Phish-Guard: Gmail Email Phishing Detection Extension

Overview

Phish-Guard is a Chrome extension designed to enhance email security by analyzing emails within Gmail and generating reports on potential phishing attempts and suspicious activity.

Purpose

The main goal of Phish-Guard is to improve Gmail users' security by identifying and flagging potential phishing threats in real-time. By providing clear and actionable warnings, the tool helps users avoid falling victim to malicious emails.

Challenges Encountered

Understanding Gmail's DOM Structure: As newcomers to Gmail's internal architecture, we faced challenges in integrating with its dynamic DOM to accurately detect when an email was opened.

Limited Experience with the Programming Language: The project required proficiency in a programming language that we had used only minimally during our studies, requiring additional learning and adaptation.

Interacting with Google Safe Browsing API: Understanding how to properly communicate with the Google Safe Browsing API and managing API keys securely was a crucial challenge.

Selecting the Right Tools: Choosing the appropriate tools and technologies to effectively implement the phishing detection logic was a key part of the development process.

Defining Phishing Email Characteristics: Identifying key indicators of phishing emails, such as suspicious language, deceptive links, and untrusted senders, to enhance detection accuracy.

Strengths and Weaknesses

Strengths

- Real-time analysis and immediate user feedback.
- Integration with Google Safe Browsing for reliable threat detection.
- Easy-to-use interface for non-technical users.

Weaknesses

- Dependency on Gmail's current DOM structure; changes could require updates.
- Limited to Gmail and Chrome; lacks cross-platform compatibility.
- Relies heavily on external APIs, which could impact performance in case of service downtime.

How the Tool Works

1. Email Monitoring: The extension observes Gmail tabs and detects when an email is opened.
2. Data Extraction: Extracts details such as sender information, subject, email body, and attachments.
3. Risk Analysis: Assesses the email's risk level based on phishing keywords, suspicious links, sender trustworthiness, and attachment types.
4. Reporting: Displays a visual risk score and highlights findings in a user-friendly report.

Code and Key Components

1. Core Function in content.js

- analyzeEmail(emailDetails)

  ### Role:

  This is the core function of the project, responsible for orchestrating the analysis of an email and determining its risk level.

  ### Key Steps:

  - Accepts emailDetails containing sender, subject, links, and content.
  - Calls calculateSuspicionScore to compute the risk score.
  - Based on the score, triggers appropriate alerts:
    - High Risk: Calls showSecurityReport to display a warning.
    - Medium Risk: Calls showSecurityReport with a cautionary message.
    - Low Risk: Calls showSafeEmailAlert for confirmation and reporting.

- calculateSuspicionScore()

  ### Role:

  Calculates a numeric score (0100) based on suspicious elements in the email.

  ### Key Checks:

  - Keywords: Looks for phishing-related phrases like "verify your account."
  - Links: Scans all links using checkUrlWithGoogle (Google Safe Browsing API).
  - Sender: Validates the sender's domain using checkDomainWithGoogle.
  - Attachments: Checks for suspicious file types like .exe, .bat, .vbs, or other potentially harmful attachments.

- showSecurityReport(score, findings)

  ### Role:

  Displays a detailed security report for high or medium-risk emails.

  ### Key Features:

  - Shows the risk score visually with a progress bar.
  - Lists suspicious findings (e.g., untrusted sender, suspicious links).
  - Provides a "Close" button to dismiss the report.

- showSafeEmailAlert(score, findings)

  ### Role:

  Shows a confirmation alert for low-risk (safe) emails.

  ### Key Features:

  - Includes a message confirming the email is safe.

    - Offers a "Report" button for the user to flag the email if they feel it's suspicious.
    - Provides feedback ("Thank you for reporting!") when the "Report" button is clicked.

- checkUrlWithGoogle(url)

  Role:

  Uses the Google Safe Browsing API to check if a URL is malicious.

  Key Features:

    - Sends the URL to Google for validation.
    - Returns true for safe URLs and false for flagged ones.

- checkDomainWithGoogle(domain)

  Role:

  Validates the sender's domain using the Google Safe Browsing API.

  Key Features:

    - Converts the domain to a valid URL format.
    - Sends the domain to Google for analysis.
    - Returns true for trusted domains and false for suspicious ones.

- isContentPhishing()

  Role:

  Checks the email content for phishing-related keywords.

  Key Features:

    - Looks for common phishing phrases like "urgent action required."
    - Returns true if any keywords are found.

2. manifest.json

Defines extension metadata and permissions, such as access to Gmail and Safe Browsing API.

3. rules.json

Contains declarative rules for blocking specific malicious domains (e.g., phishingsite.com, malware.com).

Alert Levels and How They Are Triggered

How the Risk Score is Calculated

The email is analyzed based on multiple factors, each contributing a weighted score to determine the final suspicion score (0-100).

Factor	Weight	How It Contributes
Phishing Phrases	**40%**	**Checks if the email contains suspicious keywords like “verify your account” or “urgent action required.”**
Suspicious Links	**30%**	**Evaluates links using Google Safe Browsing API to detect known phishing or malware sites.**
Untrusted Sender	**20%**	**Determines if the sender’s email domain is known, reputable, or suspicious.**
Suspicious Attachments	**10%**	**Flags potentially dangerous file types like .exe, .js, .bat.**

High-Risk Alert (Severe Phishing Threat)

Risk Score >= 70

Example Email:

Dear User,

We have detected unauthorized activity on your account. Immediate action is required to secure your information.

Click the link below to verify your account details:

Failure to act within 24 hours will result in your account being permanently disabled.

Best regards,
Account Security Team

Action Taken by Extension:
Displays a Red Warning Box indicating a high phishing risk.
Warns the user about suspicious links, sender, and phishing indicators.

Medium-Risk Alert (Suspicious Email)

30 <= Risk Score <= 69

Example Email:

Dear User,

We noticed an unusual login attempt from a new device. If this was not you, please secure your account.

Click here to confirm:

If you do not respond within 24 hours, your account may be locked for security reasons.

Best regards,
Security Team

Action Taken by Extension:
Displays an Orange Warning Box advising caution.

Provides detailed information about suspicious elements detected in the email.

Low-Risk Alert (Safe Email)

Risk Score <= 29

Action Taken by Extension:
Displays a Green Confirmation Box indicating that the email is safe.
Gives the user an option to report the email if they still believe it might be suspicious.

Setup Instructions

Prerequisites

- Google Chrome installed on your system.
- Basic understanding of Chrome extensions.

Installation Steps

1. Download and extract the project files.
2. Open Chrome and go to chrome://extensions/.
3. Enable Developer Mode.
4. Click Load unpacked and select the project folder.

Usage Instructions

1. Open Gmail in Google Chrome.
2. Navigate to an email. The extension will analyze the email in real-time.
3. Based on the risk score:
    - High Risk: Displays a detailed security report with warnings.
    - Medium Risk: Shows cautionary recommendations.
    - Low Risk: Confirms the email is safe.

Future Enhancements

- Cross-platform support (e.g., Firefox, Outlook).
- Incorporation of machine learning models for advanced phishing detection.
- Localization for multiple languages.

Acknowledgments

- Google Safe Browsing API for link and domain validation.
- Chrome Extension Documentation for development guidance.