**SVKM’S NARSEE MONJEE INSTITUTE OF MANAGEMENT STUDIES**

**SCHOOL OF TECHNOLOGY AND MANAGEMENT ENGINEERING**

****

**SUBJECT: NLP**

**PROJECT REPORT**

**SUBMITTED BY: SUBMITTED TO:**

**Name:** Shreya Gupta Dr. RajGaurav Mishra

**Class:** B.Tech CE Sem VII

**Batch:** Batch 1

**Roll no:** T084

**SAP Id:** 70022200559

**Project Report: Email Phishing Detector Chrome Extension**

**1. Introduction**

The **Email Phishing Detector** is a Chrome extension designed to help users identify and understand potential phishing attempts within their emails. By utilizing advanced detection techniques and an interactive, user-friendly interface, this tool empowers users to recognize fraudulent content and protect themselves from cyber threats , all while keeping their data secure and private.

**2. Objectives**

The primary objectives of the Email Phishing Detector project are:

* To detect and highlight phishing indicators in real-time within emails.
* To classify the overall risk level of an email based on detected red flags.
* To provide an interactive, easy-to-understand interface for users.
* To ensure data privacy by performing all analysis locally within the browser.

**3. Features**

**Smart Detection**

* Analyzes email content in real-time directly in the user’s browser.
* Detects multiple phishing indicators such as:
  + Urgency tactics and pressure language
  + Suspicious links and URL patterns
  + Generic or impersonal greetings
  + Requests for sensitive information
  + Time pressure tactics
  + Potential sender spoofing

**Risk Assessment**

* Provides a **three-level risk classification system**:
  + 🔴 **High Risk** – Likely phishing attempt
  + 🟡 **Suspicious** – Exercise caution
  + 🟢 **Low Risk** – No obvious red flags

**Interactive Analysis**

* Click on detected issues to highlight them within the email.
* Displays **visual badges** for different types of threats.
* Provides **detailed explanations** for each detected issue.
* Suggests **specific recommendations** based on the overall risk level.

**4. Usage**

**Supported Email Providers**

* Currently supports **Gmail**.

**Steps to Use**

1. Open an email in Gmail.
2. Click the **Email Phishing Detector** extension icon.
3. Select **“Scan Current Email.”**
4. Review the analysis results:
   * Overall risk level
   * Warning badges for specific threats
   * Detailed list of detected issues
5. Click any issue to highlight it in the email.
6. Review recommended actions for safety.

**5. Technical Details**

**File Structure**

email-phishing-detector/

│

├── manifest.json # Extension configuration

├── popup.html # Extension popup interface

├── popup.js # Popup functionality and UI handling

├── content.js # Email analysis and content processing

└── images/ # Extension icons

**Detection Patterns**

The extension analyzes email content for:

* Suspicious sender domains
* Urgency keywords in subject line
* Suspicious URL or hyperlink patterns
* Common phishing-related phrases
* Generic or impersonal greetings
* Time pressure tactics
* Requests for sensitive information

**6. Security Considerations**

* The extension runs **entirely within the user’s browser**.
* **No email content is sent** to any external servers.
* **All analysis is performed locally**, ensuring data privacy.
* The extension **does not collect or store** any sensitive user information.

**7. Future Enhancements**

The following features are planned for future versions of the extension:

1. Support for additional email providers (Outlook, Yahoo, etc.)
2. Integration of **machine learning-based detection** algorithms.
3. Custom **user-defined detection rules**.
4. **Historical analysis tracking** to monitor repeated threats.
5. **Bulk email scanning** functionality.
6. Integration with **known phishing databases**.
7. **Export and reporting** features for organizational use.

**8. Conclusion**

The **Email Phishing Detector Chrome Extension** is an innovative and privacy-conscious tool designed to help users recognize phishing attempts in real-time. With its intuitive design, local analysis, and robust detection logic, it enhances user security without compromising personal privacy. Future enhancements aim to make it more adaptive, intelligent, and widely applicable across various email platforms.