Cyber Safe

Phishing Detection Browser Extension

By:

Drashti Shah

Kahan Velani

Priyanshu Khambalkar

Dhruv Parmar

Project Mentor

Dr.Tejas Bhatt

Content

Aim & Objective

Aim:

The aim of this project is to develop a Browser Extension that detects phishing websites by analyzing the active tab's URL, checking its legitimacy against a predefined list, and verifying its SSL/TLS certificate details. The extension enhances cybersecurity awareness by providing real-time alerts and prevention tips to protect users from malicious websites.

Aim & Objective

Objective:

- To develop a browser extension that actively monitors website URLs and detects potential phishing threats.
- To implement a URL verification mechanism that compares active website links against a trusted database of legitimate sites.
- To integrate SSL/TLS certificate validation using the CertSpotter API, ensuring users can check the authenticity of websites.
- To enhance user awareness by providing real-time phishing alerts and security best practices.
- To create a simple and user-friendly interface that effectively informs users about website security without technical complexity.

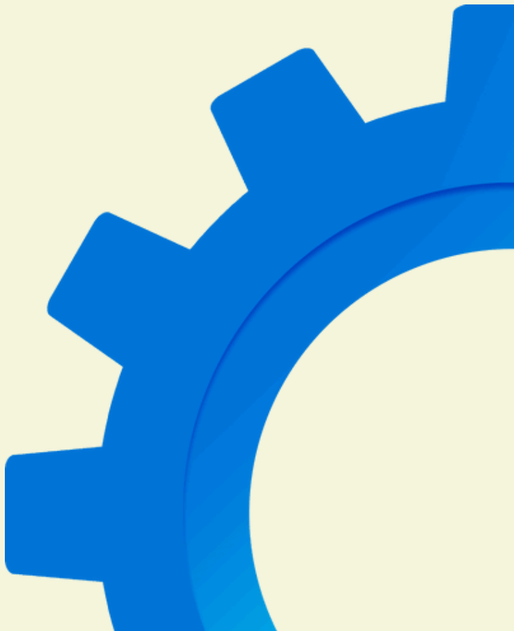
Introduction

- In today's digital world, phishing attacks are among the most common and dangerous cybersecurity threats. Attackers often create fake websites that mimic legitimate ones to steal sensitive information like passwords, credit card details, and personal data.
- To combat this, our project, Cyber Safe, introduces a browser extension to detect and prevent phishing attempts in real-time. By analyzing website URLs and verifying SSL/TLS certificates, the extension provides users with immediate alerts when they encounter potentially malicious sites.
- Unlike traditional phishing detection methods, which rely solely on blacklists, Cyber Safe offers a proactive approach. It cross-checks URLs using trusted databases and APIs like Google Safe Browsing. The extension ensures users are informed and protected while browsing, minimizing the risk of falling victim to phishing attacks.

Proposed Solution

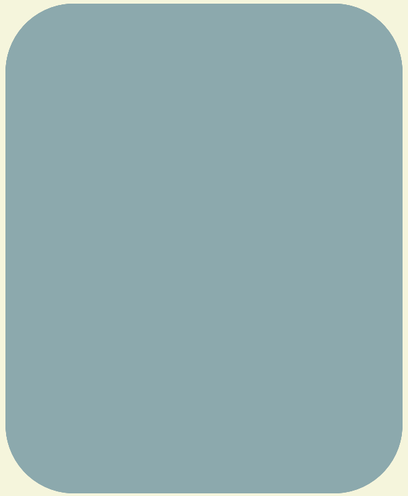
- To effectively combat phishing attacks, our project proposes the Cyber Safe browser extension. This extension leverages the Google Safe Browsing API to provide real-time protection by detecting malicious websites and safeguarding users from phishing attempts.
- Our extension Provides:
  - The extension fetches URL from active tab.
  - Checks the URL against continuously update database of malicious and unsafe sites using Google Safe Browsing API to detect sign of phishing.
  - Examines and verifies website SSL/TLS certificate to verify it legitimacy.
  - Users are instantly notified if the website is flagged as malicious.
  - The extension provides a clear pop-up notification summarizing the security status of the website.

How it will work ?

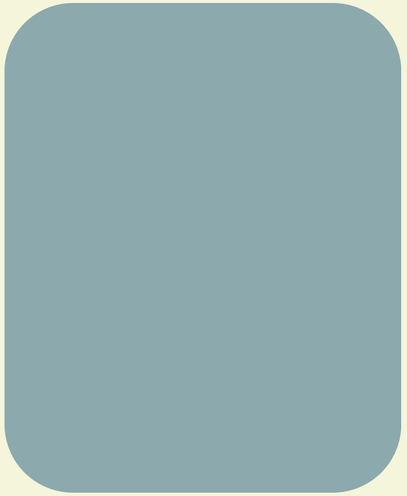
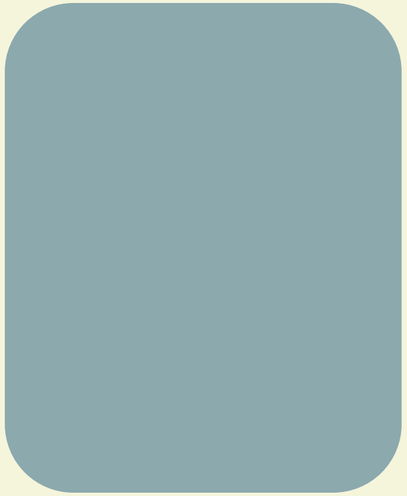
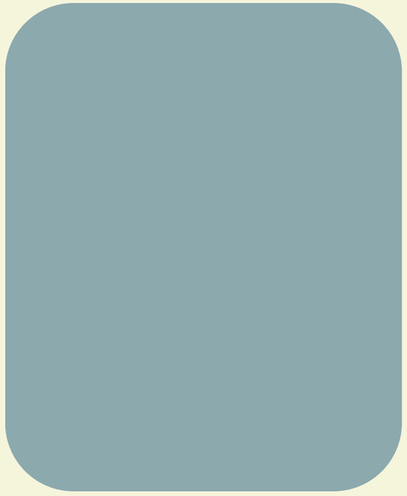
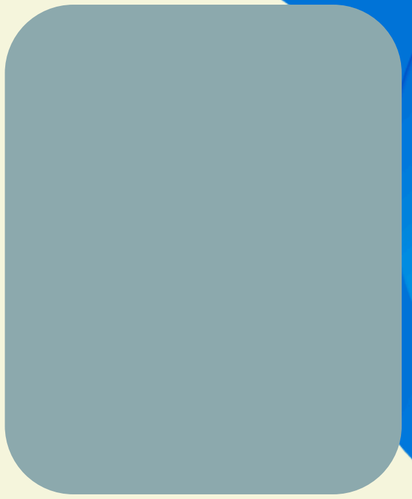


How it will work ?

How it will work ?

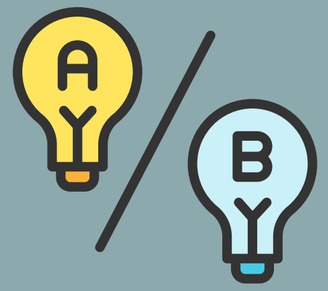


How it will work ?

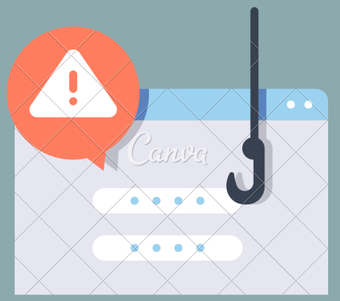

How it will work ?

Url Fetching



Comparision

SSL/TLS reading



Alert/ Pop-up

Tools And Technology Used

Tools And Technology Used

Programming Language

Api & Security Services

Development & Testing tools

Tools And Technology Used

Programming Language

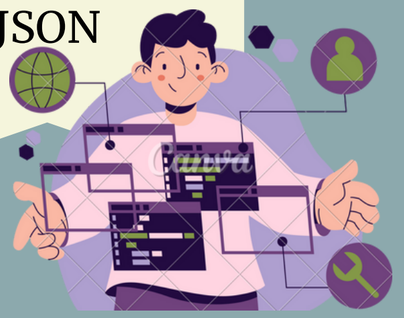
Api & Security Services

Development & Testing tools

Tools And Technology Used

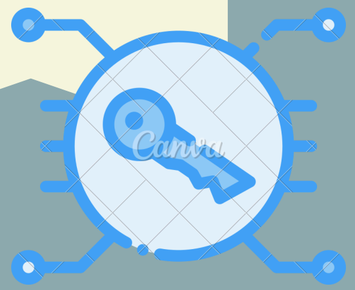
Programming Language

HTML
CSS
JAVA Script
JSON



Api & Security Services

Google Safe Browsing API
Chrome Extension API
Web Extensions API



Development & Testing tools

Visual Studio Code

Methodology

Methodology

Manifest.json

Background.js

Popup.html

Popup.css

Popup.js

Methodology

Manifest.json
For metadata of extension file.

Background.js
For background logics, events and trigger actions

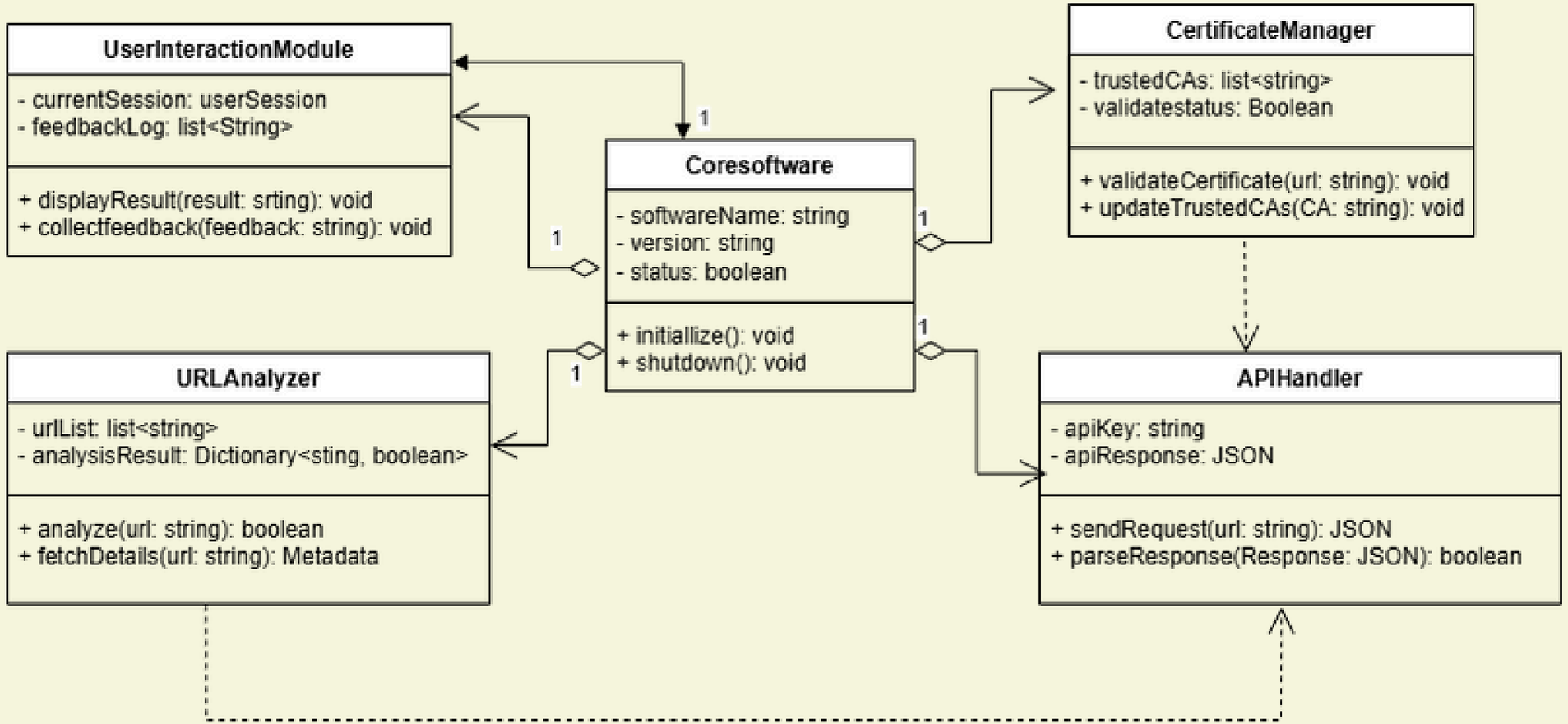
Popup.html
For pop up layout and structure

Popup.css
For visual appearance and style of popup

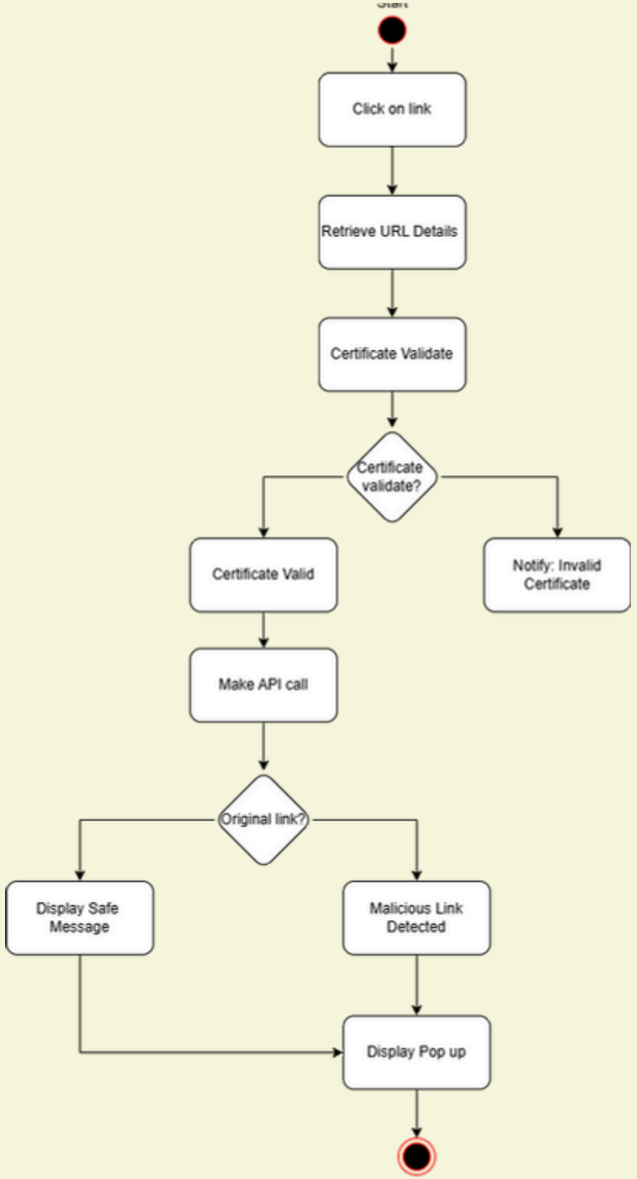
Popup.js
For handling user interaction with popup

Diagrams

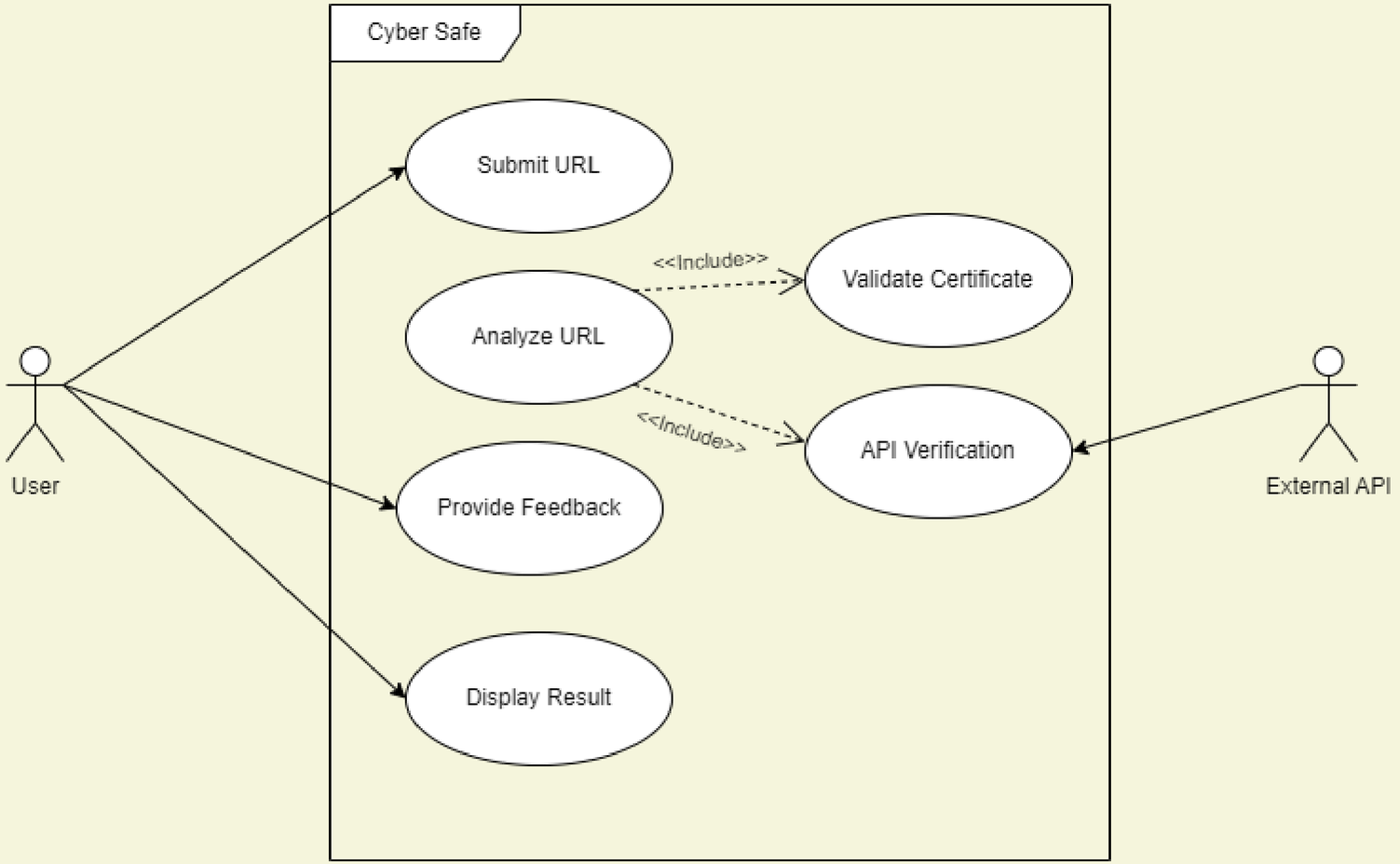
Class Diagram



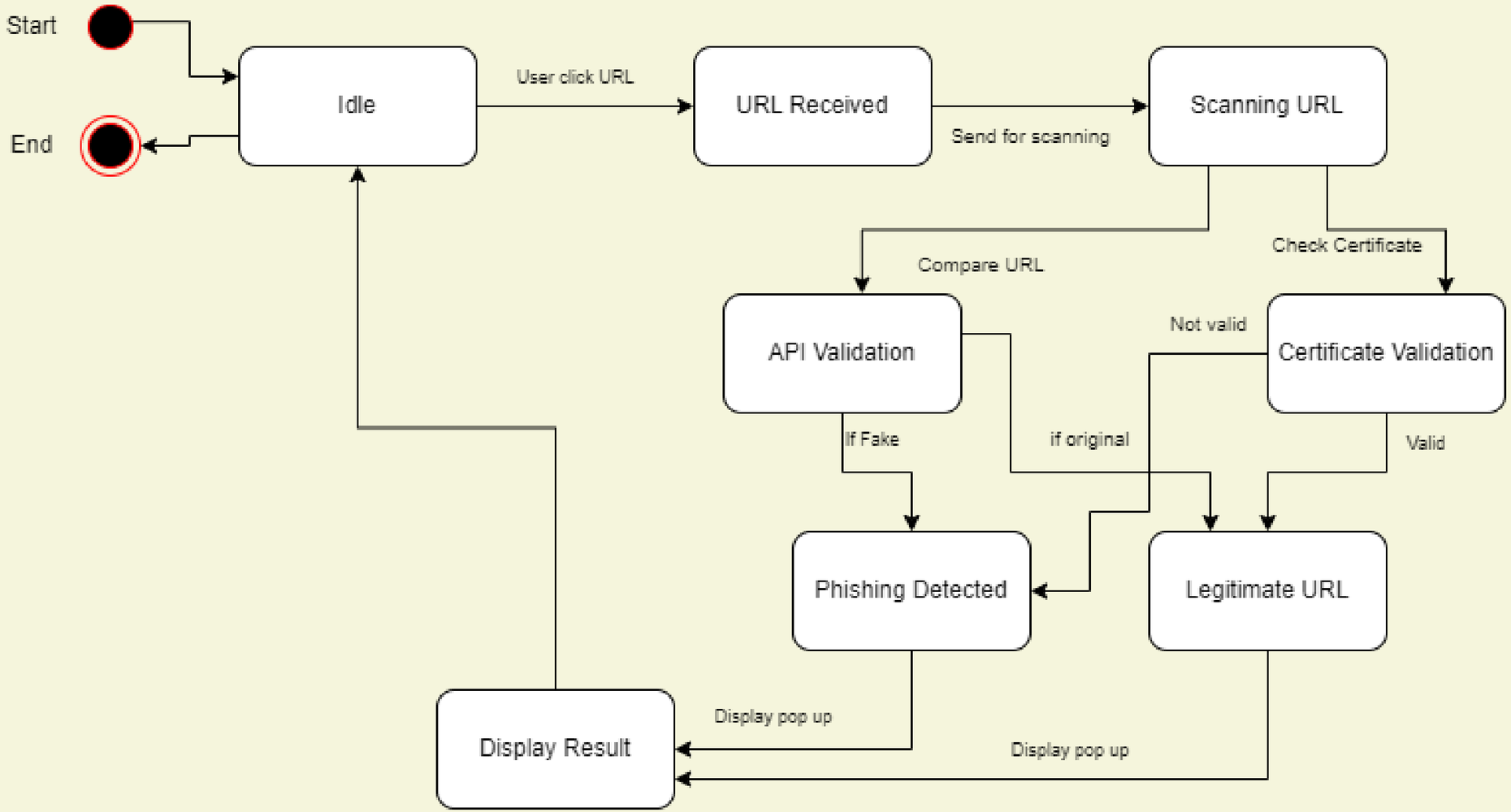
Activity Diagram



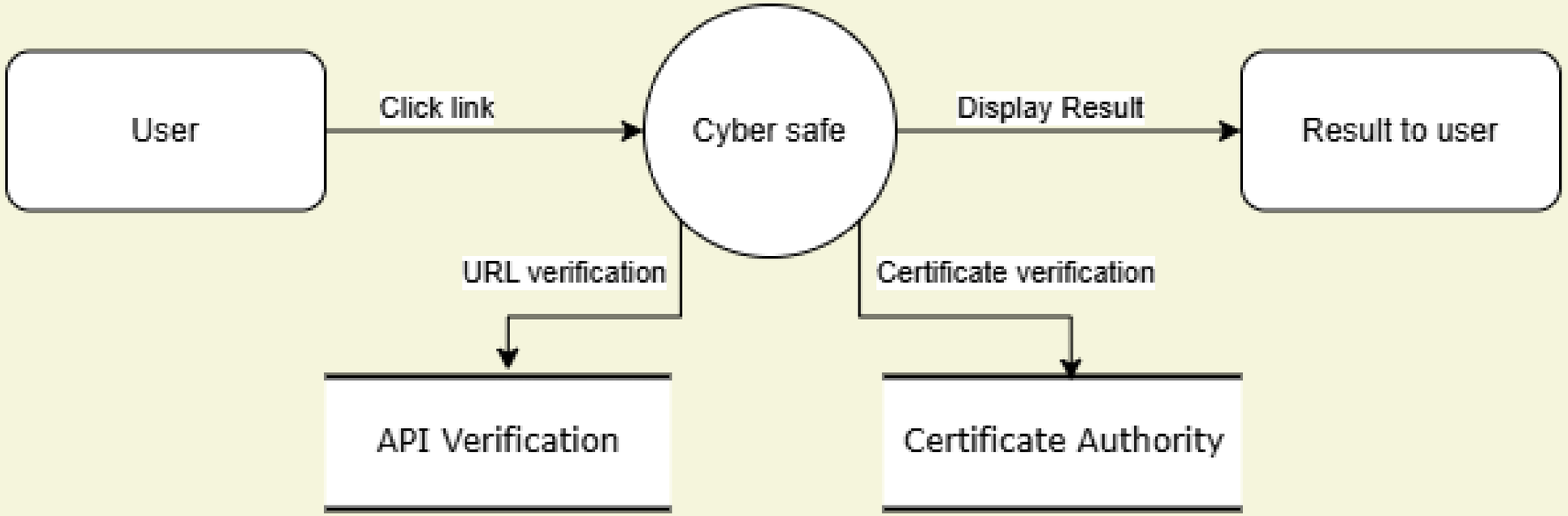
Use-CaseDiagram

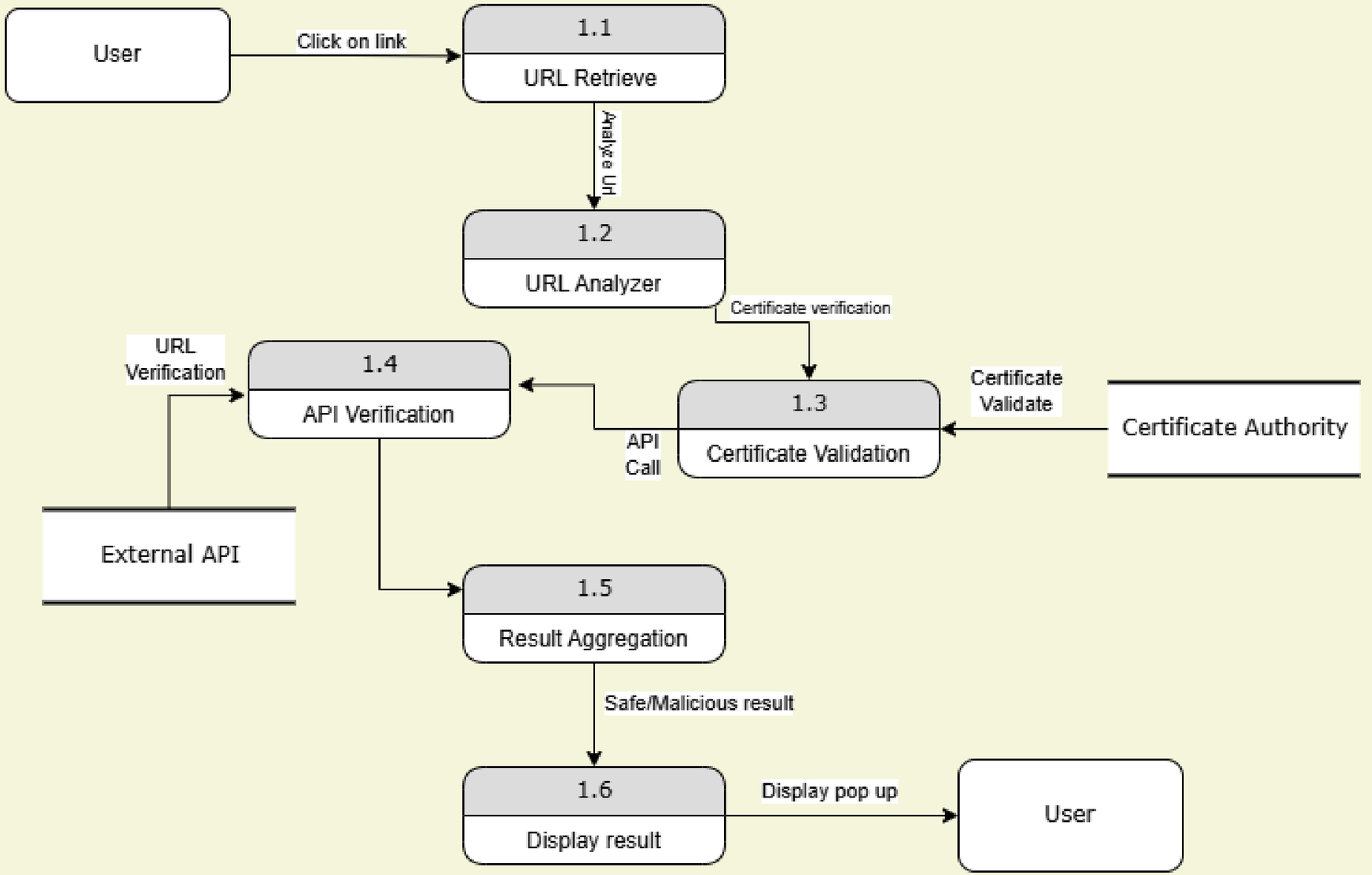


State Diagram

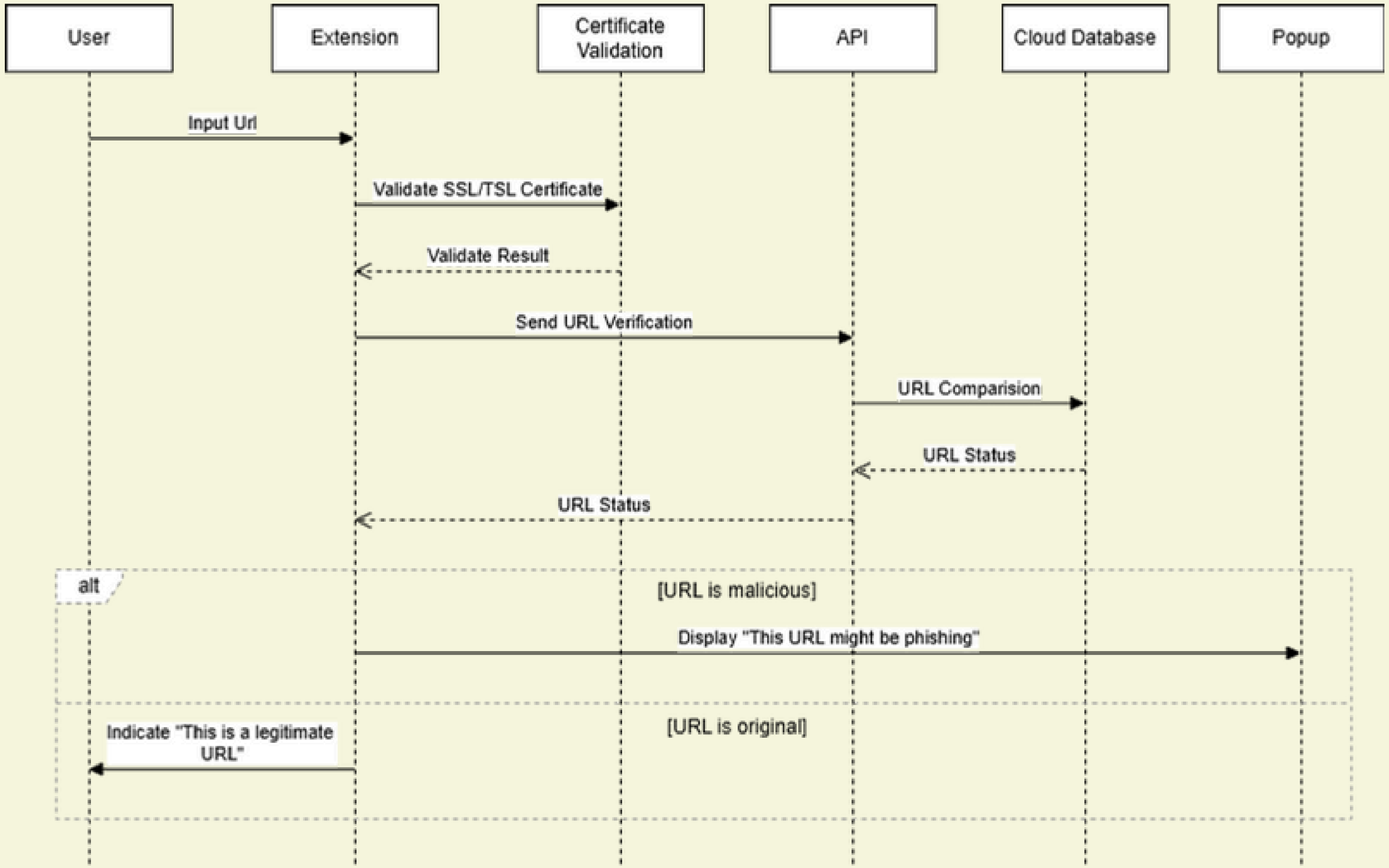


Data flow Diagram




User
Click on link
1.1
URL Retrieve
Analyze Url
1.2
URL Analyzer
Certificate verification
URL
Verification
1.4
API Verification
1.3
Certificate Validation
Certificate
Validate
Certificate Authority
API
Call
External API
1.5
Result Aggregation
Safe/Malicious result
1.6
Display result
Display pop up
User

Sequence Diagram



Challenges Faced

Challenges Faced

Challenges

Solutions

Challenges Faced

Challenges	Solutions
Verifying SSL/TLS certificates for phishing sites that may use valid certificates.	Implement additional validation checks such as analyzing the certificate issuer, domain age, and certificate revocation status.
Ensuring compatibility across multiple browsers.	Develop the extension using cross-browser frameworks like WebExtension API to ensure seamless functionality on Chrome, Firefox, and Edge.
Accurate detection of phishing websites without generating false positives.	Integrate the Google Safe Browsing API for reliable real-time URL analysis and regularly update the API key to ensure up-to-date threat detection.

Difference Between

Difference Between

Features	Cyber Safe	Other extension

Difference Between

Features	Cyber Safe	Other extension
Uses Google Safe Browsing API for real-time threat detection		
Checks SSL/TLS certificate validity		
Provides instant pop-up alerts for phishing sites		
User-friendly interface with clear security warnings		
Cross-browser compatibility (Chrome, Firefox, Edge, etc.)		
Optimized API calls to reduce response time		

Difference Between

Features	Cyber Safe	Other extension
Uses Google Safe Browsing API for real-time threat detection	✅	❌
Checks SSL/TLS certificate validity		
Provides instant pop-up alerts for phishing sites		
User-friendly interface with clear security warnings		
Cross-browser compatibility (Chrome, Firefox, Edge, etc.)		
Optimized API calls to reduce response time		

Difference Between

Features	Cyber Safe	Other extension
Uses Google Safe Browsing API for real-time threat detection	✅	❌
Checks SSL/TLS certificate validity	✅	❌
Provides instant pop-up alerts for phishing sites		
User-friendly interface with clear security warnings		
Cross-browser compatibility (Chrome, Firefox, Edge, etc.)		
Optimized API calls to reduce response time		

Difference Between

Features	Cyber Safe	Other extension
Uses Google Safe Browsing API for real-time threat detection	✅	❌
Checks SSL/TLS certificate validity	✅	❌
Provides instant pop-up alerts for phishing sites	✅	❌
User-friendly interface with clear security warnings		
Cross-browser compatibility (Chrome, Firefox, Edge, etc.)		
Optimized API calls to reduce response time		

Difference Between

Features	Cyber Safe	Other extension
Uses Google Safe Browsing API for real-time threat detection	✓	✗
Checks SSL/TLS certificate validity	✓	✗
Provides instant pop-up alerts for phishing sites	✓	✗
User-friendly interface with clear security warnings	✓	✗
Cross-browser compatibility (Chrome, Firefox, Edge, etc.)		
Optimized API calls to reduce response time		

Difference Between

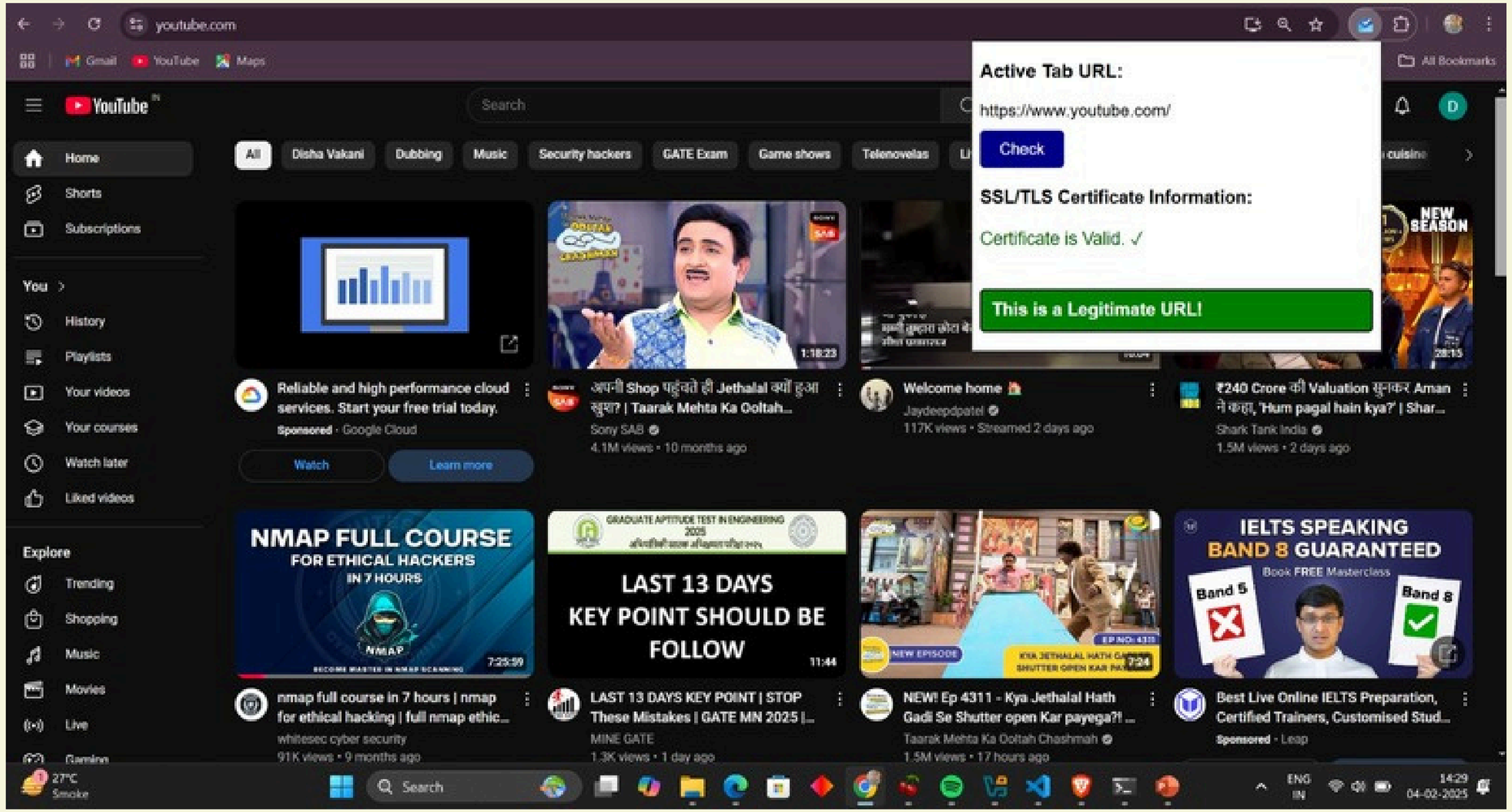
Features	Cyber Safe	Other extension
Uses Google Safe Browsing API for real-time threat detection	✓	✗
Checks SSL/TLS certificate validity	✓	✗
Provides instant pop-up alerts for phishing sites	✓	✗
User-friendly interface with clear security warnings	✓	✗
Cross-browser compatibility (Chrome, Firefox, Edge, etc.)	✓	✗
Optimized API calls to reduce response time		

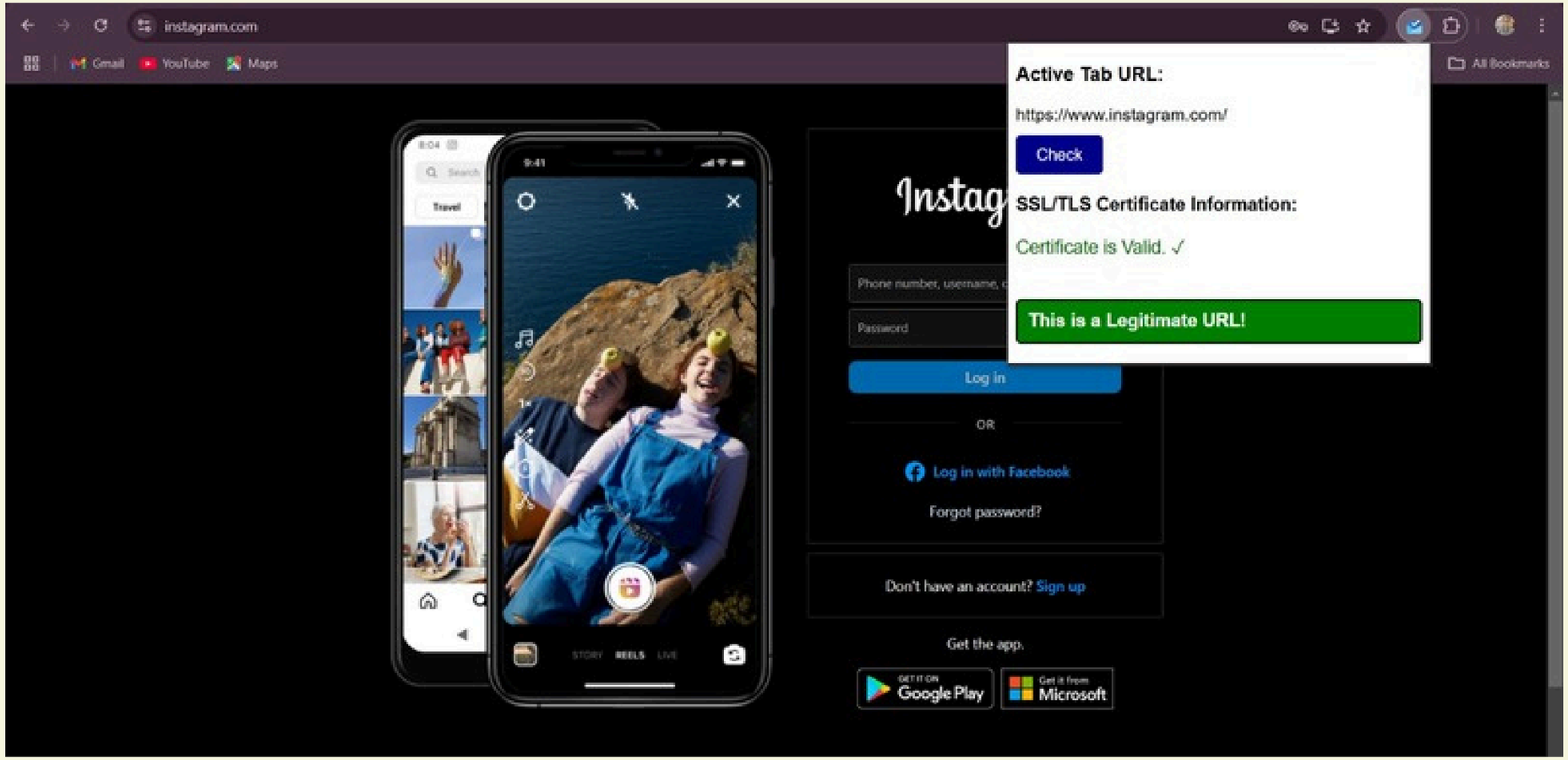
Difference Between

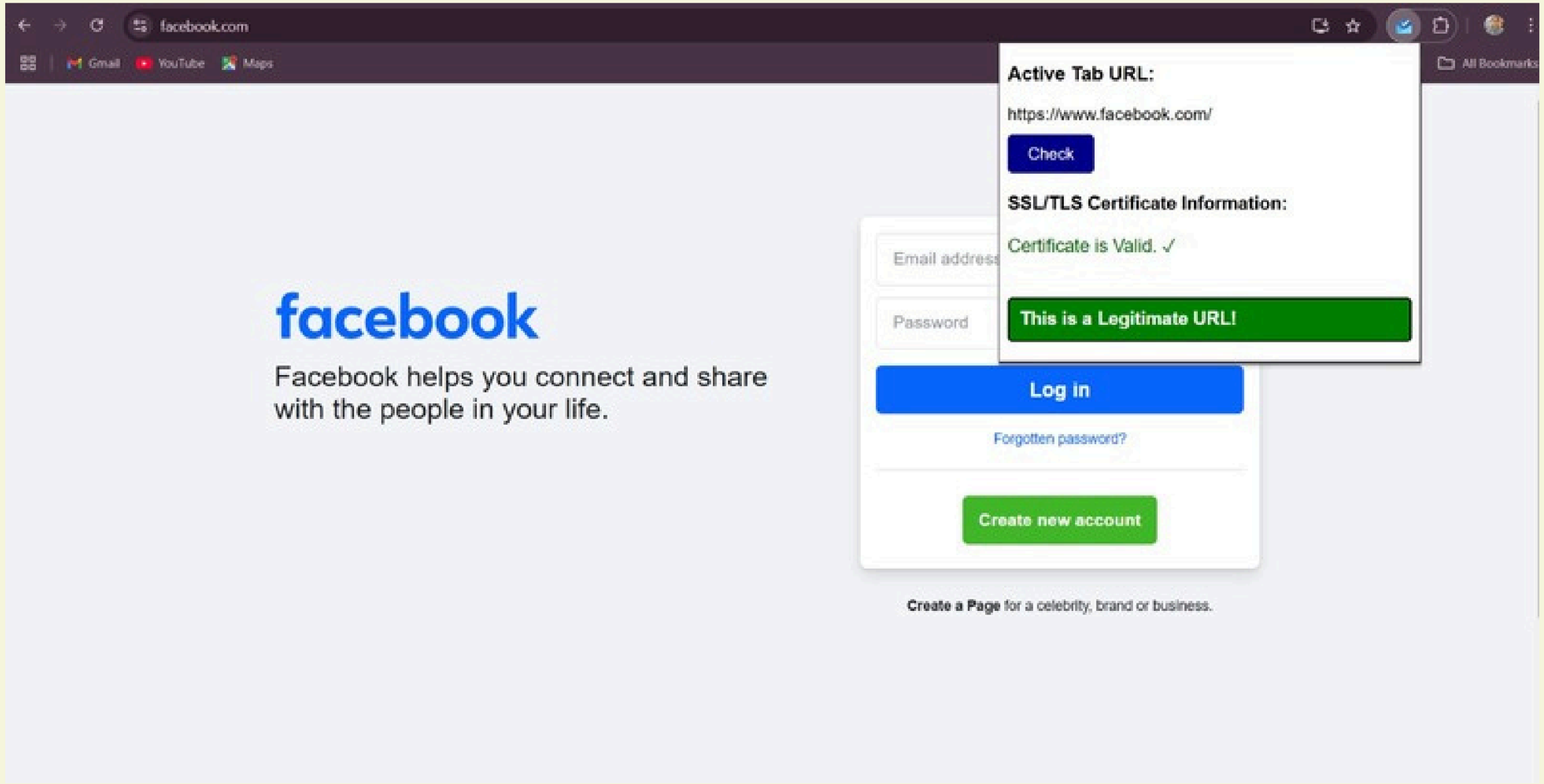
Features	Cyber Safe	Other extension
Uses Google Safe Browsing API for real-time threat detection	✓	✗
Checks SSL/TLS certificate validity	✓	✗
Provides instant pop-up alerts for phishing sites	✓	✗
User-friendly interface with clear security warnings	✓	✗
Cross-browser compatibility (Chrome, Firefox, Edge, etc.)	✓	✗
Optimized API calls to reduce response time	✓	✗

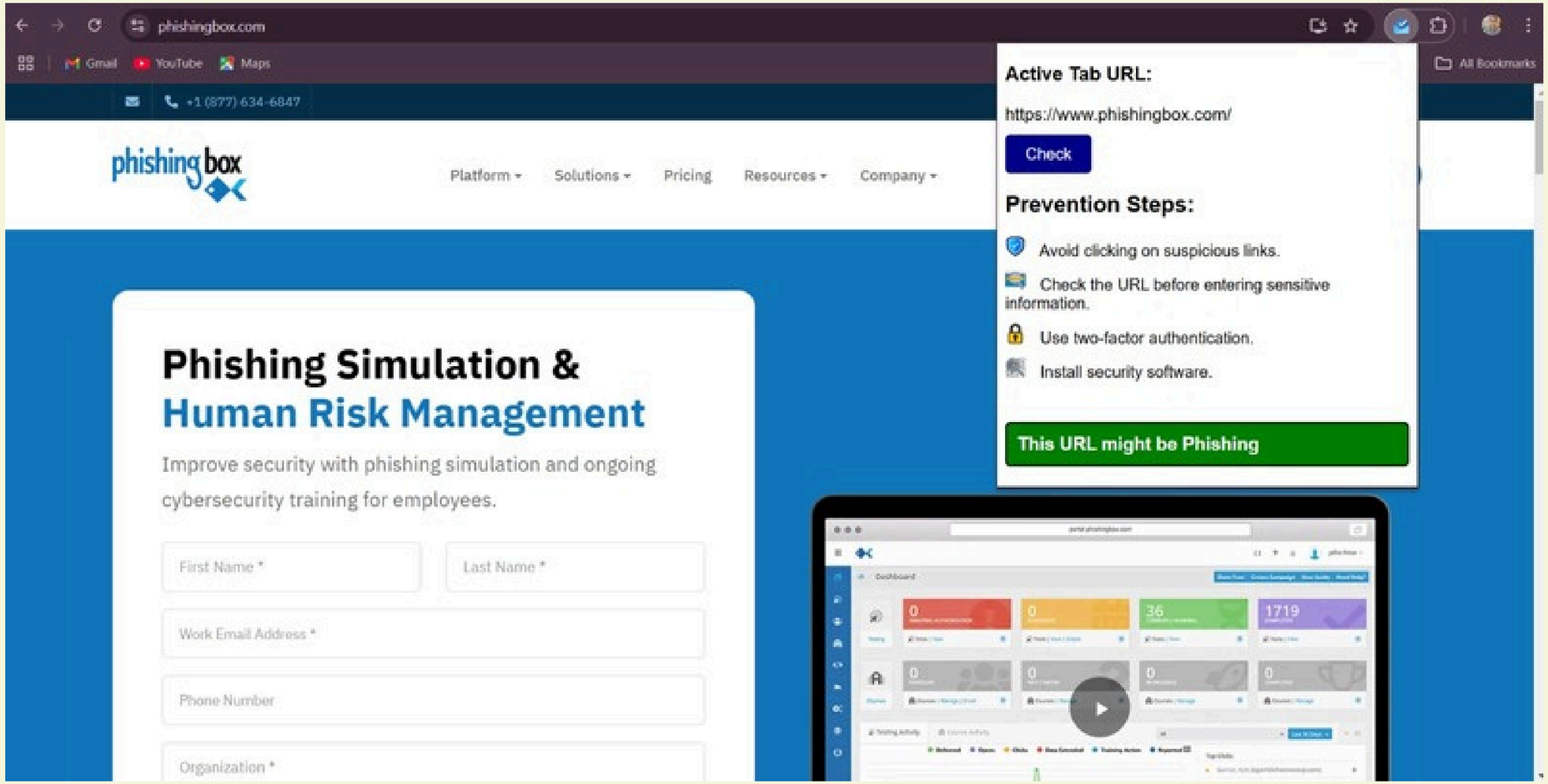
Live Demo

Snap shots


youtube.com
Active Tab URL:
https://www.youtube.com/
Check
SSL/TLS Certificate Information:
Certificate is Valid. ✓
This is a Legitimate URL!
YouTube
Search
Home
Shorts
Subscriptions
You
History
Playlists
Your videos
Your courses
Watch later
Liked videos
Explore
Trending
Shopping
Music
Movies
Live
All
Disha Vakani
Dubbing
Music
Security hackers
GATE Exam
Game shows
Telenovelas
Reliable and high performance cloud services. Start your free trial today.
Sponsored · Google Cloud
Watch
Learn more
अपनी Shop पहुंचते ही Jethalal क्यों हुआ खुश? | Taarak Mehta Ka Ooltah...
Sony SAB
4.1M views • 10 months ago
Welcome home
Jaydeepdpatel
117K views • Streamed 2 days ago
₹240 Crore की Valuation सुनकर Aman ने कहा, 'Hum pagal hain kya?' | Shar...
Shark Tank India
1.5M views • 2 days ago
NMAP FULL COURSE
FOR ETHICAL HACKERS
IN 7 HOURS
nmap full course in 7 hours | nmap for ethical hacking | full nmap ethic...
whitesec cyber security
91K views • 9 months ago
LAST 13 DAYS
KEY POINT SHOULD BE
FOLLOW
LAST 13 DAYS KEY POINT | STOP These Mistakes | GATE MN 2025 |...
MINE GATE
1.3K views • 1 day ago
NEW EPISODE
NEW! Ep 4311 - Kya Jethalal Hath Gadi Se Shutter open Kar payega?! ...
Taarak Mehta Ka Ooltah Chashmah
1.5M views • 17 hours ago
IELTS SPEAKING
BAND 8 GUARANTEED
Book FREE Masterclass
Band 5
Band 8
Best Live Online IELTS Preparation, Certified Trainers, Customised Stud...
Sponsored · Leap
27°C
Smoke
Search
ENG
IN
14:29
04-02-2025


instagram.com
Gmail
YouTube
Maps
All Bookmarks
Active Tab URL:
https://www.instagram.com/
Check
SSL/TLS Certificate Information:
Certificate is Valid. ✓
This is a Legitimate URL!
Travel
Phone number, username,
Password
Log in
OR
Log in with Facebook
Forgot password?
Don't have an account? Sign up
Get the app.
GET IT ON Google Play
Get it from Microsoft
STORY
REELS
LIVE


facebook.com
Gmail
YouTube
Maps
All Bookmarks
Active Tab URL:
https://www.facebook.com/
Check
SSL/TLS Certificate Information:
Certificate is Valid. ✓
This is a Legitimate URL!
facebook
Facebook helps you connect and share with the people in your life.
Email address
Password
Log in
Forgotten password?
Create new account
Create a Page for a celebrity, brand or business.


phishingbox.com
Gmail
YouTube
Maps
All Bookmarks
+1 (877) 634-6847
phishingbox
Platform
Solutions
Pricing
Resources
Company
Active Tab URL:
https://www.phishingbox.com/
Check
Prevention Steps:
Avoid clicking on suspicious links.
Check the URL before entering sensitive information.
Use two-factor authentication.
Install security software.
This URL might be Phishing
Phishing Simulation &
Human Risk Management
Improve security with phishing simulation and ongoing cybersecurity training for employees.
First Name *
Last Name *
Work Email Address *
Phone Number
Organization *

Future Work

Machine Learning Integration:

Feature:
Integrate machine learning models to analyze URL patterns and detect phishing attempts more accurately.

Why:
Machine learning can adapt to evolving phishing tactics, offering smarter and more effective threat detection.

Mobile Compatibility:

Feature:
Develop a mobile version of the extension to provide real-time phishing protection on smartphones and tablets.

Why:
Since many phishing attempts now target mobile users, extending protection to mobile devices ensures a safer browsing experience everywhere.

Future Work

User Reporting Feature:

Feature:
Add a user-friendly reporting option that allows users to flag suspicious websites directly from the extension.

Why:
Crowdsourced reports can help identify new threats faster, making the detection system smarter and more responsive.

Detailed Analytics Dashboard:

Feature:
Create an admin dashboard that visualizes data from the Google Safe Browsing API, including flagged URLs, detection trends, and user reports.

Why:
This helps administrators monitor phishing activity, measure the extension’s performance, and make data-driven improvements.

Future Work

Continuous Updates:

Feature:
Regularly update the extension to optimize its API integration, improve the user experience, and stay compatible with browser updates.

Why:
Consistent updates ensure the extension remains effective against the latest phishing tactics and maintains seamless performance.

Conclusion

The Cyber Safe browser extension provides a reliable and proactive solution to combat phishing attacks by integrating the Google Safe Browsing API for real-time URL analysis and SSL/TLS certificate verification. With its user-friendly interface, instant alerts, and actionable prevention tips, it enhances online safety for users.

Future developments like mobile compatibility, machine learning integration, user reporting features, and a detailed analytics dashboard will further strengthen its capabilities. Continuous updates will ensure it remains effective against evolving phishing threats.

By offering robust protection and increasing user awareness, Cyber Safe contributes to a safer and more secure browsing experience.

Reference

- Frauenstein, E. D., & Flowerday, S. V. (2016). Social network phishing: Becoming habituated to clicks and ignorant to threats? 2016 Information Security for South Africa (ISSA), Johannesburg, South Africa. **DOI: 10.1109/ISSA.2016.7802935**
- Seng, S., Al-Ameen, M. N., & Wright, M. (2017). Understanding Users' Decision of Clicking on Posts in Facebook with Implications for Phishing. Rochester Institute of Technology and Clemson University.
- Google. (n.d.). Google Safe Browsing API Documentation. Retrieved from **https://developers.google.com/safe-browsing**
- Zhang, Y., Hong, J. I., & Cranor, L. F. (2007). Cantina: A content-based approach to detecting phishing web sites. Proceedings of the 16th International Conference on World Wide Web, 639-648. **DOI: 10.1145/1242572.1242659**

Any Question ?

Thank you