

# Phishing Email Analysis Report

## 1. Basic Information

Analyst Name	Nizar Aderbaz
Date of Analysis	2025-08-22
Email Subject	"86RE: Donation For You"
Sender (From)	"Philip Fredrick" <ghulammustafa@cyber.net.pk>
Recipient	phishing@pot
Reported By	End user

## 2. Email Metadata Summary

Message-ID	<0bcd0f2-645d-41e8-8542-9e7541e0914a@BN1NAM02FT046.eop-nam02.prod.protection.outlook.com>
Return-Path	<a href="mailto:ghulammustafa@cyber.net.pk">ghulammustafa@cyber.net.pk</a>
Reply-To	<philipfredrick3690@gmail.com>
X-Mailer	Microsoft Outlook Express 6.00.2600.0000
Date Sent	Wed, 2 Aug 2023 19:27:50 -0700
Received	from User (unknown [147.78.103.9]) by mail.mail04.zhanlingol.com (Postfix) with SMTP id 6E01023FE574; Wed, 2 Aug 2023 19:27:40 +0000 (UTC)

## 3. Header Authentication Results

Check	Result	Notes
SPF	SOFTFAIL	The email came from an IP <b>not listed in the SPF record</b> , but the receiving server decides <b>not to reject the email outright</b> .
DKIM	NONE	Message Not Signed
DMARC	FAIL	Action = Quarantine

## 4. URL & Attachment Analysis

Type	Found	Details
URLs	✗	None
Attachments	✗	None

## 5. Technical Indicators

IP Addresses	<b>147.78.103.9</b> ( <b>Known malicious</b> , This IP has been reported a total of <b>191</b> times from <b>75</b> distinct sources on <b>AbuseIPDB</b> and <b>1</b> time on <b>VirusTotal</b> )  <b>159.27.24.86</b> ( <b>Known malicious</b> , This IP has been reported a total of <b>29</b> times from <b>18</b> distinct sources on <b>AbuseIPDB</b> and <b>1</b> time on <b>VirusTotal</b> )
Hosting Country	Bulgaria
Domain	None
Domain Age	None
WHOIS Status	None

## 6. Risk Evaluation

### 1. Sender Analysis:

- **From:** ghulammustafa@cyber.net.pk (appears legitimate, known individual)
- **Reply-To:** philipfredrick3690@gmail.com (redirects replies to attacker)
- **Risk: High** – sender address is spoofed to appear trustworthy.

### 2. Email Authentication Checks:

- **SPF:** SoftFail → email is **not sent from authorized servers** for cyber.net.pk.
- **DKIM:** None → email is **not cryptographically signed**.
- **DMARC:** Fail → domain policy failed, email is **quarantined**.
- **Risk: High** – authentication failures indicate likely spoofing.

### 3. Received Headers Analysis:

- **Bottom-most Received IP:** 147.78.103.9 → true origin of email (attacker-controlled).
- **Top-most Received IP:** 159.27.24.86 → relay server, unauthorized per SPF.
- **Risk: Medium-High** – email path shows relay through untrusted server.

### 4. From vs Reply-To Mismatch:

- **Observation:** “From” is a known individual; “Reply-To” is attacker’s Gmail.
- **Risk: High** – any replies go to attacker, confirming phishing intent.

## 5. Historical Reports / IP Reputation:

- Sending IP (147.78.103.9) reported **191 times by 75 distinct sources** on AbuseIPDB.
- **Risk: High** – IP has strong evidence of malicious activity.

## 6. Email Content Quality:

- Email is written with **poor English, grammar mistakes, and awkward phrasing** (e.g., “Confirm your email is good” ,, “I had one idea that never changed in my mind, that you should use your wealth to help people” ,, “I want to use my wealth to help and support selected individuals who will help people around them”...).
- **Risk: Medium** – typical phishing indicator; scammers often write emails with broken grammar or unnatural phrasing.

## 8. Overall Risk Assessment:

- **Likelihood of compromise / malicious intent: Very High**

## 7. Analyst Summary & Recommendation

The analyzed email exhibits multiple red flags strongly indicative of a **phishing attempt**:

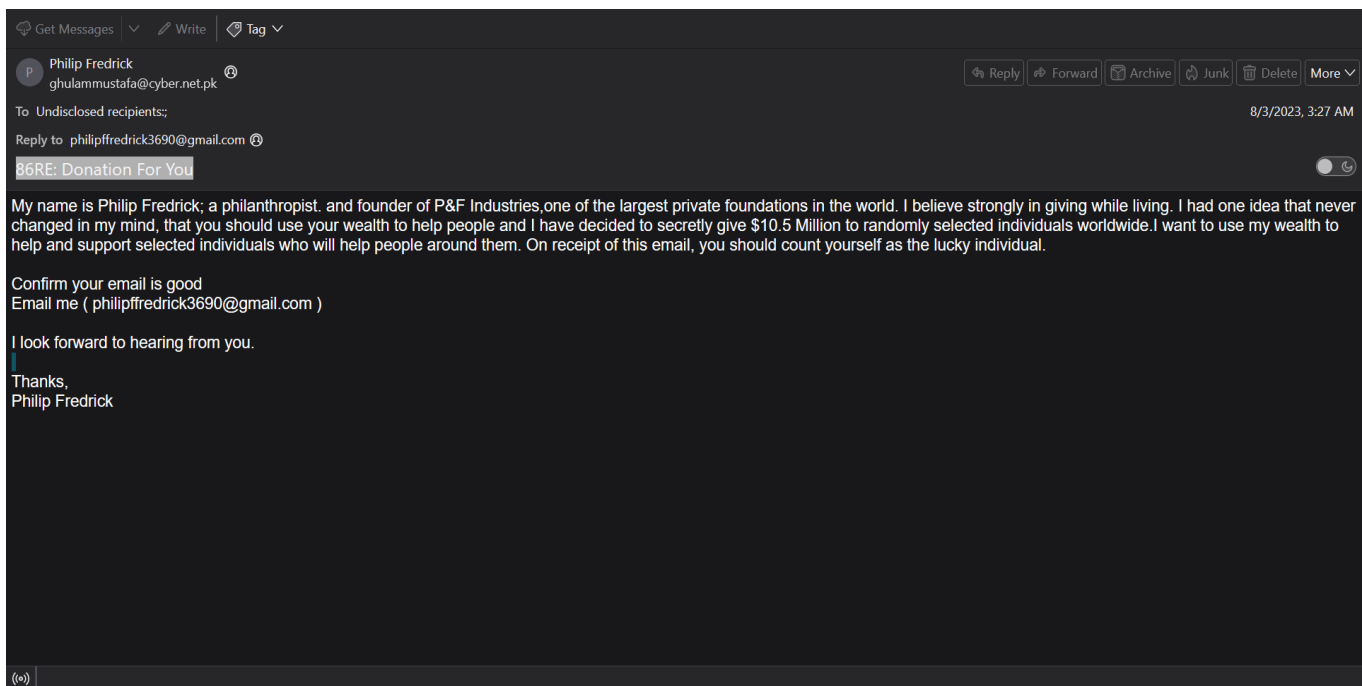
- **Spoofed sender address**: The message was sent using the legitimate email account of **ghulammustafa@cyber.net.pk**, likely via account compromise or domain abuse, while the **Reply-To** address redirects to *philipffredrick3690@gmail.com*. This technique is used to appear legitimate while ensuring attacker-controlled communication.
- **Content red flags**: The email promises a large sum of money (\$10.5 million), a well-known social engineering tactic to entice victims.
- **Poor language quality**: Multiple grammar and phrasing issues (e.g., “Confirm your email is good”) further indicate fraudulent intent.
- **High external abuse reports**: The originating IP has been flagged in AbuseIPDB and VirusTotal with multiple reports, confirming malicious history

## It is recommended :

- **Do not reply** or engage with the provided email addresses.
- **Block sender IP** at the email gateway and security appliances.
- **Report to abuse@cyber.net.pk** (the compromised domain) to notify the legitimate provider.
- **Awareness training**: Users should be reminded not to trust unsolicited financial offers, especially those containing poor English and suspicious sender/reply-to mismatches.

## 8. Attachments

**Screenshots of email :**



### Screenshot of the sender's IP address in VirusTotal :

<https://www.virustotal.com/gui/ip-address/147.78.103.9>

147.78.103.9

1 / 94  
Community Score

1/94 security vendor flagged this IP address as malicious

Reanalyze Similar More

147.78.103.9

BG Last Analysis Date 4 months ago

DETECTION DETAILS RELATIONS COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis Do you want to automate checks?

ESET	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

### Screenshot of the sender's IP address in AbuseIPDB :

<https://www.abuseipdb.com/check/147.78.103.9>

The screenshot shows the AbuseIPDB website interface. At the top, there is a navigation bar with links: Report IP, Bulk Reporter, Bulk Checker, Pricing, Docs, IP Utilities, Contact, and More. A Login button and a Sign Up button are also present. The main heading reads "AbuseIPDB » 147.78.103.9". Below this, a green box contains a search bar with the IP address 147.78.103.9 and a CHECK button. A feedback button is visible on the left. The main content area states: "147.78.103.9 was found in our database! This IP was reported 191 times. Confidence of Abuse is 0%:". A progress bar shows 0%. Below this, a table lists details: ISP (OpenSolutions), Usage Type (Data Center/Web Hosting/Transit), and ASN (Unknown).

Property	Value
ISP	OpenSolutions
Usage Type	Data Center/Web Hosting/Transit
ASN	Unknown

### Screenshot of the sender's mail server IP address (from the second 'Received' header) in VirusTotal :

<https://www.virustotal.com/gui/ip-address/159.27.24.86>

The screenshot shows the VirusTotal website interface for the IP address 159.27.24.86. The top navigation bar includes a search bar with the IP address, and links for Sign in and Sign up. The main content area features a circular "Community Score" of 1/94. A warning message states: "1/94 security vendor flagged this IP address as malicious". Below this, the IP address 159.27.24.86 (159.27.0.0/16) is displayed, along with the AS number AS 58593 (Shanghai Blue Cloud Technology Co., Ltd) and the country CN. The last analysis date is 18 days ago. The interface includes tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. A banner encourages joining the community. The "Security vendors' analysis" section shows results from MalwareURL, Acronis, Abusix, and ADMINUSLabs, all marked as "Clean".

Vendor	Analysis Result
MalwareURL	Malware
Acronis	Clean
Abusix	Clean
ADMINUSLabs	Clean

**Screenshot of the sender's mail server IP address (from the second 'Received' header) in AbuseIPDB :**

<https://www.abuseipdb.com/check/159.27.24.86>

The screenshot shows the AbuseIPDB website interface. At the top, there is a navigation bar with the AbuseIPDB logo and links for Report IP, Bulk Reporter, Bulk Checker, Pricing, Docs, IP Utilities, Contact, and More. There are also Login and Sign Up buttons. Below the navigation bar, the main heading reads "AbuseIPDB » 159.27.24.86". A green search bar contains the IP address "159.27.24.86" and a "CHECK" button. To the left of the search bar is a vertical "feedback" button. Below the search bar, a message states "159.27.24.86 was found in our database!". Below this, it says "This IP was reported 29 times. Confidence of Abuse is 0%:". A progress bar shows 0% confidence. Below the progress bar, there is a table with the following information:

ISP	Shanghai Blue Cloud Technology Co.,Ltd
Usage Type	Data Center/Web Hosting/Transit
ASN	AS58593

## Automation & Tools:

To streamline email header analysis, **MXToolbox's Email Header** Analyzer was utilized to automatically parse and interpret the headers. This automation facilitated quick identification of SPF, DKIM, and DMARC results, the true originating IP, and potential relay servers. By leveraging this tool, the analysis process became more efficient, reducing manual inspection errors and accelerating phishing detection.

<https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=435570d2-d70a-45ad-9f6e-035dfc409956>