

# **Phishing Email Analysis Report**

**Prepared By: Dennis Gilbert**

**Date: April 10, 2025**

## Table Of Content

Executive Summary .....	3
Tools Used .....	4
Email.....	5
Email Metadata analysis .....	6
URL Analysis.....	7
Key Indicators of Phishing.....	9
Recommendations.....	10
Conclusion.....	11

## **Executive Summary**

This report summarizes the analysis of phishing emails to identify common tactics and assess threat levels. URLs were examined using tools like Symantec Bluecoat, URLScan.io, and VirusTotal, to detect malicious links. Email headers were analyzed for anomalies, including weak or missing SPF records, mismatched return and "From" addresses, and suspicious sender IPs checked via AbuseIPDB.

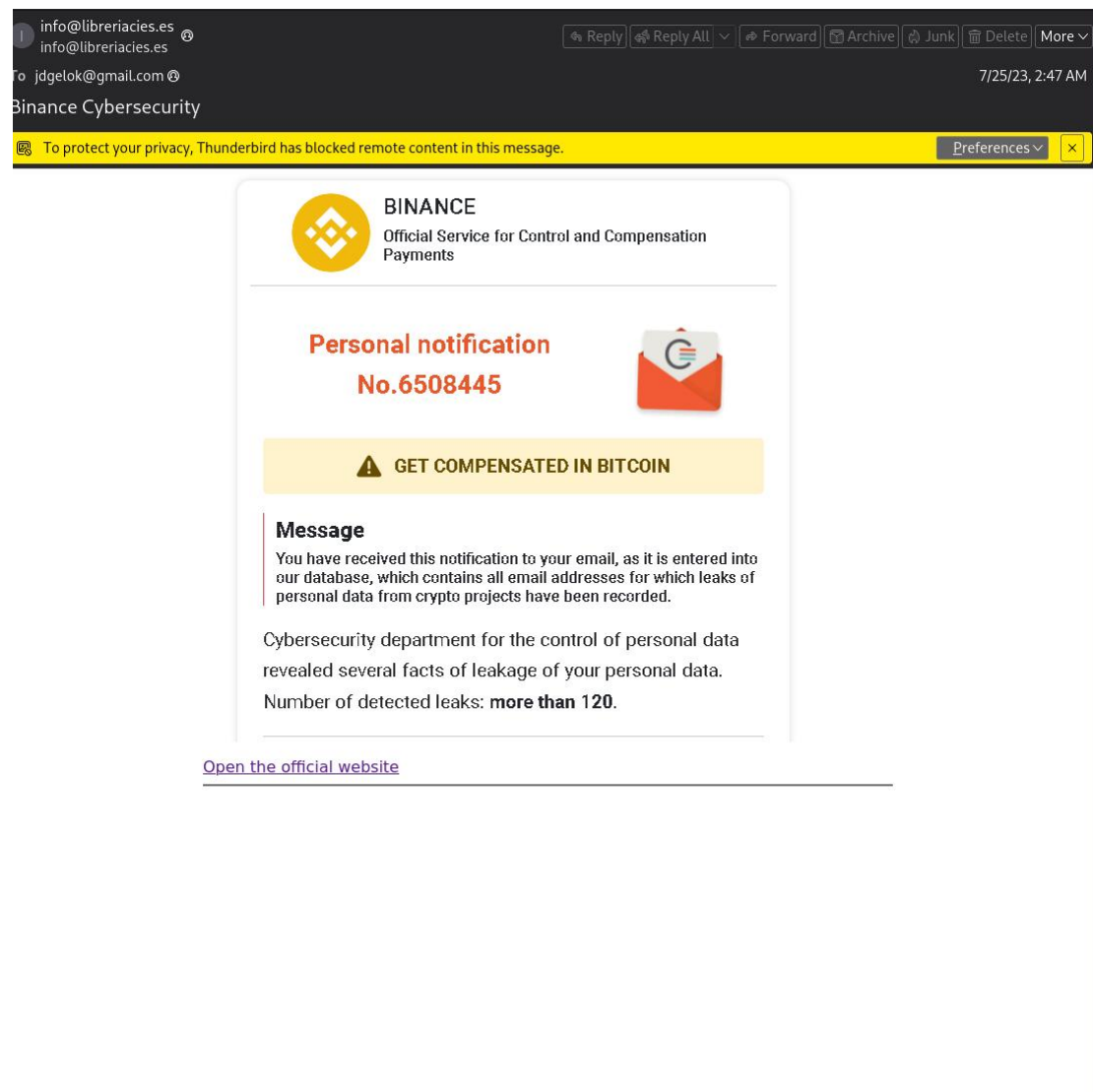
The findings highlight key indicators of phishing and reinforce the importance of thorough email analysis and security awareness.

## **Tools Used**

- **Symantec Bluecoat** – for checking domain categorization and reputation.
- **URLScan.io** – to visualize how the link behaves when accessed.
- **VirusTotal** – for scanning the URL across multiple antivirus engines.
- **AbuseIPDB** – to check sender IP reputation.
- **SPF Record Lookup Tools** – to check domain authentication.

# Email

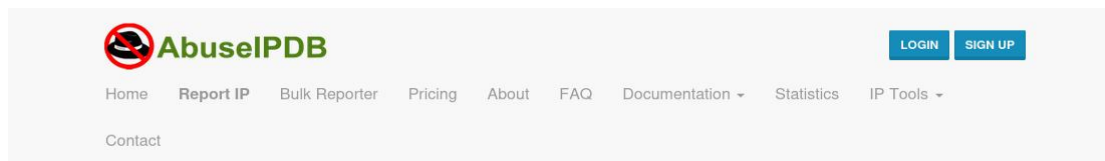
This is the email that will be analyzed



## Email Metadata Analysis

### Sender Information:

- Return Path Vs From: The Return Path is [info@libreriacies.es](mailto:info@libreriacies.es) while it was from PH0PR19MB5396.namprd19.prod.outlook.com(::1). This indicates spoofing.
- SPF Record: Set to “none” which means no authentication is present.
- Sender IP Address: 217.18.161.43. From the scan on AbuseIPDB, it shows that the sender’s IP address has been reported a total of 3 times from 2 distinct sources. It was reported under the following categories; Brute-Force, Phishing and Email Spam.



### AbuseIPDB » 217.18.161.43

Check an IP Address, Domain Name, or Subnet  
e.g. 102.90.97.63, microsoft.com, or 5.188.10.0/24

217.18.161.43

**217.18.161.43 was found in our database!**

This IP was reported 3 times. Confidence of Abuse is 0%: ?

0%

ISP	SIAPI Networks
Usage Type	Data Center/Web Hosting/Transit
ASN	AS42220
Hostname(s)	serlogal.arnoia.com
Domain Name	siapi.es
Country	Spain
City	Granada, Andalusia

IP info including ISP, Usage Type, and Location provided by [IPInfo](#). Updated biweekly.

[REPORT 217.18.161.43](#) [WHOIS 217.18.161.43](#)

**IP Abuse Reports for 217.18.161.43:**

This IP address has been reported a total of **3** times from 2 distinct sources. 217.18.161.43 was first reported on October 11th 2021, and the most recent report was **3 years ago**.

**Old Reports:** The most recent abuse report for this IP address is from **3 years ago**. It is possible that this IP is no longer involved in abusive activities.

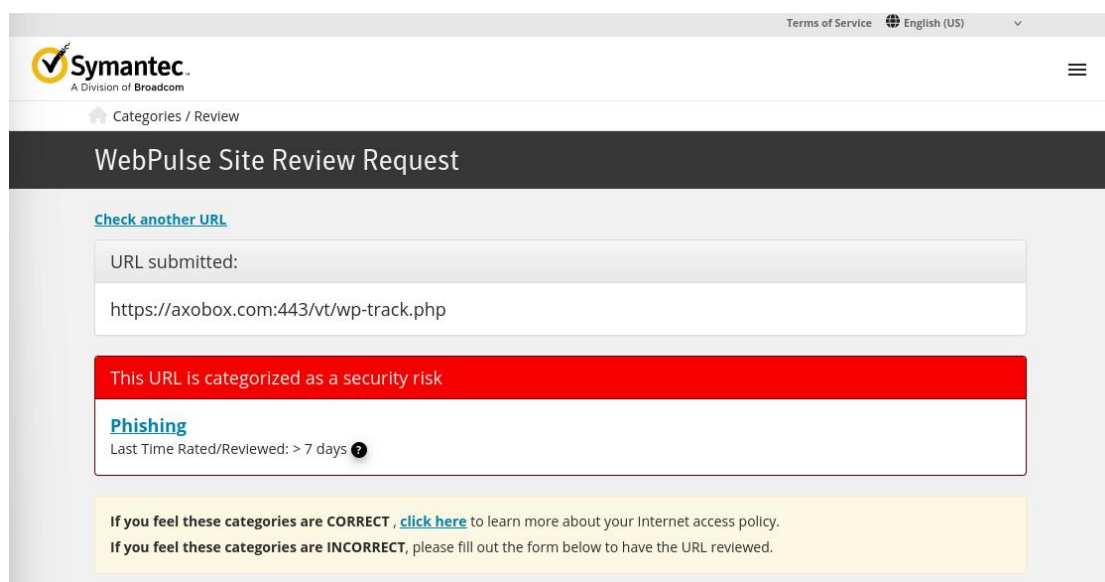
- DKIM / DMARC: Not configured and ineffective

**Conclusion:** The email header shows multiple signs of spoofing and poor sender domain security.

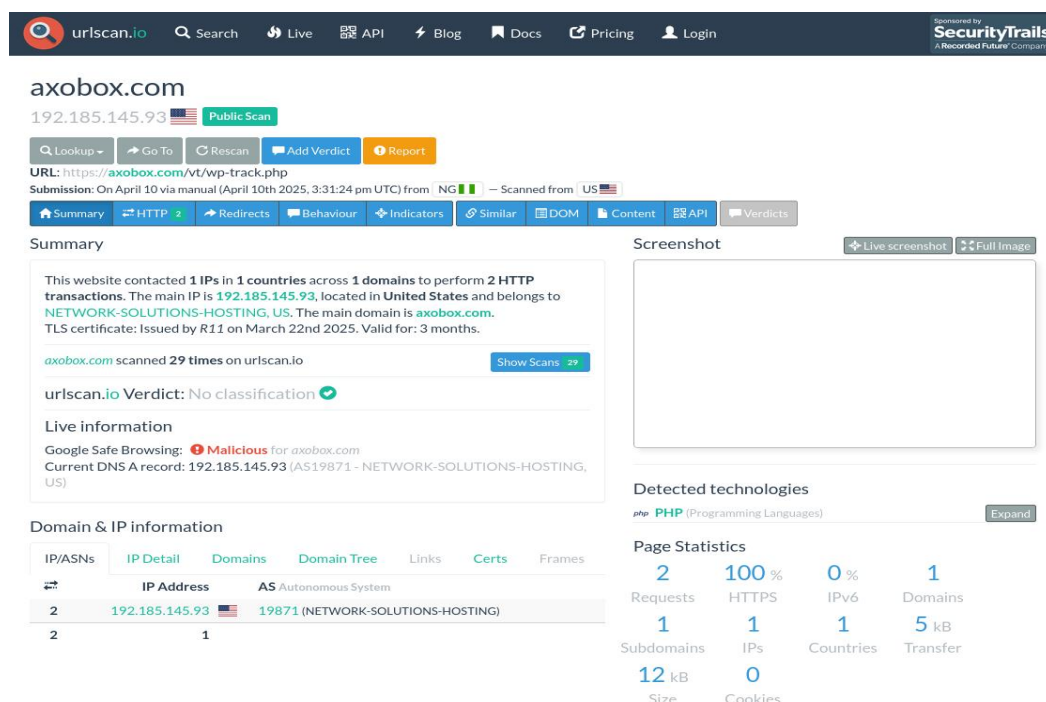
## URL Analysis

The embedded URL which is : <https://axobox.com/vt/wp-track.php> was tested using the tools listed above .

Symantec Bluecoat: This tool classified the URL as a security risk under “Phishing” category.



URLScan.io: It was classified as Malicious by Google Safe Browsing but was not given any classification by URLScan.io.



VirusTotal: 10 out of 96 security vendors flagged it as malicious.

The screenshot shows the VirusTotal analysis page for the URL `https://axobox.com/vt/wp-track.php`. The interface is dark-themed. At the top, a navigation bar includes the VirusTotal logo, a search bar, and links for 'Sign in' and 'Sign up'. Below the navigation bar, a summary section displays a 'Community Score' of 10/96, a status of 200, and a last analysis date of 1 month ago. A prominent red banner indicates that 10/96 security vendors flagged the URL as malicious. The main content area is divided into three tabs: 'DETECTION', 'DETAILS', and 'COMMUNITY'. The 'DETECTION' tab is active, showing a table of security vendors' analysis results. The table lists 20 vendors, with 10 flagged as 'Phishing' or 'Malicious' and 10 marked as 'Clean'. A 'Reanalyze' button and a 'Search' bar are located at the top right of the detection section. A 'Join our Community' banner is also visible above the table.

Security vendors' analysis		Do you want to automate checks?	
BitDefender	Phishing	CyRadar	Malicious
ESET	Phishing	Forcepoint ThreatSeeker	Phishing
Fortinet	Phishing	G-Data	Phishing
Kaspersky	Phishing	Lionic	Phishing
Sophos	Phishing	Webroot	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
benkow.cc	Clean	BlockList	Clean
Blueliv	Clean	Certego	Clean
Chong Lua Dao	Clean	CINS Army	Clean
CMC Threat Intelligence	Clean	CRDF	Clean
Criminal IP	Clean	Cyble	Clean
desenmascara.me	Clean	DNS8	Clean

**Conclusion:** The URL was clearly malicious and designed to harvest user information.



## **Key Indicators of Phishing**

- Urgent language prompting immediate response
- Email came from an unverified source pretending to be a legitimate organization.
- Technical indicators (SPF, IP, Return Path) failed verification.

## **Recommendations**

- Always verify URLs before clicking, especially those prompting login or sensitive actions.
- Enable SPF, DKIM, and DMARC on organizational domains.
- Train users to recognize phishing tactics and report suspicious emails.
- Implement IP reputation checks and enhanced spam filtering.

## **Conclusion**

The analyzed email demonstrated common phishing characteristics, including domain spoofing, malicious links, and deceptive sender metadata. With the help of security tools, this email was identified as a phishing attempt, underlining the need for continued vigilance and proper email authentication practice.

