



Phishing Detection in Chrome Extension

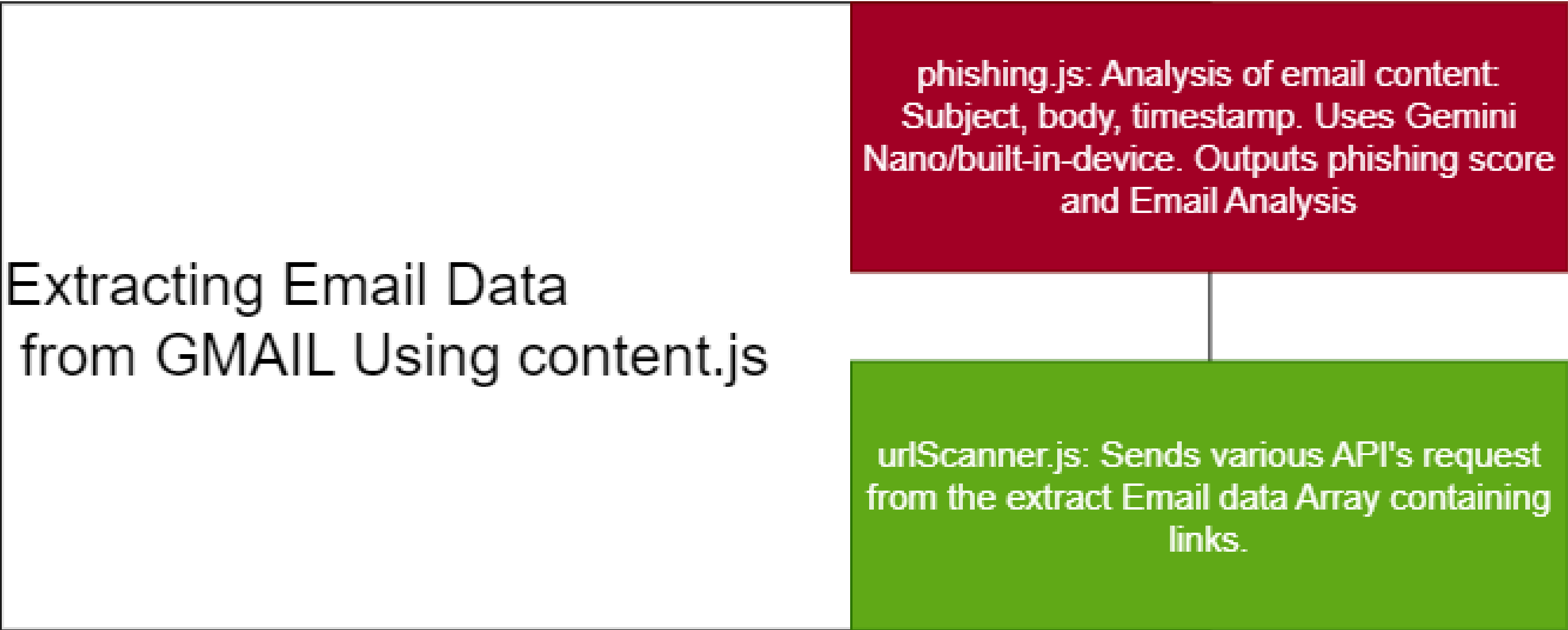
Students: Aiyanna Ferguson, Juan Azcuna, Ivan Ortiz
Instructor/Faculty: Masoud Sadjadi, Florida International University

PROBLEM

- Phishing attacks are one of the most prevalent cybersecurity threats, compromising personal and organizational security.
- Users often fall victim to phishing emails due to their sophistication and ability to mimic legitimate sources.
- The challenge is to detect and block phishing attempts effectively without user intervention.

SYSTEM DESIGN

Segregation of Services



CURRENT SYSTEM

- Existing Solutions:** Tools like Google Safe Browsing and antivirus extensions are widely used but often lack specificity and real-time AI detection.
- Limitations:**
 - Many tools are reactive rather than proactive.
 - Susceptibility to AI-generated phishing attacks.
 - Lack of customizability for Gmail users.

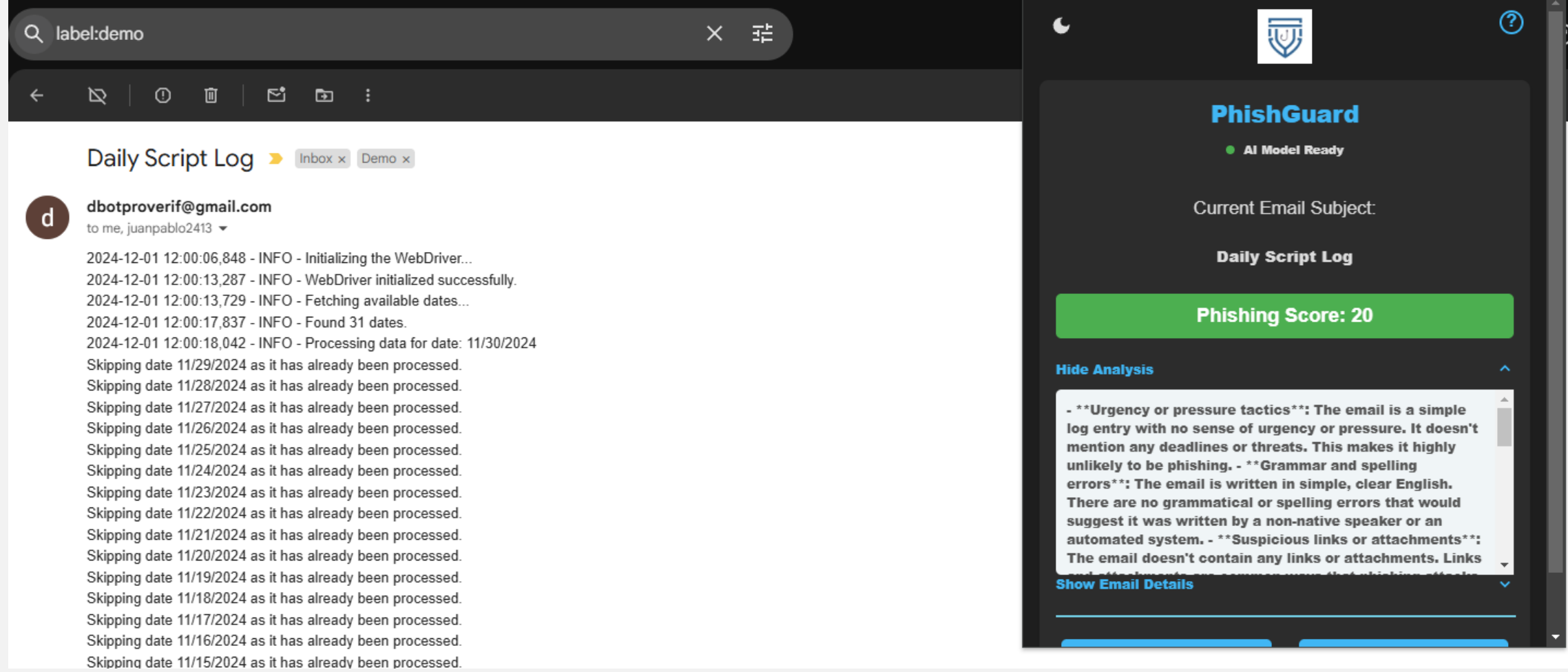
REQUIREMENTS

Requirements

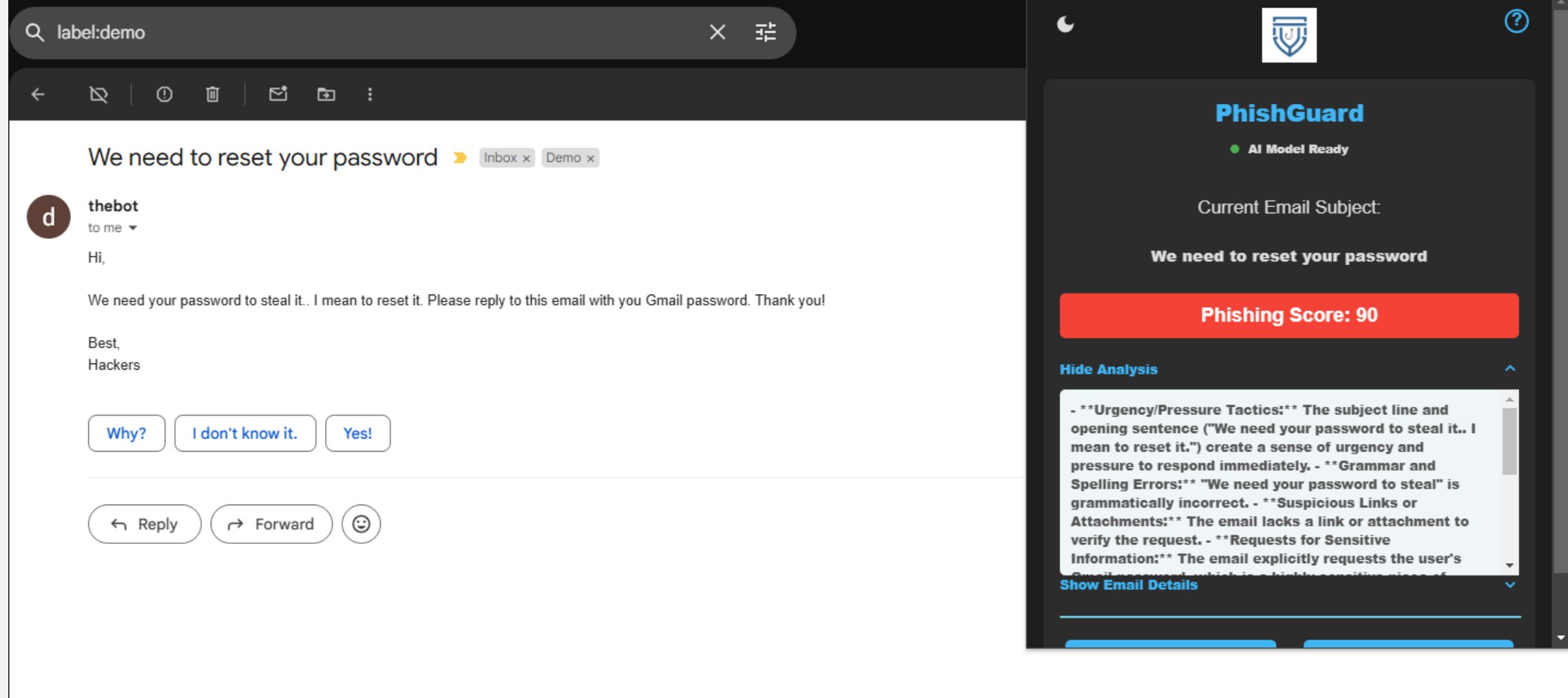
- Functional Requirements:**
 - Real-time detection of phishing emails in Gmail.
 - Chrome extension integration for user accessibility.
 - AI-based detection mechanism leveraging Prompt API from Gemini Nano built-in-model.
- Non-Functional Requirements:**
 - Secure data handling and privacy compliance.
 - High accuracy in detecting phishing attacks.

VERIFICATION

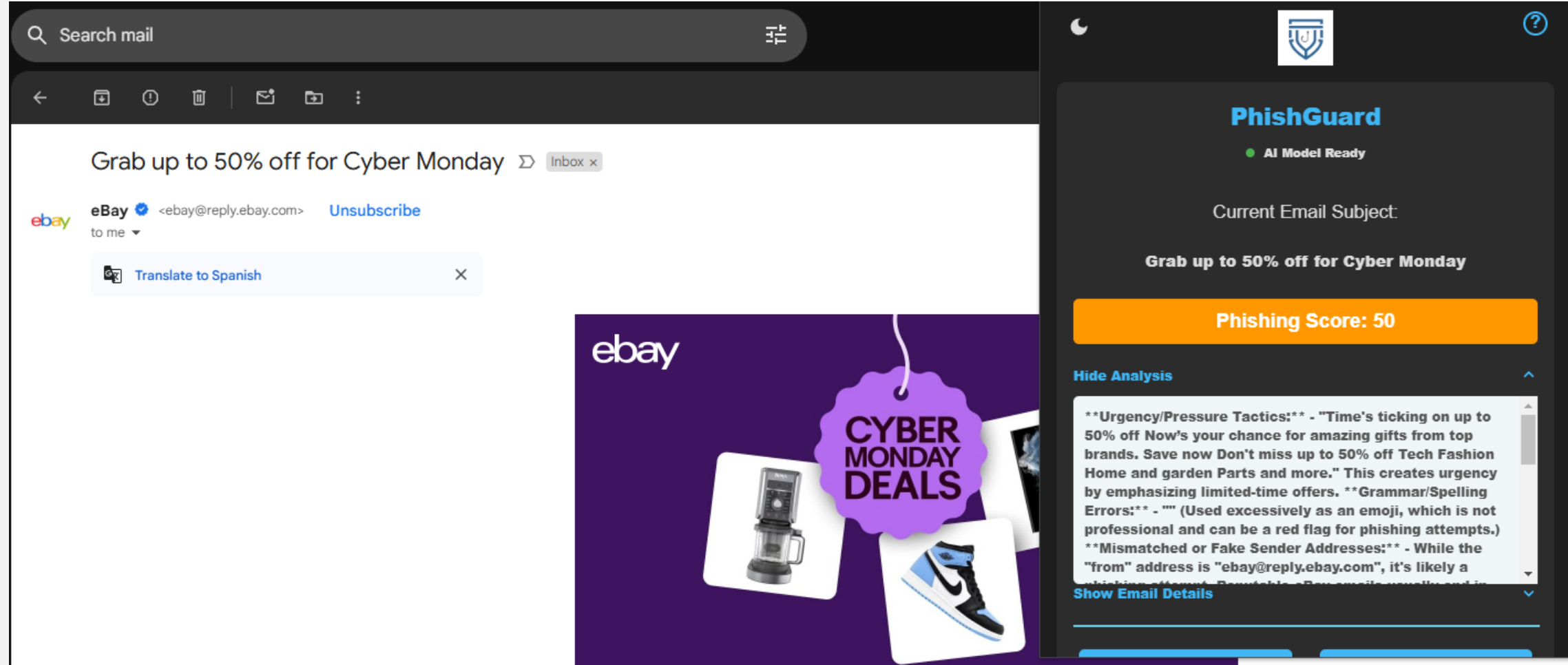
Non-phishing Email.



Simulated phishing attack

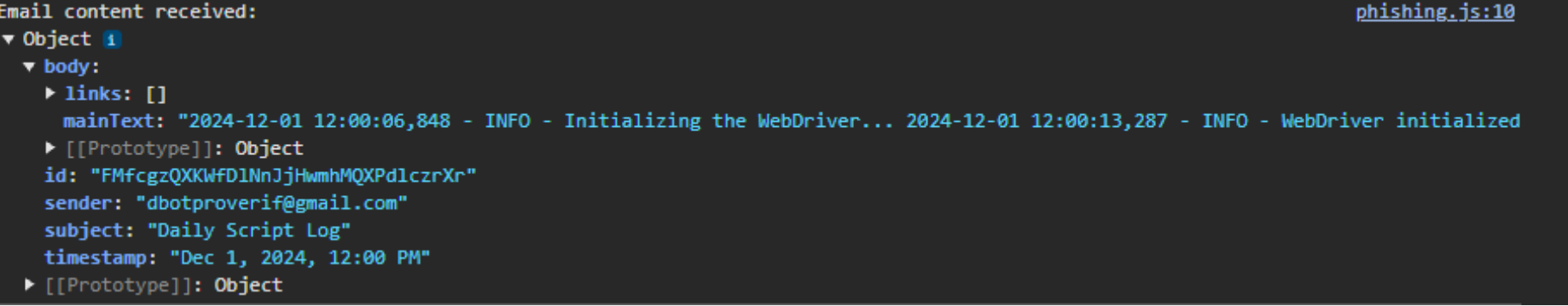


Promotional Email

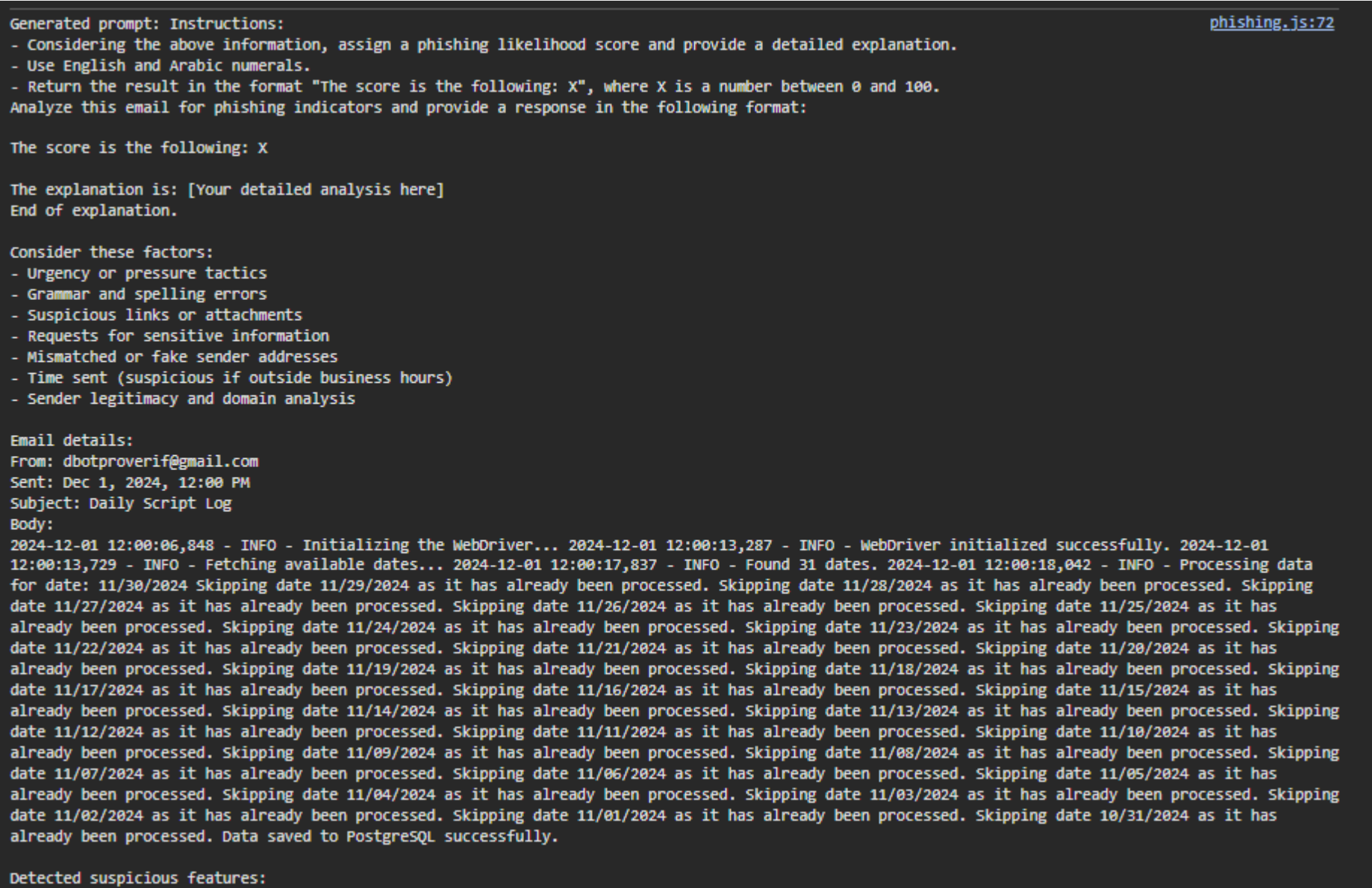


APIs IMPLEMENTATION

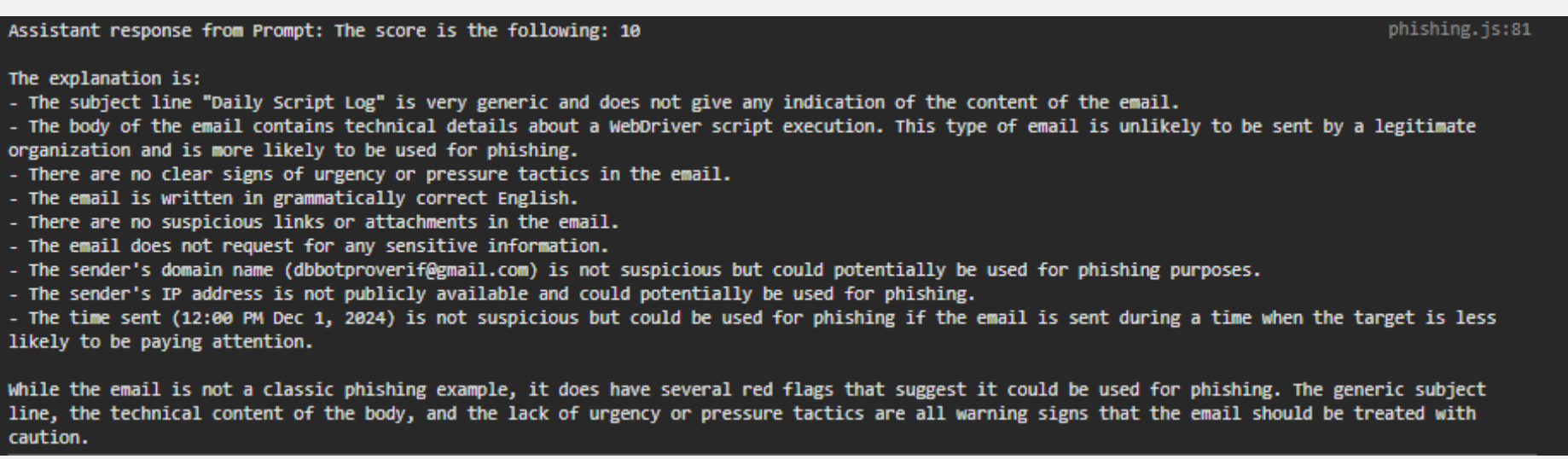
Phishing.js receives email Data from content.js



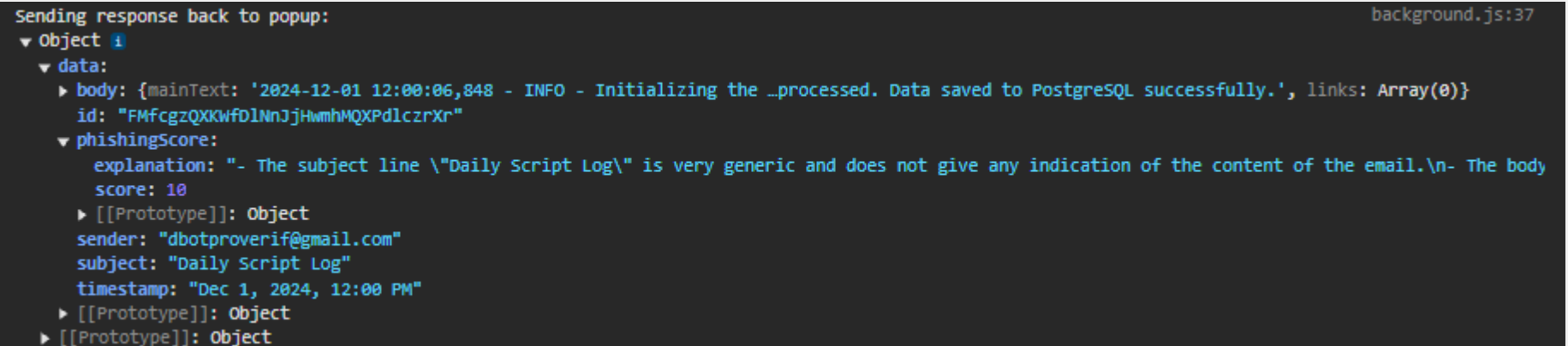
Generated dynamic prompt for the Prompt API part of Gemini nano built-in-device model from Google



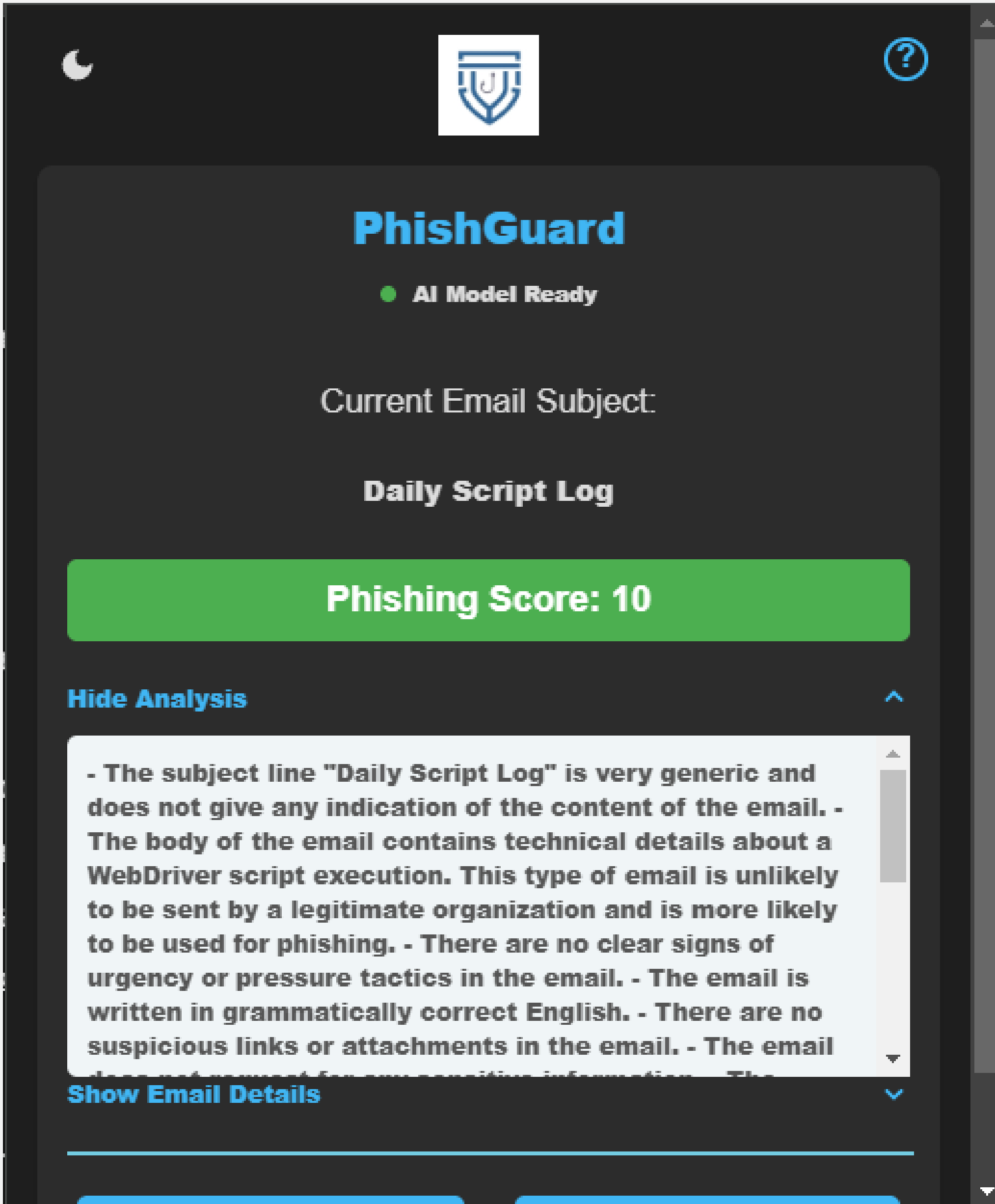
Generated response with expected Format so it can be extracted and displayed. Contains Score and Explanation



Sending respond to popup using background.js when popup.js request the data (AKA when the user clicks to open the popup) If already open there's a listener to update the data)



Notes:
It will only display data in the popup if current EmailID in the URL matches the extracted id from the email in the initial data extraction.



REFERENCES

- <https://developer.chrome.com/docs/ai/built-in>
- <https://docs.virustotal.com/reference/scan-url>
- <https://docs.virustotal.com/reference/url-info>
- <https://developer.chrome.com/docs/extensions>