



Knight Foundation

School of Computing and Information Sciences

Florida International University

Fall 2024 Capstone Project

Phishing Detection in Chrome Extension

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

PROBLEM

Phishing is a social engineering tactic that uses deception and disguise to trick users into divulging sensitive information about themselves or an organization. It poses a significant threat to the data of organizations and online users especially by the means of spear phishing. Many users have fallen victim to these attacks by clicking email links that redirect them to malicious sites (Varshney et al., 2024).

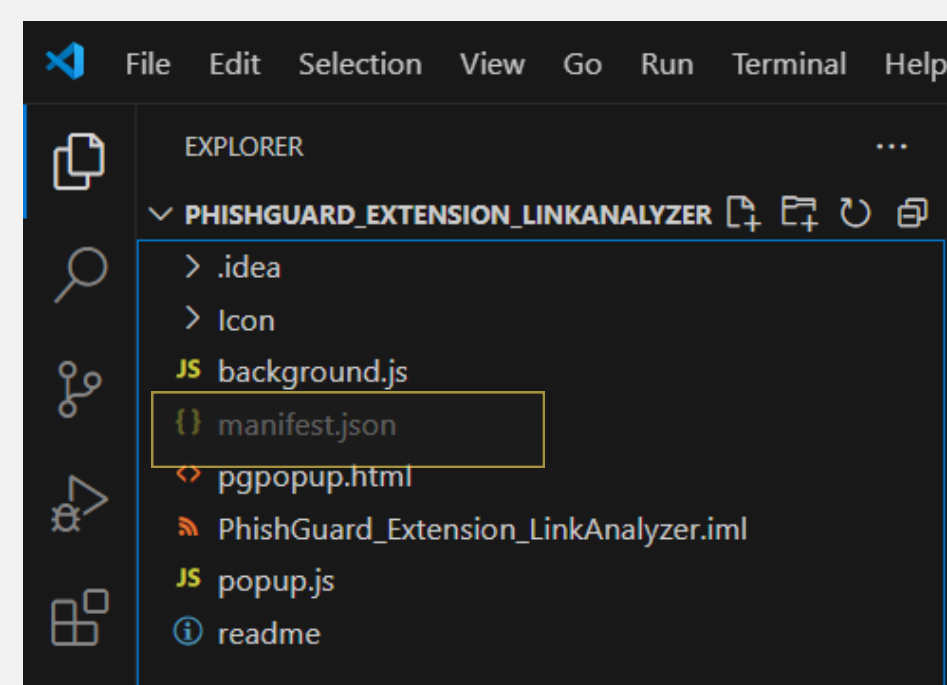


Over 90% of cybersecurity incidents begin with spear phishing (Varshney et al., 2024).

IMPLEMENTATION

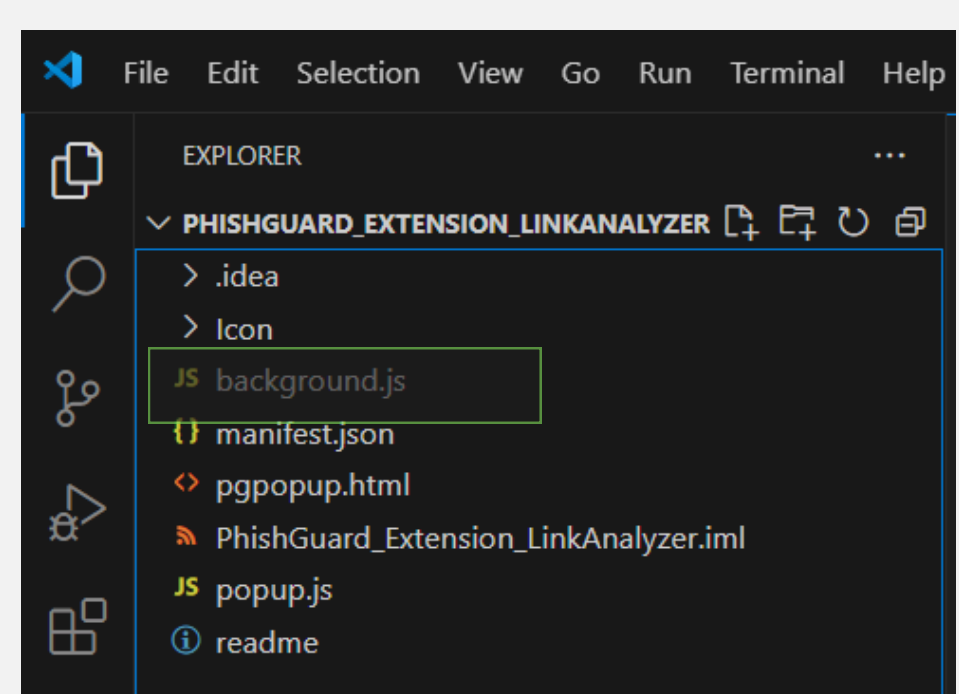
There are nine (9) core user interface (UI) components needed for Chrome extensions to operate efficiently ("Extensions / Develop"). The link analyzer utilizes three (3) of them for proper functioning including permissions, service workers, and messaging.

USER SECURITY: DEFINING PERMISSIONS



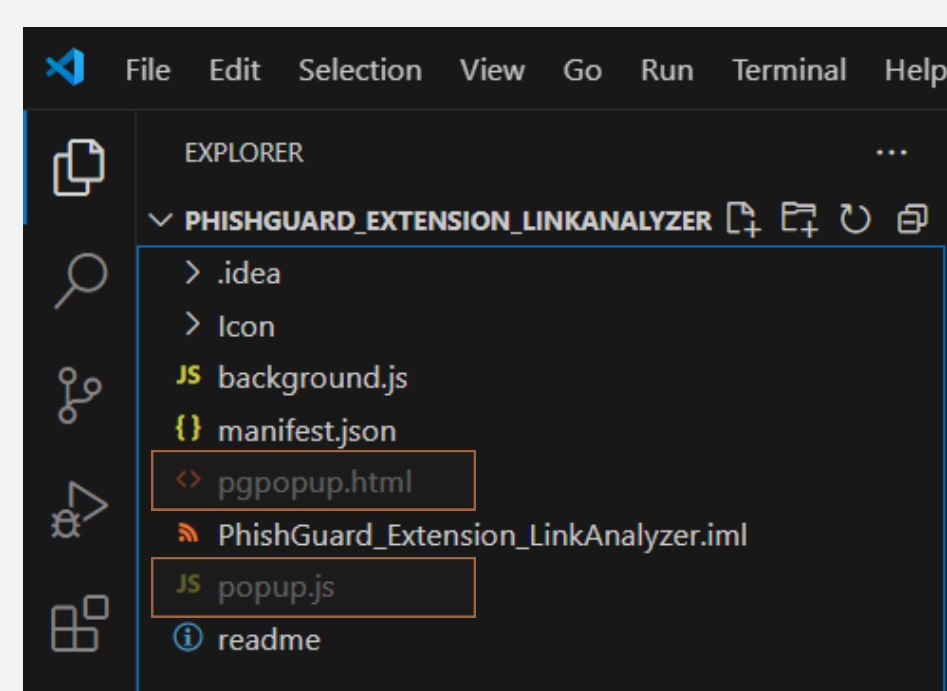
The extension's link analyzing feature is equipped with proper permissions that ensure user security. For example, the active tab permission only allows access to the tab the user is operating, otherwise this access is denied. It also defines a limited number of hosts in which the extension would interact with when in use.

SERVICE WORKER



The service worker in this case, background.js, manages the background processes and coordinates tasks for the extension. This script, along with the popup script incorporates messaging that allows both to communicate with each other to determine the results of the link analysis and alert the user of its safety.

USER INTERFACE

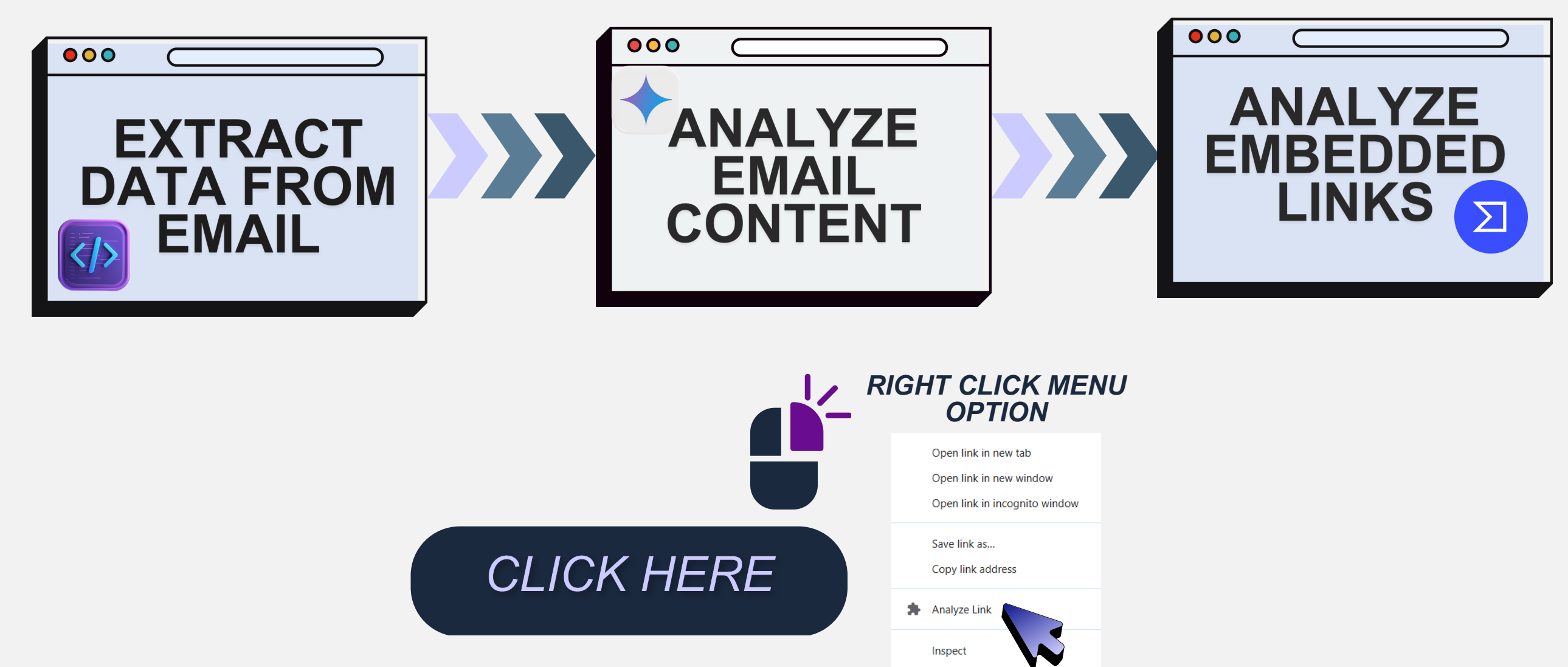


The user interface describes how the user is able to interact with the extension in order to analyze their links. PhishGuard provides two (2) options. One allows users to right-click a link within their email and select 'Analyze Link' while the other allows users to input the link by clicking directly on the extension within their Chrome browser.

OBJECTIVE

Extensions give online users the ability to add additional functionalities to their webpage. The PhishGuard Chrome extension aims to further user awareness and knowledge of spear phishing by analyzing Gmail content to determine the likeability of an email being a phishing attempt and offering users the ability to analyze links. This poster provides an overview of the extension's link analyzing feature using the public version of VirusTotal API v3.

PROJECT OVERVIEW



OBSTACLES

LIMITATIONS

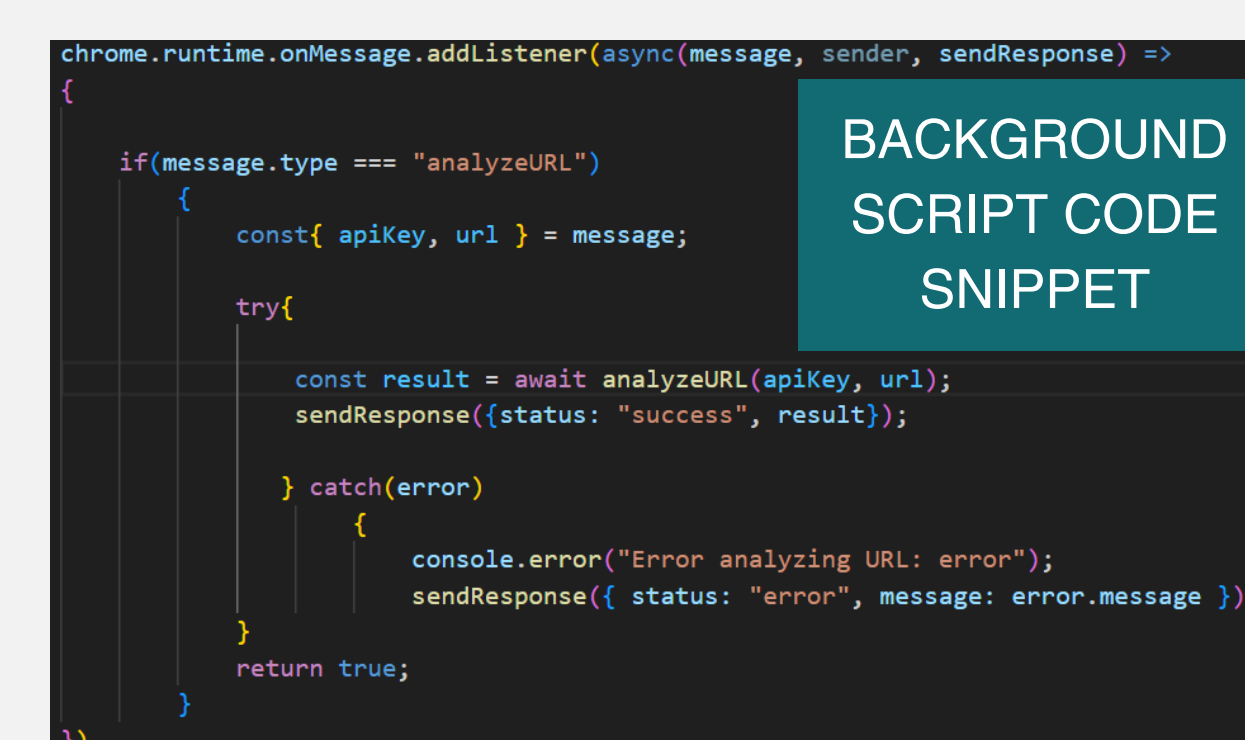
Numerous tests were conducted for the link analyzer during the debugging phase to improve the codes in order to yield the desired outcome. However, two main limitations stood out that prevented the link analysis from being conducted: CORS (Cross-Origin Resource Sharing) Blocking and Error Handling Difficulties.

When trying to carry-out the link analysis and fetch the reports to advise users of the link's safety, access to fetch reports from VirusTotal's API was blocked by the CORS policy. A possible solution would be to include an 'Access-Control-Allow-Origin' header within the code to bypass CORS and fetch the required information. However, this may expose sensitive regarding the user.

Further research and development are needed to ensure API (Application Programming Interface) calls are made in compliance to Chrome's CORS policies. This combined with refining error handling and messaging within the background and popup scripts can aid in the overall improvement of PhishGuard's link analysis capabilities.

STRUCTURE

MESSAGE HANDLING BETWEEN BACKGROUND AND POPUP SCRIPTS.

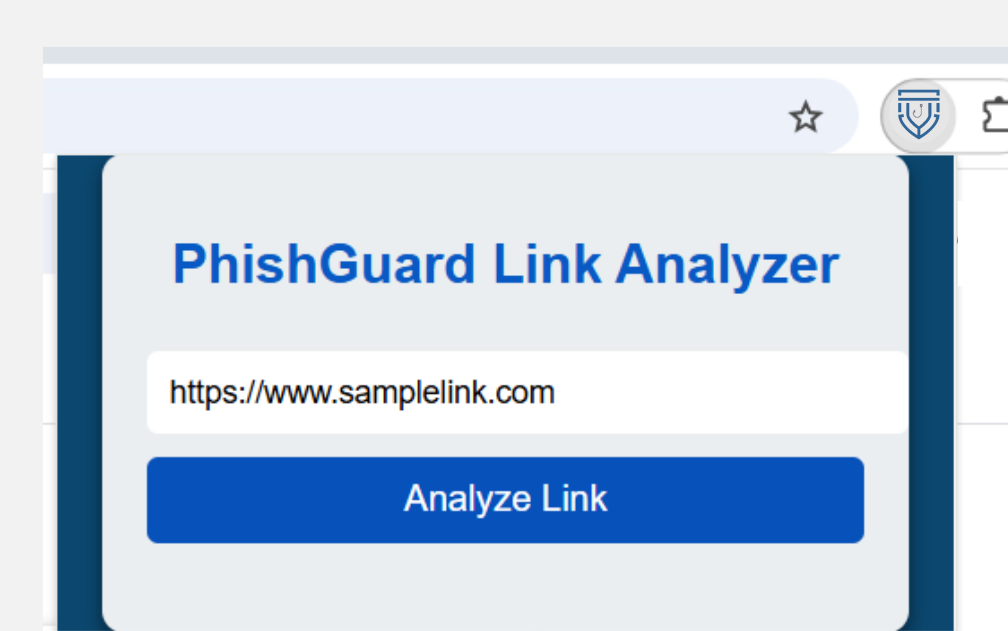


The popup script prompts the background script to conduct the analysis. The background script listens for this request, conducts analysis, and send results to the popup to display the appropriate alert for the user.

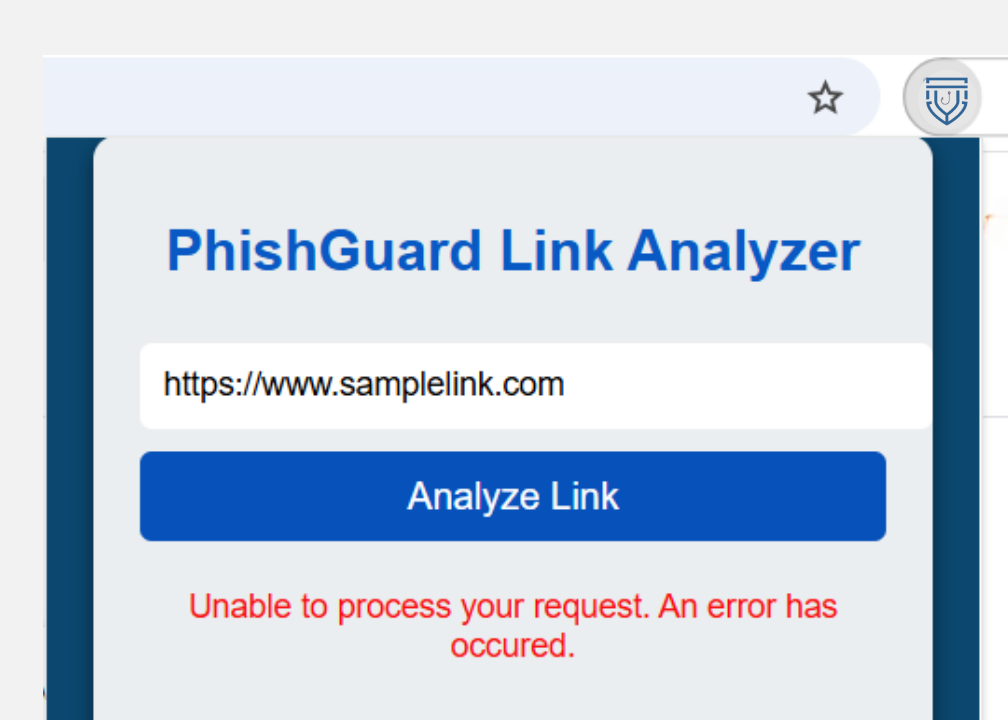


FUNCTIONALITY

STEP 1: USER ENTERS LINK TO TRIGGER ANALYSIS

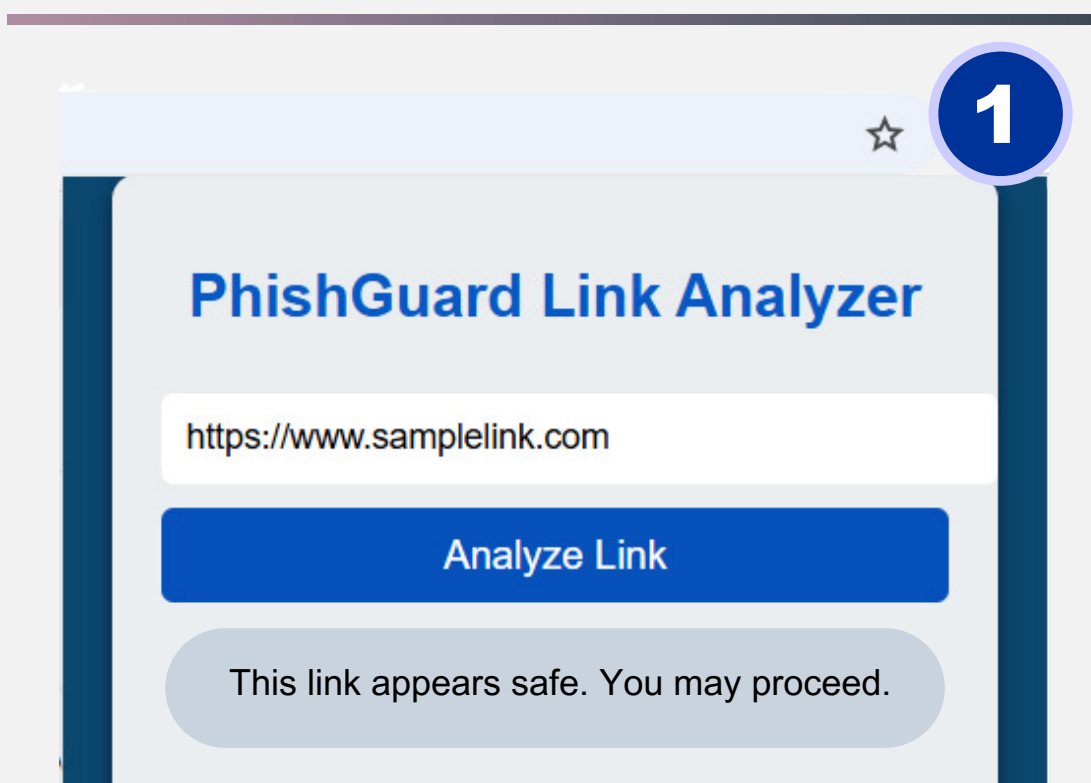


ACTUAL RESULT

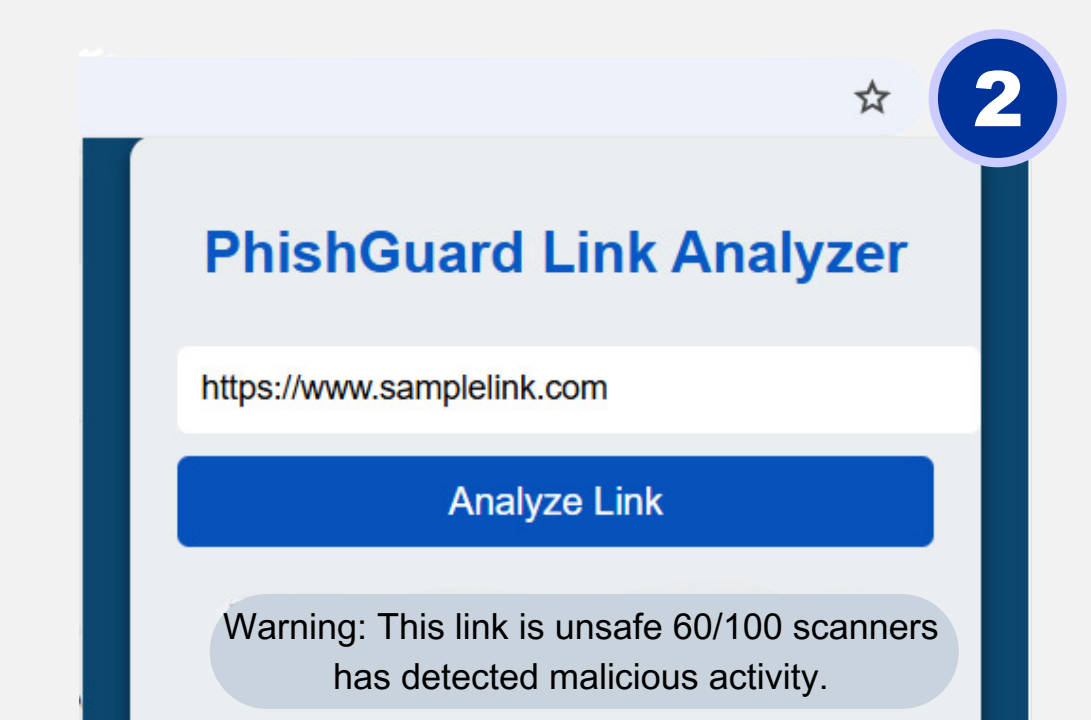


DESIRED RESULTS

IF THE LINK IS FOUND SAFE



IF THE LINK IS FOUND UNSAFE



Knight Foundation
School of Computing
and Information Sciences

FLORIDA INTERNATIONAL UNIVERSITY

References

- Varshney, Gaurav, et al. "Anti-Phishing: A Comprehensive Perspective." Expert Systems with Applications, vol. 238, 15 Mar. 2024, p. 122199, doi:10.1016/j.eswa.2023.122199.
- "Protect User Privacy." Chrome for Developers, 2018, developer.chrome.com/docs/extensions/develop/security-privacy/user-privacy.
- "Extensions / Develop." Chrome for Developers, developer.chrome.com/docs/extensions/develop.