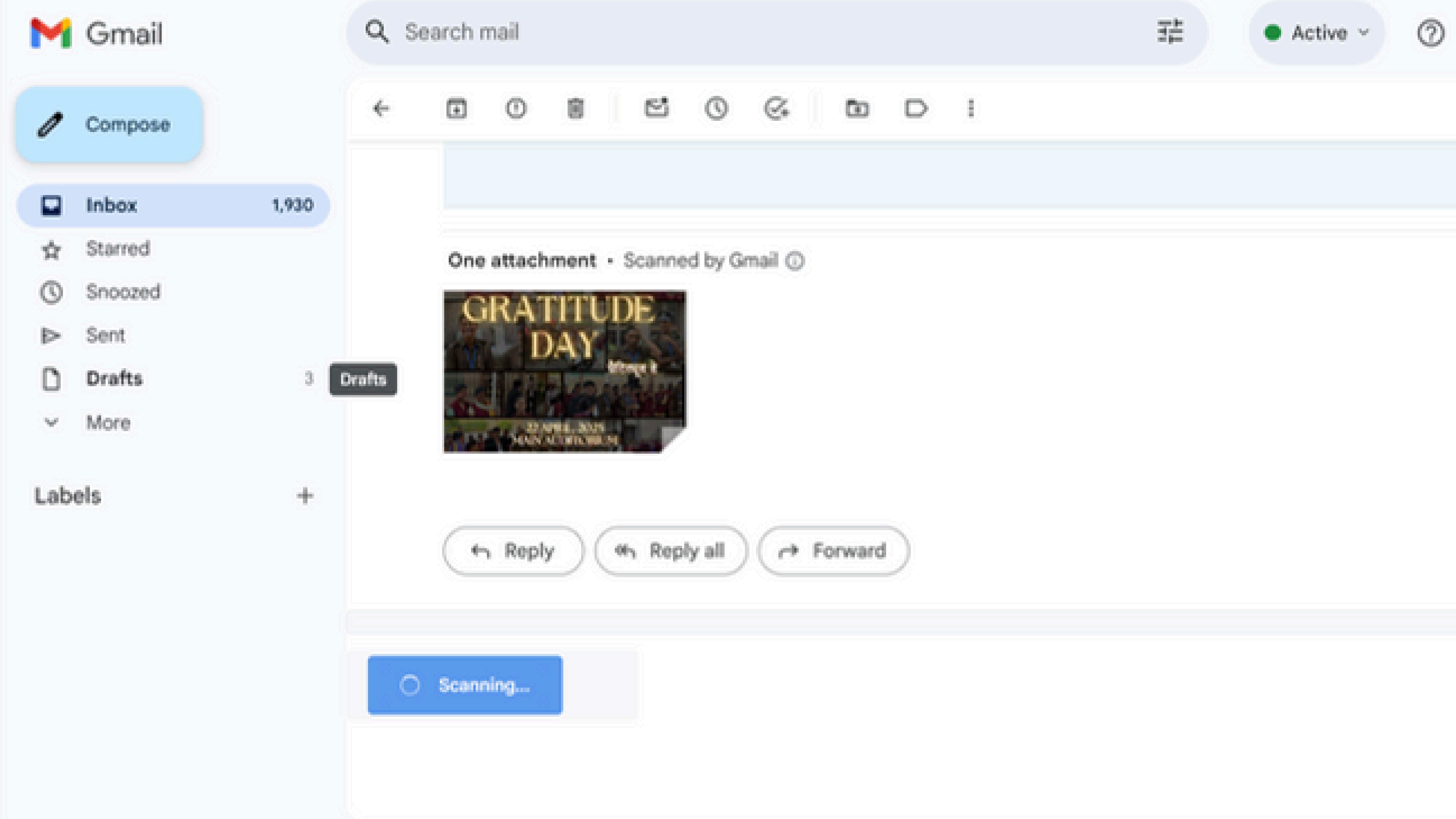
Package and submit it to the Chrome Web Store.

FILE GUARD

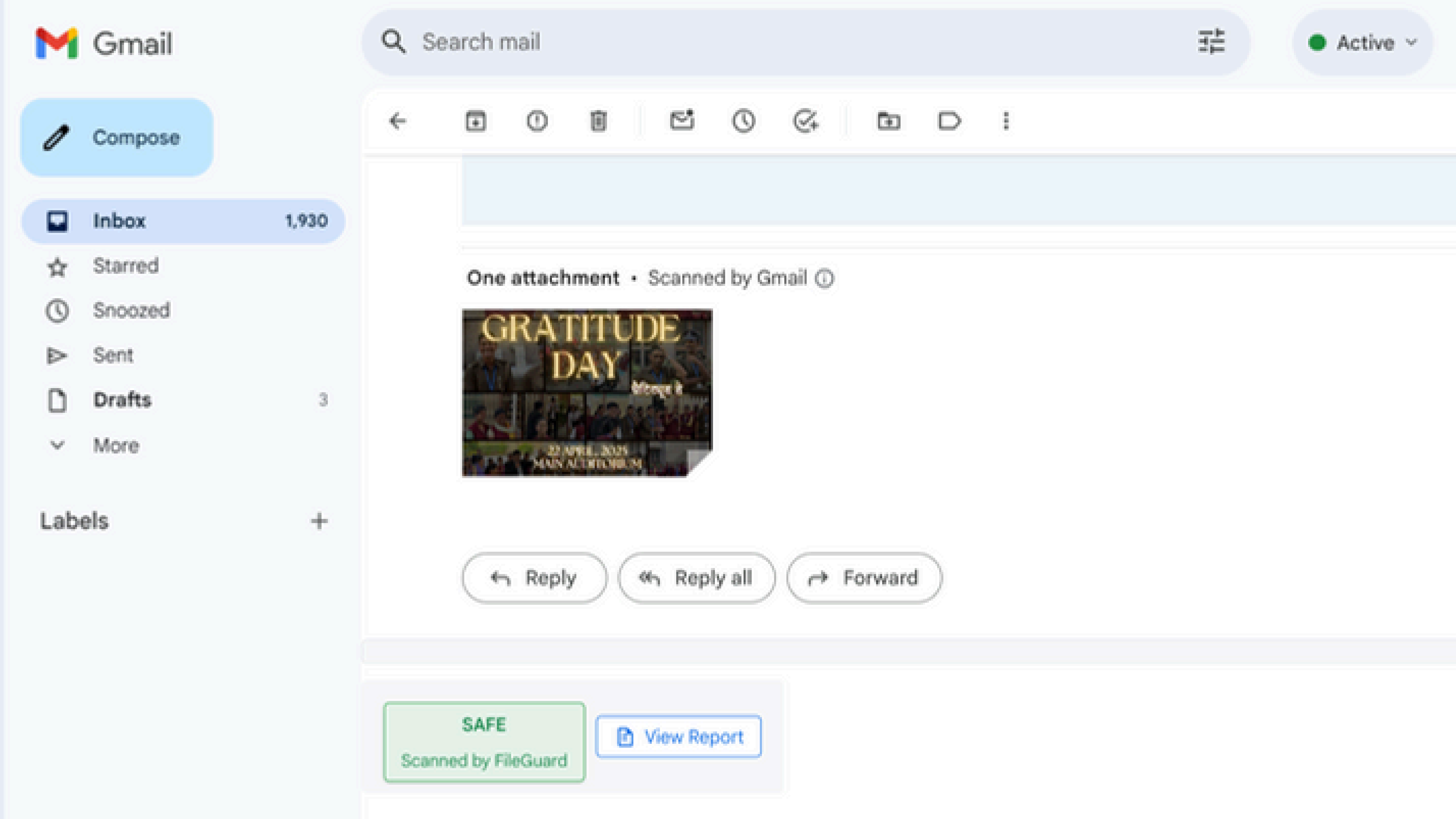
FILE GUARD



One attachment • Scanned by Gmail



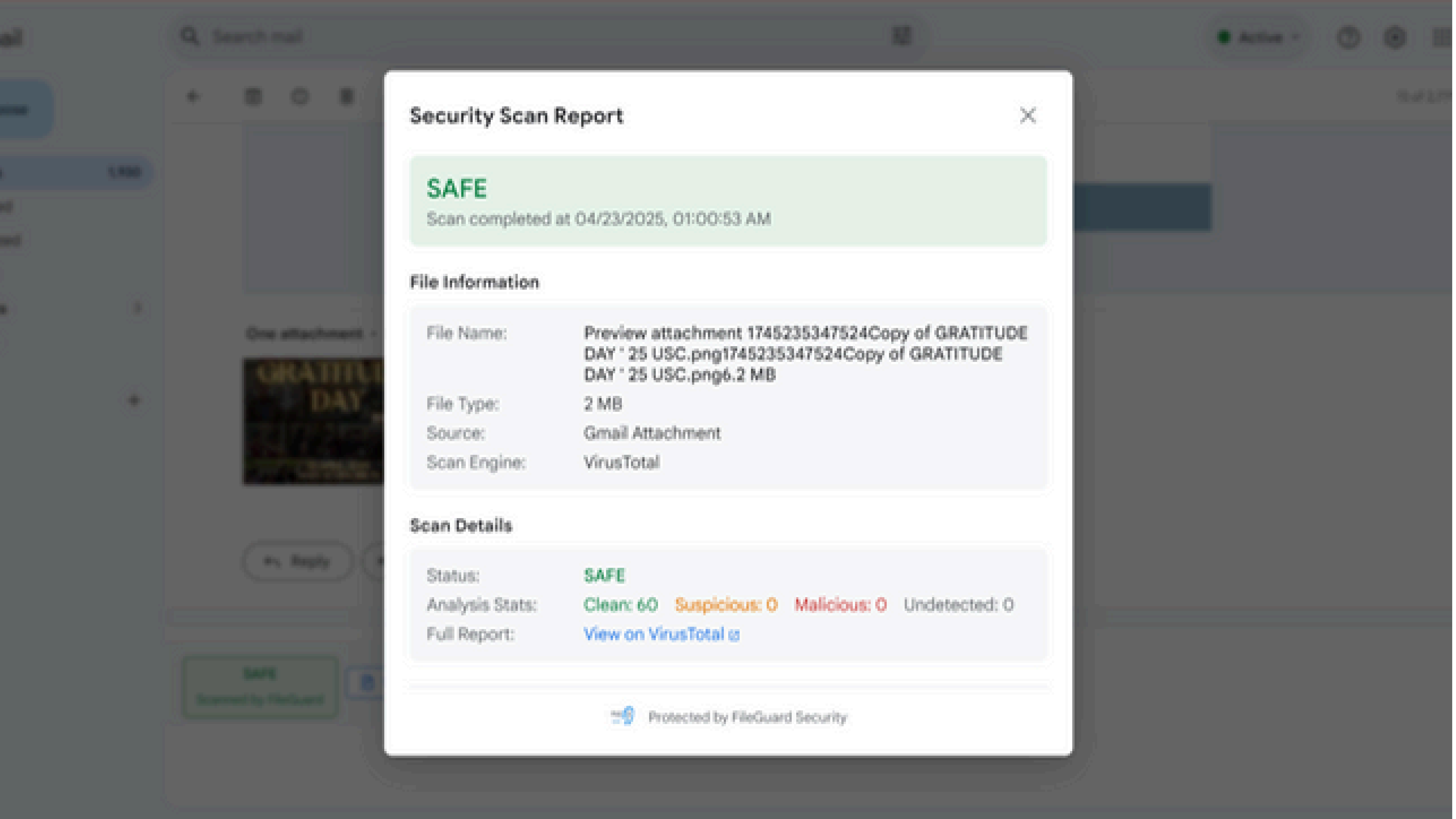
Gmail
Search mail
Active
Compose
Inbox 1,930
Starred
Snoozed
Sent
Drafts 3
Drafts
More
Labels
One attachment • Scanned by Gmail
GRATITUDE DAY
Reply
Reply all
Forward
Scanning...



One attachment • Scanned by Gmail

SAFE

Scanned by FileGuard



Security Scan Report

SAFE

Scan completed at 04/23/2025, 01:00:53 AM

File Information

File Name: Preview attachment 1745235347524Copy of GRATITUDE DAY ' 25 USC.png1745235347524Copy of GRATITUDE DAY ' 25 USC.png6.2 MB

File Type: 2 MB

Source: Gmail Attachment

Scan Engine: VirusTotal

Scan Details

Status: SAFE

Analysis Stats: Clean: 60 Suspicious: 0 Malicious: 0 Undetected: 0

Full Report: View on VirusTotal

Protected by FileGuard Security

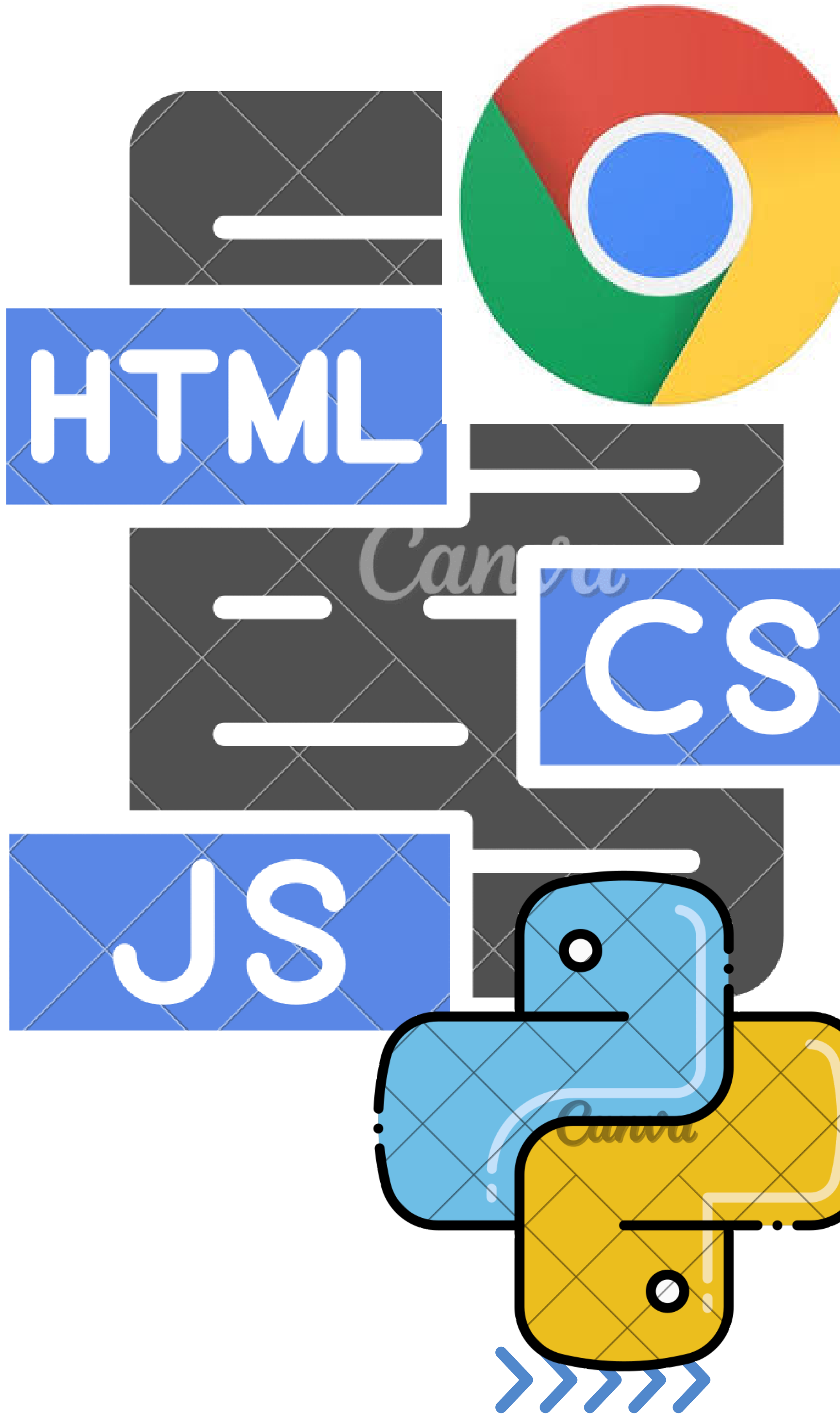
TECH STACK

FRONTEND: HTML, CSS, JavaScript.

BACKEND: Python

DATABASE: VirusTotal Malware Database

API: VirusTotal API , Chrome Extension API



Front-End

Provides the "Scan" button, results modal, and visual feedback.

Developed using HTML, CSS, and JavaScript.

GUI

When integrated into Gmail, the tool adds features like:

- Scan Button: Visible next to email attachments.
- Scan Report Modal: A pop-up or small window shows detailed results after scanning.
- Visual Indicators: Use colors or icons (green for safe, red for malicious) for quick understanding.

Back-End

A server-side system (e.g., Node.js or Python) communicates with external malware scanners like VirusTotal to analyze files .

Processing and API Integration:

Handles file scanning by communicating with external APIs (e.g., VirusTotal).

Built using Node.js, Python.

Database:

No Traditional Database Used

- In our project, we did not use a traditional database like MongoDB or MySQL to store data.

Malware Detection using VirusTotal API

- Instead of storing files or user data, we focused on scanning and verifying uploaded files.
- We integrated VirusTotal API, a trusted tool for checking files for malware and viruses.

Hardware Requirements

Processor

Processor: Dual-core or higher (Quad-core recommended for heavy workloads).

RAM

RAM: 4GB or higher (8GB recommended for multitasking).

Storage

Storage: 10GB free space (more for large files or logs).

FILE GUARD

FILE GUARD

COMPARISON BETWEEN EXISTING SOFTWARES

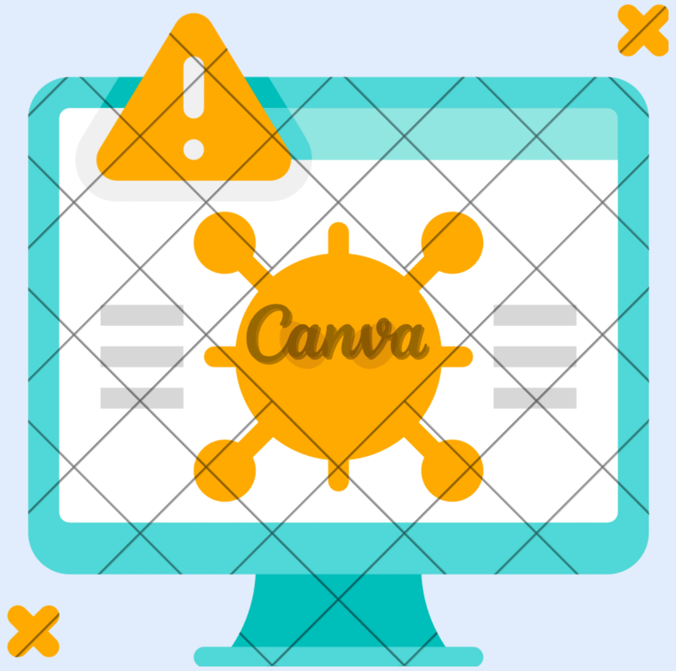
Gmail’s Anti Malware Softwares vs File Guard

Google Workspace (Enterprise)

Uses Google's internal malware detection system, which operates automatically in the background.

Automated scanning with no user interaction or detailed feedback.

Scans each attachment automatically but doesn't store scan logs.



File Guard

1. Enhanced Detection
Uses 70+ antivirus engines through VirusTotal
Higher detection rate for new and complex threats
Reduced false positives through consensus scanning

2. User Control
Choose when to scan attachments
Review detailed threat analysis
Make informed decisions about attachments

3. Comprehensive Reports
Detailed scan results from multiple engines

FILE GUARD

FILE GUARD

THANK YOU!