# Task 2: Phishing Website and Email Analysis

Name: Posaram Dewasi

Email: posurabari95@gmail.com

Date: 05 Aug 2025

Github Link = https://github.com/posurabari/nmap-network-scan-task/upload/main/Task-2

## Introduction

This report presents the analysis of a phishing website and a fake phishing email. The goal is to understand how phishing attacks work, how they lure users into clicking malicious links, and how to identify such emails using tools.

## 1. Collected Phishing URL

Phishing URL used for this task:

http://allegrolokalnie.pl-oferta5208251.icu

Note: This URL was taken from a public phishing link database for educational analysis only.

## 2. Analysis Using Online Tools

The phishing link was scanned using online tools like VirusTotal and URLVoid. Below are the observations based on the results (screenshots of actual results should be attached):

- VirusTotal: Detected as a phishing/malicious site.

- URLVoid: Listed as suspicious by multiple scanning engines.

## 3. Fake Phishing Email Sample

**From: support123@allegro.com  
To: posaram123@gmail.com  
Subject: Action Required: Your Allegro Account is Suspended  
  
Dear Allegro User,  
  
We have detected suspicious activity in your Allegro account.  
Please verify your identity by clicking the link below:  
  
 https://allegro-login-update.vercel.app  
  
If you do not verify within 24 hours, your account will be suspended permanently.  
Thank you,  
Allegro Security Team**

## 4. Email Header Analysis

A fake email header was analyzed using Google's message header analyzer tool. The analysis helps trace the origin of the email and detect suspicious routing.

Sample Header:

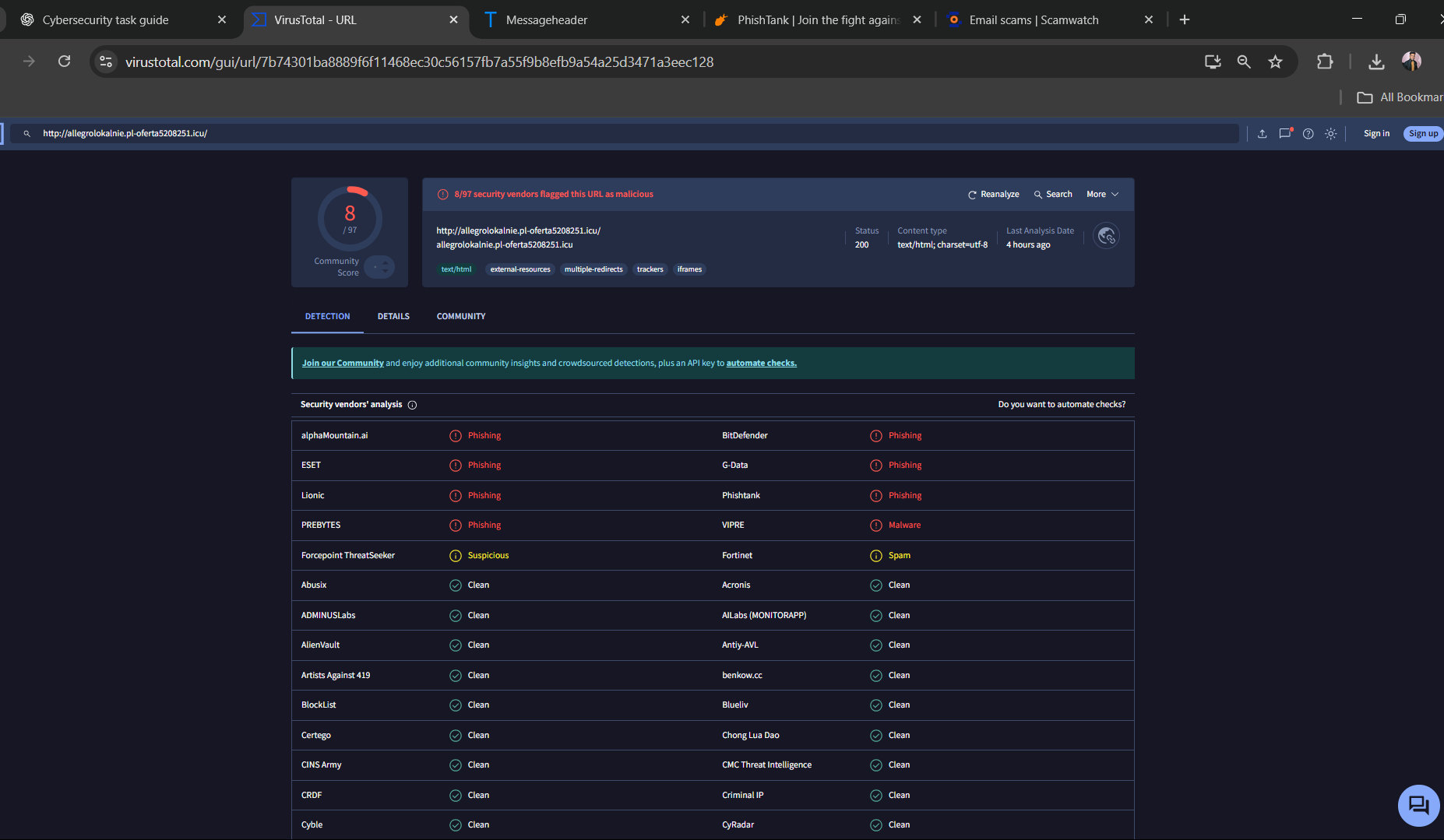
**Return-Path: <support123@allegro.com>  
Received: from suspiciousdomain.com (unknown [123.45.67.89])  
 by mail.example.com (Postfix) with ESMTP id A1B2C3D4  
 for <posaram123@gmail.com>; Mon, 05 Aug 2025 10:00:00 +0000 (UTC)  
Subject: Urgent Allegro Account Verification Needed  
From: Allegro Support <support123@allegro.com>  
To: posaram123@gmail.com**

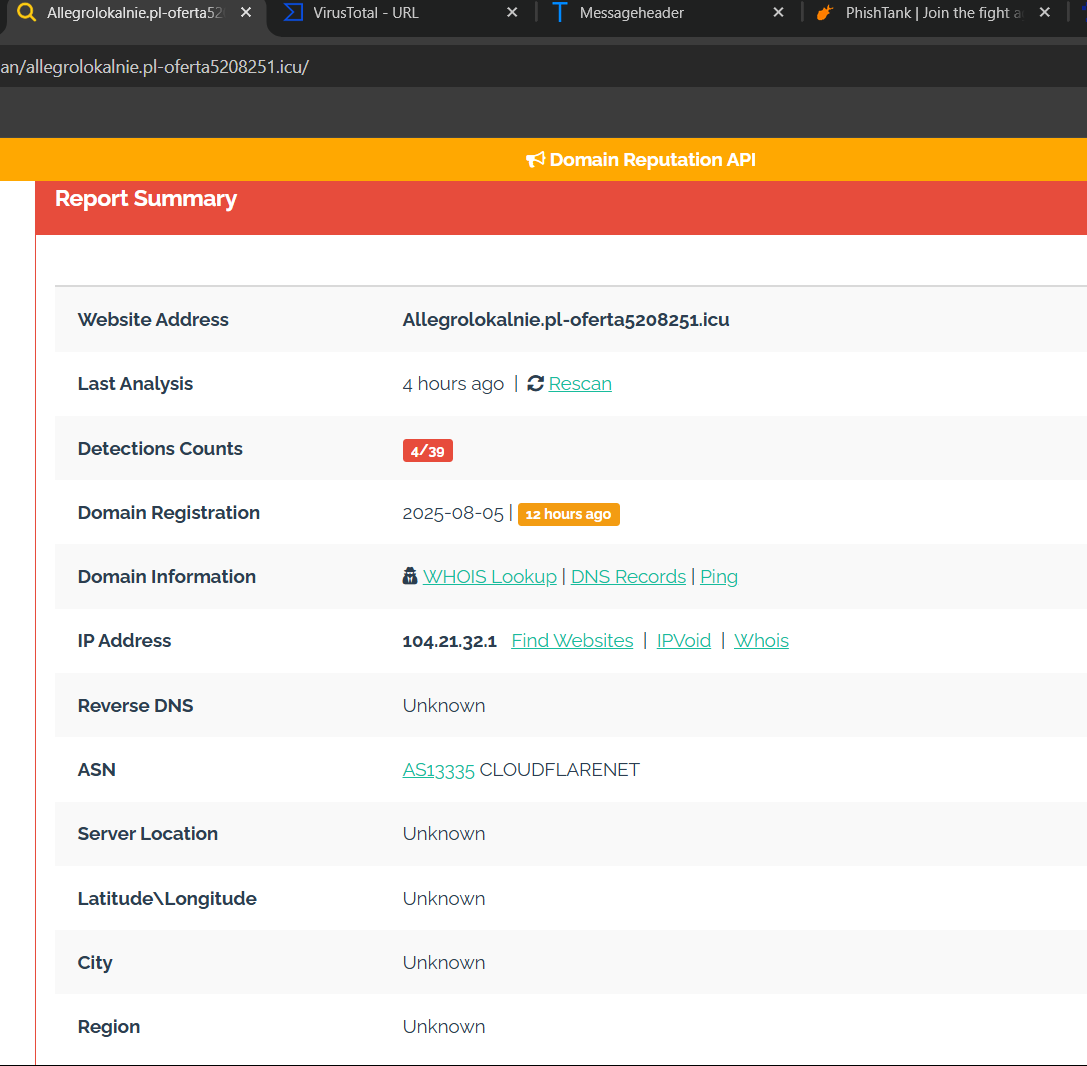
The header shows that the email originated from a suspicious domain and is likely spoofed.

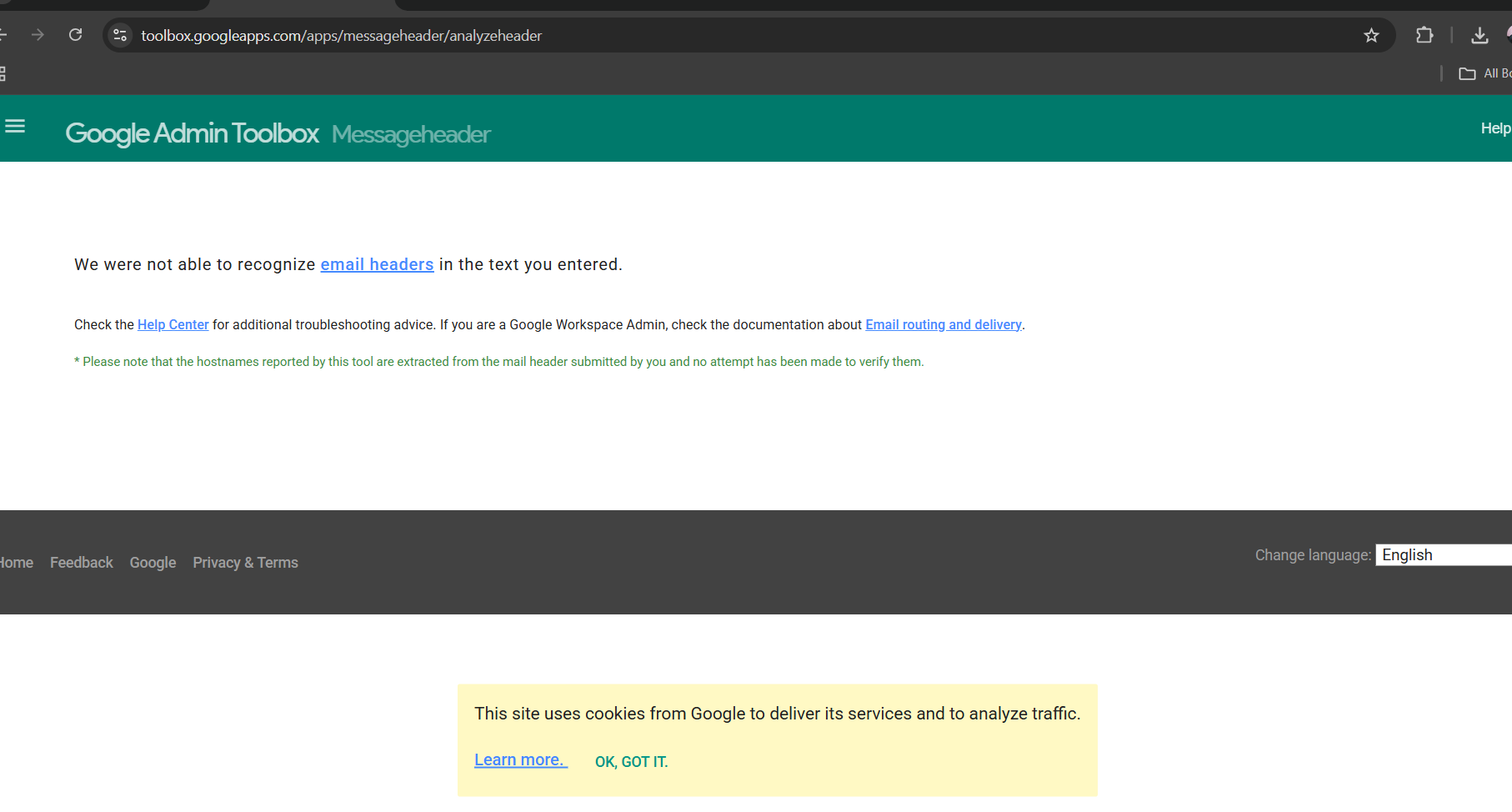
## 5. Conclusion

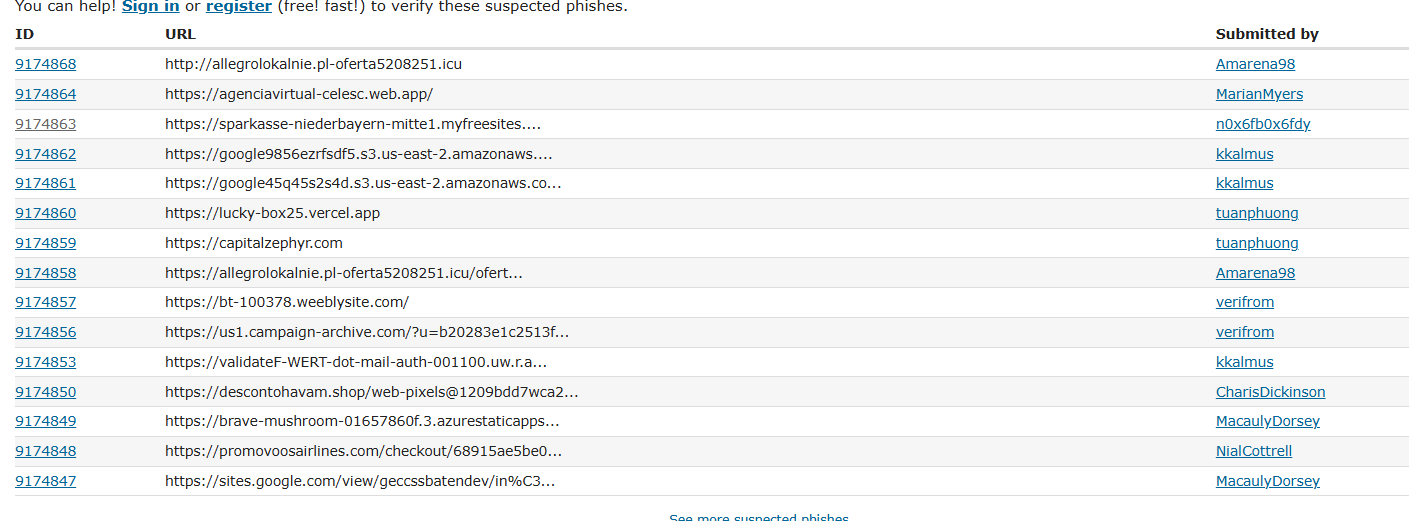
This analysis demonstrates the key components of phishing attacks and how to identify them. Using tools like VirusTotal, URLVoid, and email header analyzers, we can detect phishing websites and spoofed emails. It is crucial to avoid clicking on suspicious links and to verify the authenticity of emails from unknown sources.

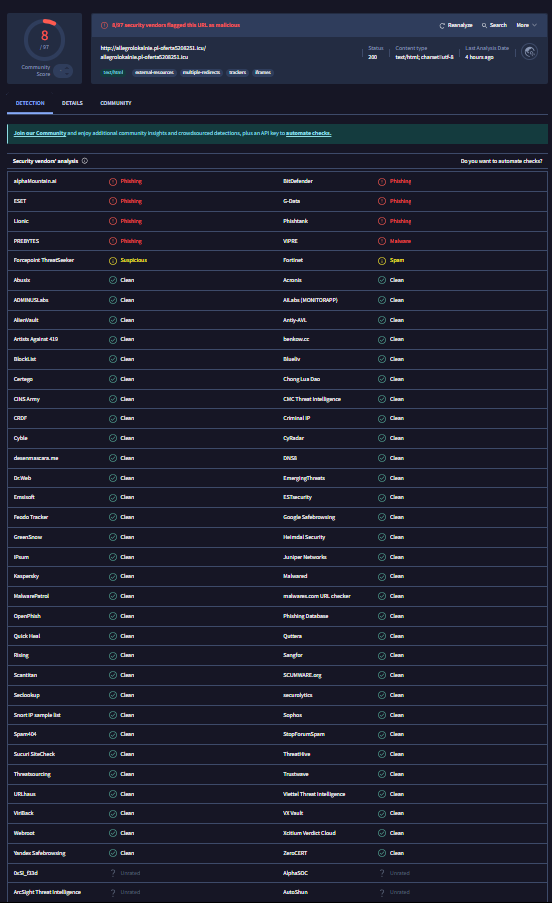
**6. Screenshot:-**

****

****

****

****

****