# Phishing Link Scanner Report

By Shivam Chauhan

## Introduction

In today's digital world, malicious websites are a major threat. Hackers often disguise phishing websites as legitimate platforms to steal sensitive information. This URL Security Scanner is designed to help users detect potential phishing, suspicious, or malicious websites before they interact with them.

This program was developed using Python and utilizes the following technologies:
- Regular Expressions (re) for pattern matching
- Requests library for API calls
- urllib for URL parsing
- VirusTotal API for reputation analysis

## This program performs three key security checks to analyze a URL:

1. Blacklist Check – Determines if the URL belongs to a known phishing or malware site.

2. Suspicious Keyword Detection – Scans the URL for words commonly used in phishing attacks.

3. VirusTotal Reputation Analysis – Uses the VirusTotal API to check if security vendors have flagged the URL.

## How It Works

Step 1: User Input – The program prompts the user to enter a URL.

Step 2: Blacklist Verification – The URL is compared against a list of known phishing and malicious domains.

Step 3: Suspicious Keyword Detection – The script scans for high-risk words like 'login', 'bank', 'verify', and 'security'.

Step 4: VirusTotal API Reputation Check – The URL is submitted to VirusTotal for a security scan.

Step 5: Final Report – The results are displayed in a clear, human-readable format.

## Sample URL Scans & Results

### Example 1: Safe Website

User Input: https://example.com

Result: URL Analysis Result: Safe (No detections)

Conclusion: This website is clean and has no reported threats.

### Example 2: Suspicious URL

User Input: https://login-secure.com

Result: The URL contains suspicious keywords!

Why is it suspicious?

- The URL includes 'login' and 'secure', which are commonly used in phishing attacks.

Advice: Proceed with caution. Double-check if the website is legitimate.

### Example 3: Blacklisted Website

User Input: http://phishingsite.net/reset-password

Result: The URL is in a known phishing blacklist!

Why is it dangerous?

- This website has been previously reported as a phishing or malware site.

Advice: Do NOT click on this link—it's unsafe.

### Example 4: VirusTotal Detection

User Input: https://banksecure-update.com

Result: URL Analysis Result: Potentially Malicious (3 security vendors flagged this site)

Why is it dangerous?

- Three independent security vendors have reported this URL as unsafe.

Advice: Avoid this website at all costs!

## Key Features & Enhancements

• Blacklist Integration – Blocks access to known phishing/malware sites.

• Keyword Detection – Identifies URLs with phishing-related words.

• VirusTotal API Check – Provides real-time threat analysis.

• User-Friendly Results – Displays results in a clear, easy-to-understand format.

• Error Handling – Prevents crashes in case of API failures or bad input.

## Future Improvements

• Expanded Blacklist Database – Automatically update the blacklist with real-time threat intelligence.

• Bulk URL Scanning – Allow users to check multiple URLs at once.

• Graphical Interface (GUI) – Convert the script into an easy-to-use application.

• Multi-API Integration – Use Google Safe Browsing API and PhishTank API for even better detection.

## Final Thoughts

This URL Security Scanner is a powerful and effective tool to detect potential threats before you interact with a suspicious link. By combining static analysis (blacklist & keyword detection) with real-time scanning (VirusTotal API), this script provides a reliable security check for any website.

Stay safe online, and always verify URLs before clicking!