

# **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
~\phishing_pot\email\sample-3501.eml - Mousepad

1 Received: from SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (:::1) by
2 LV3P223MB0531.NAMP223.PROD.OUTLOOK.COM with HTTPS; Wed, 17 Jul 2024 19:40:22
3 +0000
4 Received: from SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (2603:10b6:a03:333::20)
5 by SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (2603:10b6:a03:45a::15) with
6 Microsoft SMTP Server (version=TLS1_2,
7 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7762.29; Wed, 17 Jul
8 2024 19:40:19 +0000
9 Received: from CO1PEPF000042AB.namprd03.prod.outlook.com
10 (2603:10b6:a03:333::30) by SJ1P223MB0531.NAMP223.PROD.OUTLOOK.COM (2603:10b6:a03:333::20) with Microsoft SMTP Server (version=TLS1_2,
11 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7762.28 via Frontend
12 Transport; Wed, 17 Jul 2024 19:40:19 +0000
13 Authentication-Results: spf=pass (sender IP is 151.80.93.107)
14 smtp.mailfrom=sk.globalexceltrade.xyz; dkim=none (message not signed)
15 header.from=sk.globalexceltrade.xyz; dmarc=none action=none header.from=sk.globalexceltrade.xyz
16 Received-SPF: Pass (protection.outlook.com: domain of sk.globalexceltrade.xyz
17 designates 151.80.93.107 as permitted sender)
18 receiver=protection.outlook.com; client-ip=151.80.93.107;
19 helo=sk.globalexceltrade.xyz; pr=6
20 Received: from sk.globalexceltrade.xyz (151.80.93.107) by
21 CO1PEPF000042AB.mail.protection.outlook.com (10.167.243.37) with Microsoft
22 SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384) id 15.20.7784.11
23 via Frontend Transport; Wed, 17 Jul 2024 19:40:19 +0000
24 X-IncomingTopHeaderMarker:
25 OriginalChecksum:22790E3802832C7949E707898FC09B6820DFBA021577077F009CE46002EAF7CE;UpperCasedChecksum:CE9999ADE930073602730732E962EAFD14AC8B04ECC056BC647270ECC39E08C;SizeAsReceived:470;Count:8
26 Received: by sk.globalexceltrade.xyz (Postfix, from userid 48)
27 id 3F5D04514; Wed, 17 Jul 2024 15:38:09 -0400 (EDT)
28 To: phishingpot
29 Subject: =?UTF-8?B?Q2haQW91c1AKMzAUMDwAIEVUSCBSZXdhcmQgTk9KIGZvc1BIIEpwbWl0ZWQvVGlzSBPbm51Q==?
30 From: =?UTF-8?B?Q2haQW91c1AKMzAUMDwAIEVUSCBSZXdhcmQgTk9KIGZvc1BIIEpwbWl0ZWQvVGlzSBPbm51Q==?
31 Content-Type: multipart/mixed; boundary="=3F5D04514"
32 Content-Id: <0240717193809.3F5D04514@sk.globalexceltrade.xyz>
33 Date: Wed, 17 Jul 2024 15:38:09 -0400 (EDT)
34 X-IncomingHeaderCount: 0
35 Return-Path: apache@sk.globalexceltrade.xyz
36 X-MS-Exchange-Organization-ExpirationStartTime: 17 Jul 2024 19:40:18.9934
37 (UTC)
38 X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
39 X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00000000
40 X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
41 X-MS-Exchange-Organization-Network-Message-Id:
42 02c03ac-3120-4e38-152c-0bdcab90a034
43 X-EOAAttributedMessage: 0
44
```

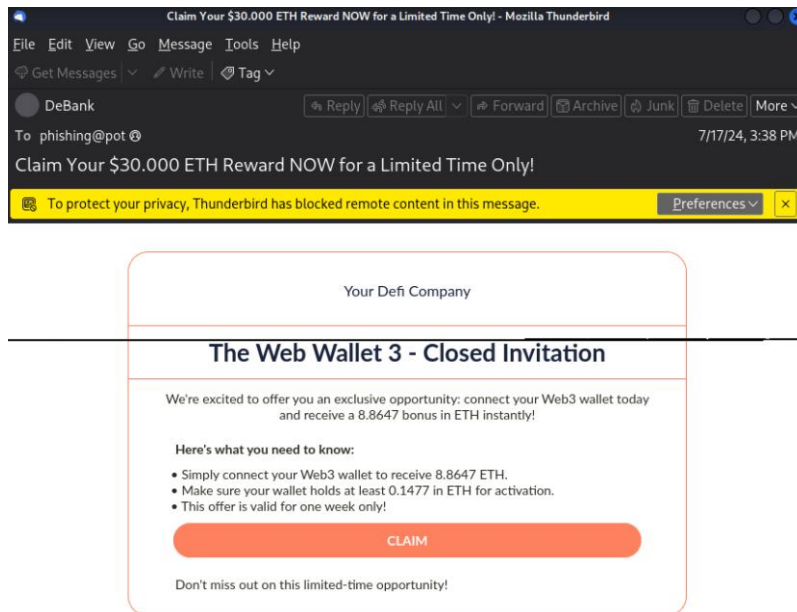
### 2.2 Email Authentication Results

- **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

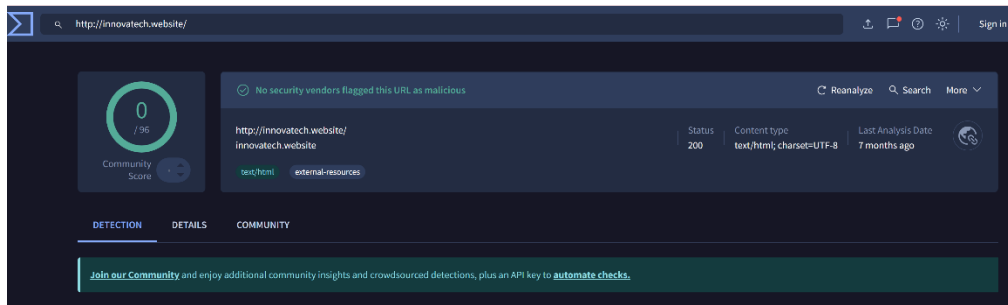
- **URL Found in Email:** <https://innovatech.website>



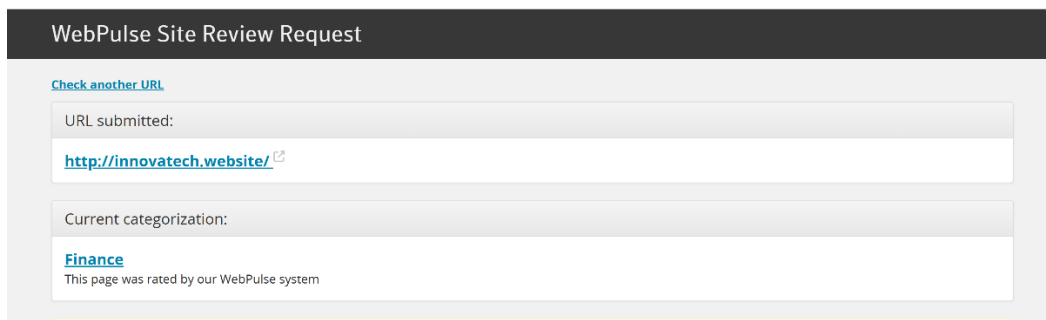
- I extracted the link and performed scans using the following tools:
  - **URLScan.io**

The image shows the URLScan.io website interface. The top navigation bar includes a search icon, 'urlscan.io', 'Home', 'Search', 'Live', 'API', 'Blog', and 'Docs'. The main content area displays the scan results for 'innovatech.website'. The IP address is '188.114.97.3' with a 'Public Scan' button. The submitted URL is 'http://innovatech.website/' and the effective URL is 'https://innovatech.website/'. The submission was on April 07 via manual (April 7th 2025, 5:01:18 am UTC) from QA, scanned from NL. The interface includes tabs for Summary, HTTP (34), Redirects, Links (2), Behaviour, Indicators, Similar, and DOM. The Summary section states: '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 CLOUDFLARENET, US. The main domain is innovatech.website. TLS certificate: Issued by WE1 on April 3rd 2025. Valid for: 3 months.' Below this, it says 'innovatech.website scanned 2 times on urlscan.io' with a 'Show Scans 2' button. The verdict is 'urlscan.io Verdict: No classification' with a green checkmark. The live information section shows the current DNS A record: '188.114.97.3 (AS13335 - CLOUDFLARENET, US)'.

## ○ VirusTotal



## ○ Bluecoat SiteReview



### 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:**
  - Report the phishing attempt to Microsoft via the Security & Compliance Center.
  - 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