

# **Phishing Email Analysis Report**

By:

Kifayah Oladejo, Cybersecurity Analyst

Date: 06 November, 2025

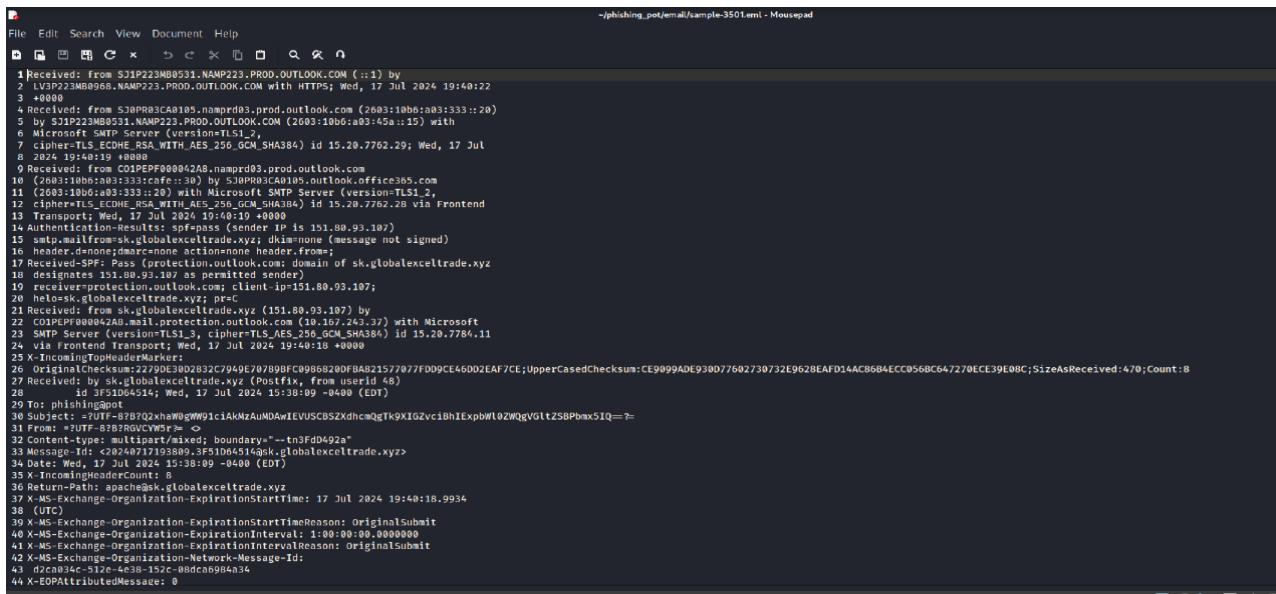
## **1. Executive Summary**

Conducted an in-depth analysis of a suspicious email received through the corporate email gateway. The email was isolated in a sandboxed virtual environment and subjected to multi-layered analysis techniques, including header inspection, URL reputation analysis, and threat intelligence gathering. Based on the results, it is concluded that the email is a phishing attempt designed to lure users into clicking a malicious link.

## 2. Email Metadata Analysis

### 2.1 Sender Information

- **Return-Path:** apache@sk.globalexceltrade.xyz
- **Sending Server:** SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (::1)
- **Sender IP Address:** 151.80.93.107
- **IP Reputation Check (AbuseIPDB):** No existing reports were found for this IP address in the AbuseIPDB database. However, the lack of reports does not indicate safety, especially given the suspicious context.



```
File Edit Search View Document Help
File Edit Search View Document Help
1 Received: from SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (::1) by
2 LV3P223MB0068.NAMP223.PROD.OUTLOOK.COM with HTTPS; Wed, 17 Jul 2024 19:40:22
3 +0000
4 Received: from SJ0PR03CA0105.namprd03.prod.outlook.com (2603:10b6:a03:333::28)
5 by SJ3P223MB0531.NAMP223.PROD.OUTLOOK.COM (2603:10b6:a03:454::15) with
6 Microsoft SMTP Server (version=TLS1_2,
7 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7762.28 via Frontend
8 2024-19:40:19 +0000
9 Received: from CO1PEF0004ZAB.namprd03.prod.outlook.com
10 (2603:10b6:a03:333::28) by SJ0PR03CA0105.outlook.office365.com
11 (2603:10b6:a03:333::28) with Microsoft SMTP Server (version=TLS1_2,
12 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7762.28 via Frontend
13 2024-19:40:19 +0000
14 Authentication-Results: spf=pass (sender IP is 151.80.93.107)
15 smtputf8=none;globalexceltrade.xyz;dkim=none (message not signed)
16 header.d=none;dmarc=none actions=none header.from;
17 Received-SPF: Pass (protection.outlook.com: domain of sk.globalexceltrade.xyz
18 designates 151.80.93.107 as permitted sender)
19 Authentication-Results: dkim=none header.from=sk.globalexceltrade.xyz;
20 helo=sk.globalexceltrade.xyz; prc=none
21 Received: from sk.globalexceltrade.xyz (151.80.93.107) by
22 CO1PEF0004ZAB.mail.protection.outlook.com (10.167.243.37) with Microsoft
23 SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384) id 15.20.7784.11
24 2024-19:40:19 +0000
25 X-MS-Transport-Processor:
26 originalChecksum=>2270DE30D2832C7949E70780BFC09868200FBAB21577077FD09CE46D02EAF7CE;UpperCasedChecksum:CE9999ADE930077602730732E9628EAFD14ACB6B4ECC056BC647279ECE39E08C;SizeAsReceived:470;Count:8
27 Received: by sk.globalexceltrade.xyz (Postfix, from user@46)
28 id 3F310D451A; Wed, 17 Jul 2024 19:40:09 +0400 (EDT)
29 To: phishing@not
30 Subject: [REDACTED]76/Q2XhWmgW901ciAKWzAUNDwIEVUSCBZXdhcmQgTk9XIOZvcibHIEpbWl0ZWQgVGltZSBPbm5IQ=?=
31 From: <UTF-8@R0GWCWMr> - C
32 Content-type: multipart/mixed; boundary="--tn3FdFd4q2a"
33 Message-Id: <0240717193809.3F510D4514@sk.globalexceltrade.xyz>
34 Date: Wed, 17 Jul 2024 15:38:09 -0400 (EDT)
35 X-IncomingHeaderCount: 8
36 Return-Path: apache@sk.globalexceltrade.xyz
37 X-MS-Exchange-Organization-ExpirationStartTime: 17 Jul 2024 19:40:18.9934
38 (UTC)
39 X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
40 X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.000000
41 X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
42 X-MS-Exchange-Organization-Network-Message-Id:
43 d2c0N34c-512e-4e30-152c-08dcab984a34
44 X-EOPAttributedMessage: 0
```

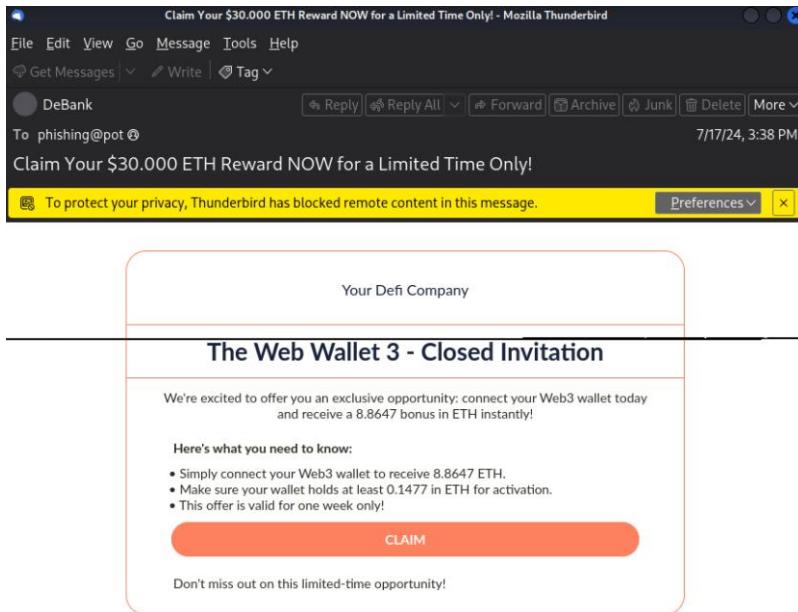
### 2.2 Email Authentication Results

- **SPF (Sender Policy Framework): PASS**
  - The SPF record validated successfully, suggesting that the sending server is authorized to send mail on behalf of the domain. However, SPF alone is not a reliable indicator of legitimacy.
- **DKIM (DomainKeys Identified Mail): NONE**
  - No DKIM signature was present, indicating the email was not cryptographically signed. This reduces the credibility and makes the email susceptible to spoofing.
- **DMARC (Domain-based Message Authentication, Reporting, and Conformance): NONE**
  - The domain lacks a DMARC policy, increasing the likelihood of unauthorized use and spoofing.

### 3. Embedded URL Analysis

#### 3.1 Suspicious Link

- URL Found in Email: <https://innovatech.website>



- I extracted the link and performed scans using the following tools:
  - URLScan.io

The screenshot shows the URLScan.io interface for the URL [innovatech.website](http://innovatech.website/). The IP address listed is 188.114.97.3. The main summary section states that the website contacted 2 IPs in 1 countries across 1 domains to perform 34 HTTP transactions. The main IP is 188.114.97.3, located in Amsterdam, Netherlands and belongs to CLOUDFLAREN.NET, US. The main domain is innovatech.website. The TLS certificate was issued by WE1 on April 3rd 2025, valid for 3 months. The "Summary" tab is selected, showing the following details:

- This website contacted 2 IPs in 1 countries across 1 domains to perform 34 HTTP transactions.
- The main IP is 188.114.97.3, located in Amsterdam, Netherlands and belongs to CLOUDFLAREN.NET, US. The main domain is innovatech.website.
- TLS certificate: Issued by WE1 on April 3rd 2025. Valid for: 3 months.

The "urlscan.io Verdict" is "No classification". The "Live information" section shows the Current DNS A record: 188.114.97.3 (AS13335 - CLOUDFLAREN.NET, US). Other tabs visible include Summary, HTTP, Redirects, Links, Behaviour, Indicators, Similar, and DOM.

- **VirusTotal**

The screenshot shows the VirusTotal analysis page for the URL <http://innovatech.website/>. The main summary indicates that no security vendors flagged this URL as malicious. Below this, detailed information is provided: Status 200, Content type text/html; charset=UTF-8, and Last Analysis Date 7 months ago. The interface includes tabs for DETECTION, DETAILS, and COMMUNITY, and a call-to-action to Join our Community.

- **Bluecoat SiteReview**

The screenshot shows the WebPulse Site Review Request form. The URL <http://innovatech.website/> has been submitted. The current categorization is listed as **Finance**, with a note stating "This page was rated by our WebPulse system". There is also a link to "Check another URL".

### 3.2 Threat Intelligence on Domain

- **Domain:** innovatech.website

A WHOIS lookup revealed

Registrar:HOSTINGER operations, UAB

Registered On:2024-05-28

The domain appears to be newly registered and lacks a solid reputation, which is consistent with common phishing infrastructure.

## 4. Threat Intelligence Analysis

### 4.1 IP Address Reputation

- **IP Address:** 151.80.93.107
- The IP address did not return any reports on AbuseIPDB. However, attackers often rotate IPs and domains, so absence of prior activity does not imply trustworthiness.

### 4.2 Indicators of Compromise (IoCs)

- **Email Header Anomalies:** Missing DKIM/DMARC, mismatched Return-Path and sending server.
- **Malicious URL:** The URL embedded in the email links to a suspicious domain.
- **Unusual Return-Path Domain:** sk.globalexceltrade.xyz is a non-standard and suspicious domain name.

## 5. Conclusion & Recommendations

### 5.1 Conclusion

Based on comprehensive email header inspection, authentication failures, and third-party threat intelligence scans, I assess this email to be a **confirmed phishing attempt**. The email was crafted to trick recipients into clicking a potentially malicious link hosted at innovatech.website. The domain and IP involved exhibit red flags consistent with phishing infrastructure.

### 5.2 Recommendations

1. **Immediate Quarantine:** Ensure the email is removed from all user inboxes.
2. **Block Indicators:** Add innovatech.website and 151.80.93.107 to all perimeter security blocklists (firewall, proxy, email gateway).
3. **Report to Authorities:**
  - o Report the phishing attempt to Microsoft via the Security & Compliance Center.
  - o Submit indicators to APWG and Google Safe Browsing.
4. **Security Awareness Campaign:** Notify users about this phishing attempt and reinforce phishing awareness training.
5. **Enhance Email Filtering:** Strengthen email gateway rules to enforce strict DMARC/DKIM/SPF policies.
6. **Threat Hunting:** Initiate monitoring of internal logs and endpoints for any interaction with the flagged domain/IP.

**Report Prepared by:**

**Kifayah Oladejo**

Cybersecurity Analyst