Phishing Email Analysis Report

By:

Olatunji T.Lawal, Cybersecurity Analyst

Date: 13th April, 2025

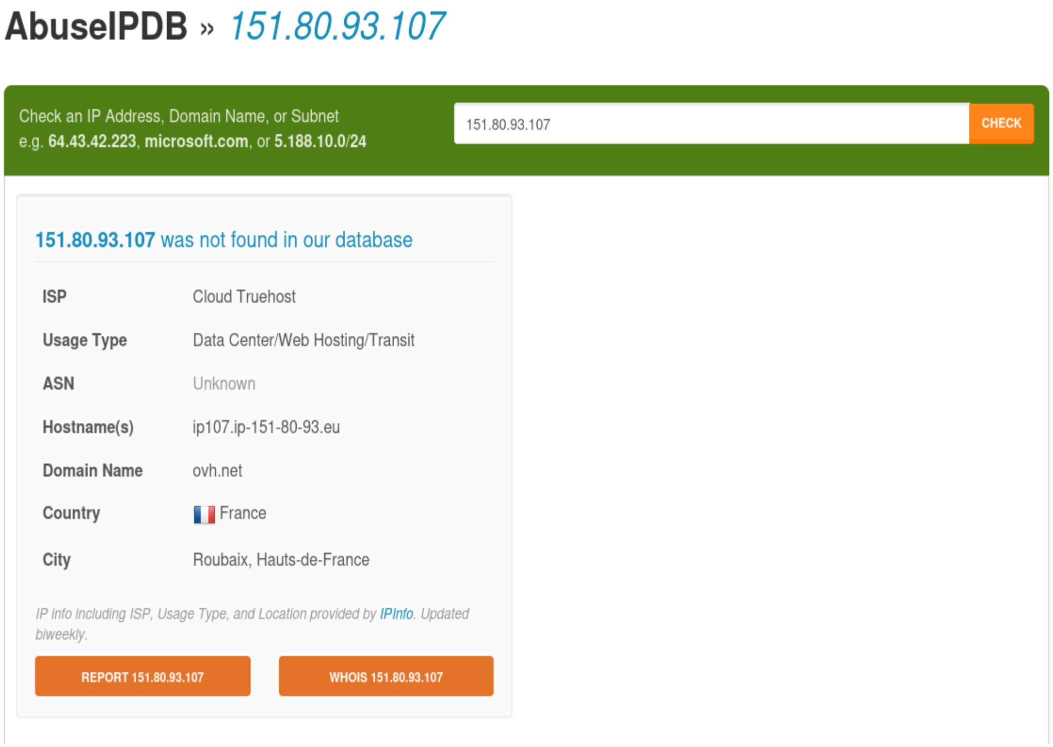
1. Executive Summary

I thoroughly investigated a dubious email that I had obtained over the business email gateway. After the email was isolated in a sandboxed virtual environment, it was subjected to a variety of multi-layered analytical techniques, including header inspection, URL reputation analysis, and threat intelligence gathering. Based on the results, the email is identified as a phishing attempt, which aims to deceive recipients into clicking on a harmful 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.



AbuseIPDB » *151.80.93.107*

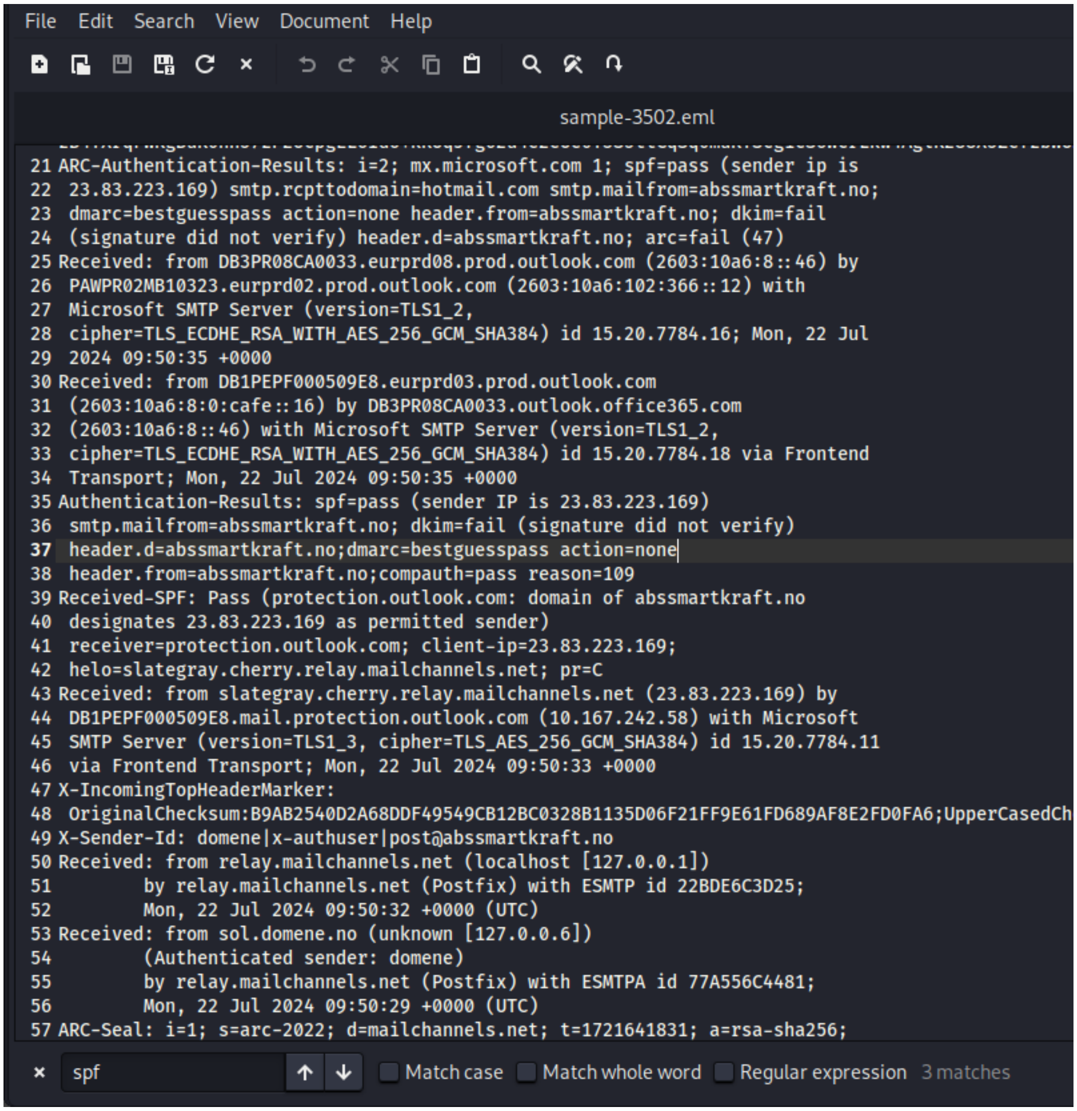
Check an IP Address, Domain Name, or Subnet
e.g. **64.43.42.223**, **microsoft.com**, or **5.188.10.0/24**

151.80.93.107 CHECK

151.80.93.107 was not found in our database

ISP	Cloud Truehost
Usage Type	Data Center/Web Hosting/Transit
ASN	Unknown
Hostname(s)	ip107.ip-151-80-93.eu
Domain Name	ovh.net
Country	France
City	Roubaix, Hauts-de-France

IP info including ISP, Usage Type, and Location provided by IPInfo. Updated biweekly.



```
ARC-Authentication-Results: i=2; mx.microsoft.com 1; spf=pass (sender ip is
 23.83.223.169) smtp.rcpttodomain=hotmail.com smtp.mailfrom=abssmartkraft.no;
 dmarc=bestguesspass action=none header.from=abssmartkraft.no; dkim=fail
 (signature did not verify) header.d=abssmartkraft.no; arc=fail (47)
Received: from DB3PR08CA0033.eurprd08.prod.outlook.com (2603:10a6:8::46) by
 PAWPR02MB10323.eurprd02.prod.outlook.com (2603:10a6:102:366::12) with
 Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7784.16; Mon, 22 Jul
 2024 09:50:35 +0000
Received: from DB1PEPF000509E8.eurprd03.prod.outlook.com
 (2603:10a6:8:0:cafe::16) by DB3PR08CA0033.outlook.office365.com
 (2603:10a6:8::46) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.7784.18 via Frontend
 Transport; Mon, 22 Jul 2024 09:50:35 +0000
Authentication-Results: spf=pass (sender IP is 23.83.223.169)
 smtp.mailfrom=abssmartkraft.no; dkim=fail (signature did not verify)
 header.d=abssmartkraft.no;dmarc=bestguesspass action=none
 header.from=abssmartkraft.no;compauth=pass reason=109
Received-SPF: Pass (protection.outlook.com: domain of abssmartkraft.no
 designates 23.83.223.169 as permitted sender)
 receiver=protection.outlook.com; client-ip=23.83.223.169;
 helo=slategray.cherry.relay.mailchannels.net; pr=C
Received: from slategray.cherry.relay.mailchannels.net (23.83.223.169) by
 DB1PEPF000509E8.mail.protection.outlook.com (10.167.242.58) with Microsoft
 SMTP Server (version=TLS1_3, cipher=TLS_AES_256_GCM_SHA384) id 15.20.7784.11
 via Frontend Transport; Mon, 22 Jul 2024 09:50:33 +0000
X-IncomingTopHeaderMarker:
 OriginalChecksum:B9AB2540D2A68DDF49549CB12BC0328B1135D06F21FF9E61FD689AF8E2FD0FA6;UpperCasedCh
X-Sender-Id: domene|x-authuser|post@abssmartkraft.no
Received: from relay.mailchannels.net (localhost [127.0.0.1])
        by relay.mailchannels.net (Postfix) with ESMTP id 22BDE6C3D25;
        Mon, 22 Jul 2024 09:50:32 +0000 (UTC)
Received: from sol.domene.no (unknown [127.0.0.6])
        (Authenticated sender: domene)
        by relay.mailchannels.net (Postfix) with ESMTPA id 77A556C4481;
        Mon, 22 Jul 2024 09:50:29 +0000 (UTC)
ARC-Seal: i=1; s=arc-2022; d=mailchannels.net; t=1721641831; a=rsa-sha256;
```

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. It means the sender's domain has a published SPF record (in DNS). The IP address of the server matches an IP listed on the SPF record. The email passes the SPF check, suggesting it's more likely to be legitimate.

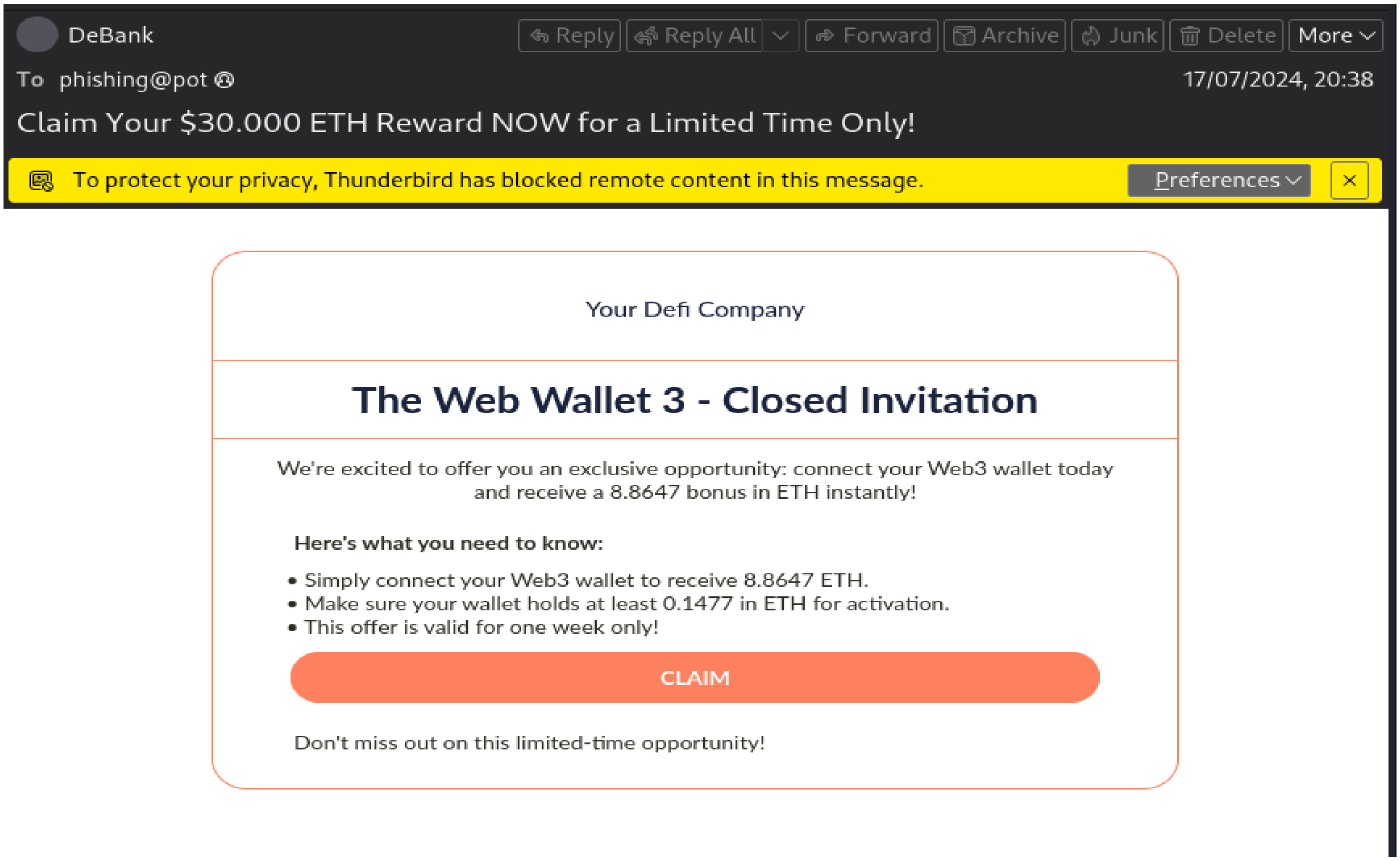
      However, SPF alone is not a reliable indicator of legitimacy.
- **DKIM (Domain Keys Identified Mail)**: NONE
    - No DKIM signature was present, indicating the email was not cryptographically signed. This reduces the credibility and makes the email susceptible to spoofing.

- **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://devicetechie.site



DeBank

To phishing@pot

17/07/2024, 20:38

Claim Your $30.000 ETH Reward NOW for a Limited Time Only!

To protect your privacy, Thunderbird has blocked remote content in this message.

Your Defi Company

The Web Wallet 3 - Closed Invitation

We're excited to offer you an exclusive opportunity: connect your Web3 wallet today and receive a 8.8647 bonus in ETH instantly!

Here's what you need to know:

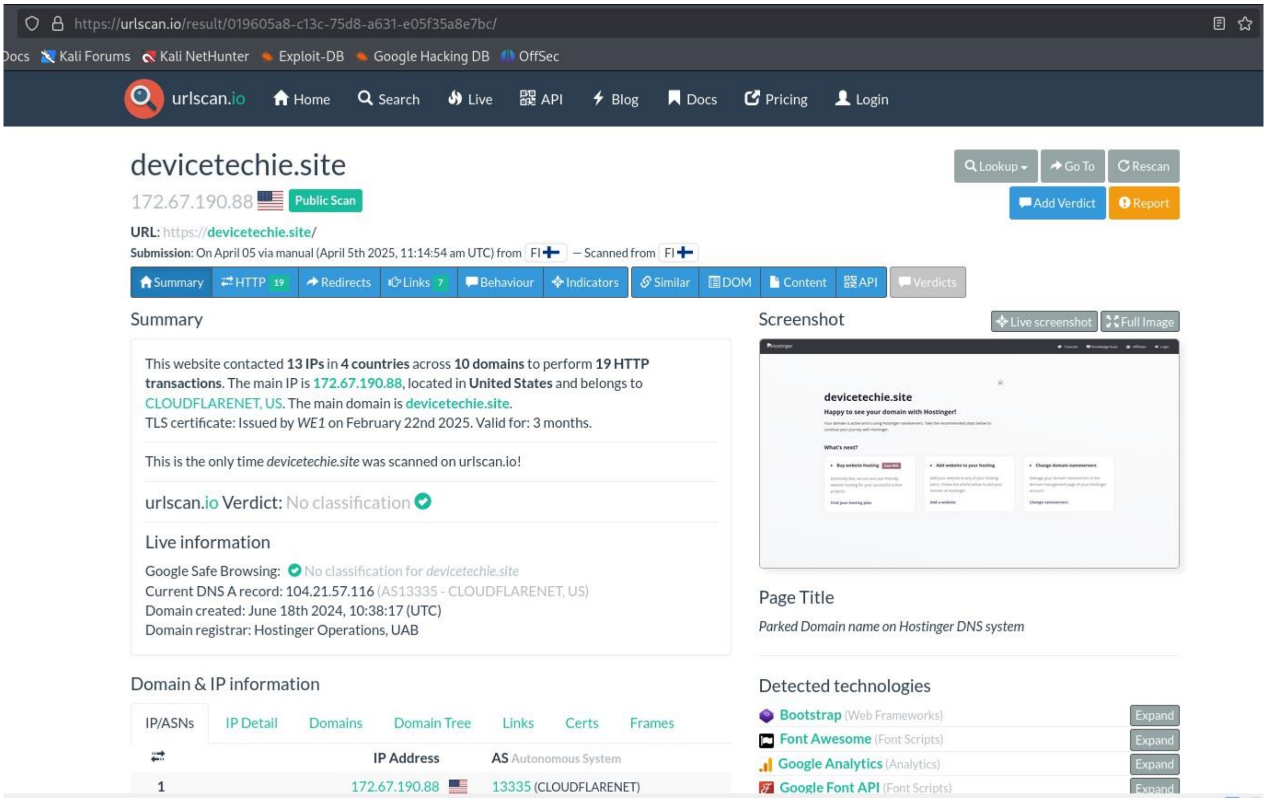
- Simply connect your Web3 wallet to receive 8.8647 ETH.
- Make sure your wallet holds at least 0.1477 in ETH for activation.
- This offer is valid for one week only!

CLAIM

Don't miss out on this limited-time opportunity!

I extracted the link and performed scans using the following tools:

- **URLScan.io**


https://urlscan.io/result/019605a8-c13c-75d8-a631-e05f35a8e7bc/
Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
urlscan.io Home Search Live API Blog Docs Pricing Login
Lookup Go To Rescan
Add Verdict Report
Summary HTTP 19 Redirects Links 7 Behaviour Indicators Similar DOM Content API Verdicts
Live screenshot Full Image
devicetechie.site
Happy to see your domain with Hostinger!
IP/ASNs IP Detail Domains Domain Tree Links Certs Frames
Expand

devicetechie.site

172.67.190.88 Public Scan

URL: https://devicetechie.site/

Submission: On April 05 via manual (April 5th 2025, 11:14:54 am UTC) from FI — Scanned from FI

Summary

This website contacted **13 IPs** in **4 countries** across **10 domains** to perform **19 HTTP transactions**. The main IP is 172.67.190.88, located in **United States** and belongs to CLOUDFLARENET, US. The main domain is devicetechie.site.
TLS certificate: Issued by *WE1* on February 22nd 2025. Valid for: 3 months.

This is the only time *devicetechie.site* was scanned on urlscan.io!

urlscan.io Verdict: No classification ✓

Live information

Google Safe Browsing: ✓ No classification for *devicetechie.site*
Current DNS A record: 104.21.57.116 (AS13335 - CLOUDFLARENET, US)
Domain created: June 18th 2024, 10:38:17 (UTC)
Domain registrar: Hostinger Operations, UAB

Screenshot

Page Title

Parked Domain name on Hostinger DNS system

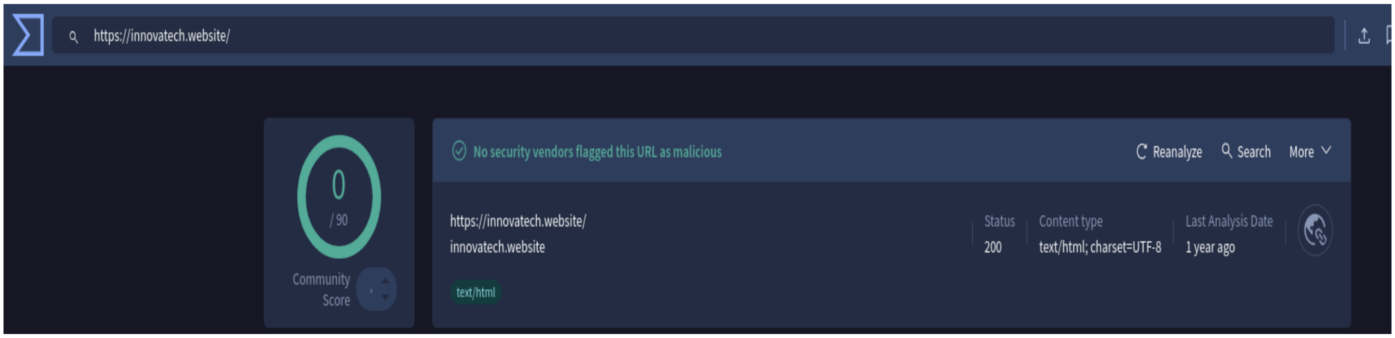
Domain & IP information

	IP Address	AS Autonomous System
1	172.67.190.88	13335 (CLOUDFLARENET)

Detected technologies

Bootstrap (Web Frameworks)
Font Awesome (Font Scripts)
Google Analytics (Analytics)
Google Font API (Font Scripts)

- **VirusTotal**



https://innovatech.website/

0 /90

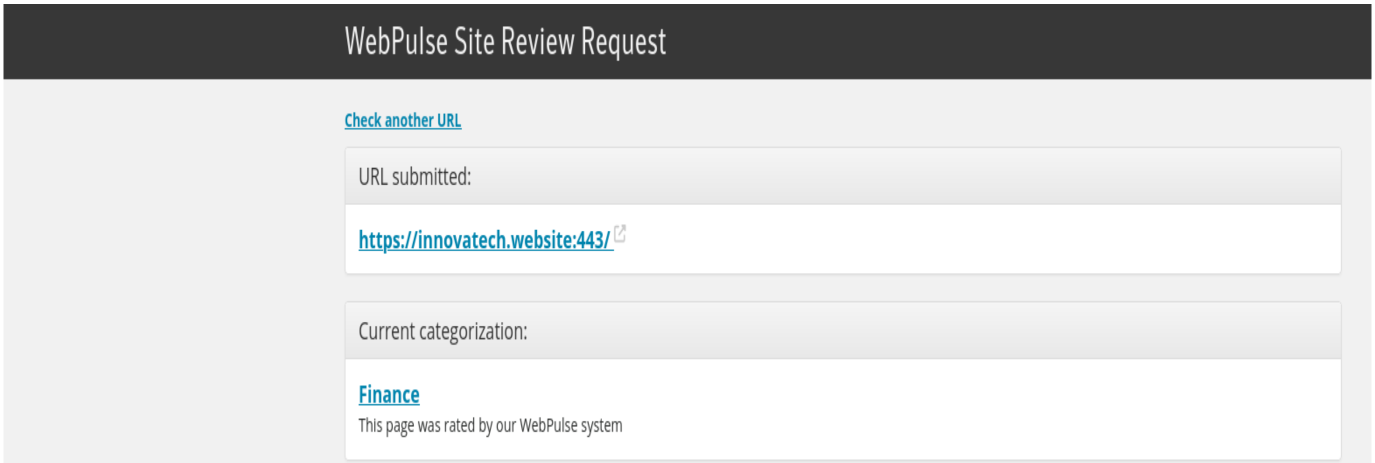
No security vendors flagged this URL as malicious

https://innovatech.website/
innovatech.website

text/html

Status	Content type	Last Analysis Date
200	text/html; charset=UTF-8	1 year ago

- **Bluecoat Site Review**



WebPulse Site Review Request

Check another URL

URL submitted:

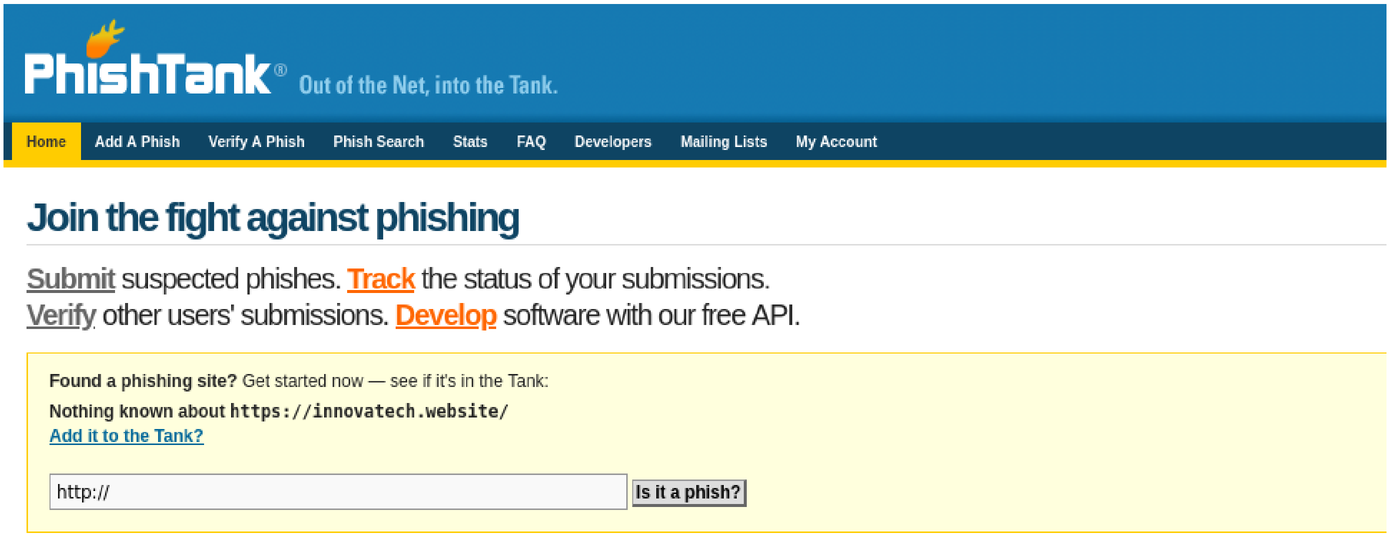
https://innovatech.website:443/

Current categorization:

Finance

This page was rated by our WebPulse system

- **PhishTank SiteReview**



Join the fight against phishing

Submit suspected phishes. Track the status of your submissions.
Verify other users' submissions. Develop software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

Nothing known about `https://innovatech.website/`

Add it to the Tank?

http:// **Is it a phish?**

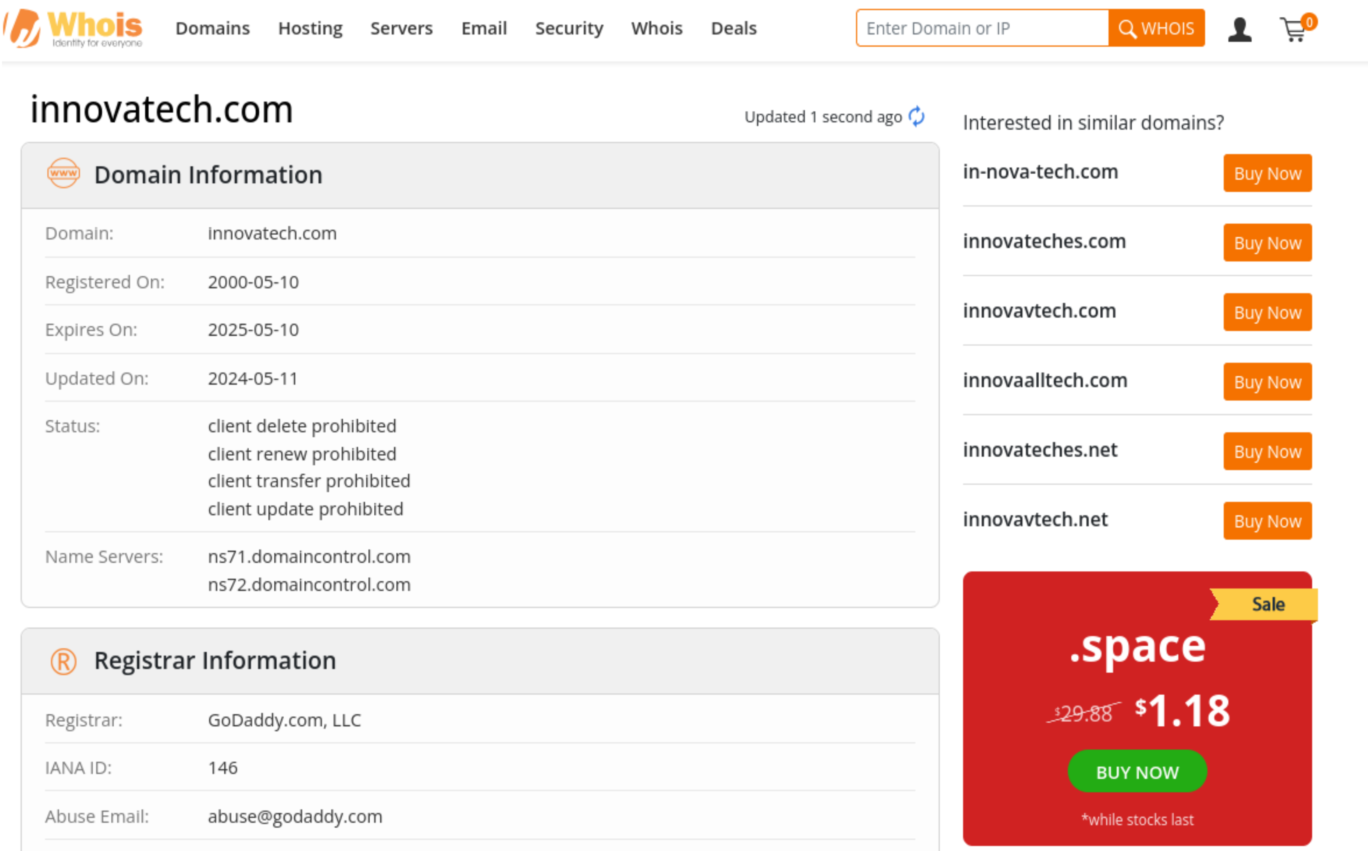
3.2 Threat Intelligence on Domain

- **Domain**: devicetechie.site

A WHOIS lookup revealed

Registrar: GoDaddy.com LLC

Registered On: 2000-05-10



innovatech.com

Updated 1 second ago

Domain Information

Domain:	innovatech.com
Registered On:	2000-05-10
Expires On:	2025-05-10
Updated On:	2024-05-11
Status:	client delete prohibited client renew prohibited client transfer prohibited client update prohibited
Name Servers:	ns71.domaincontrol.com ns72.domaincontrol.com

Registrar Information

Registrar:	GoDaddy.com, LLC
IANA ID:	146
Abuse Email:	abuse@godaddy.com

Interested in similar domains?

in-nova-tech.com	Buy Now
innovateches.com	Buy Now
innovavtech.com	Buy Now
innovaalltech.com	Buy Now
innovateches.net	Buy Now
innovavtech.net	Buy Now

4. Threat Intelligence Analysis

4.1 IP Address Reputation

- **IP Address**: 151.80.93.107

  There were no reports on AbuseIPDB for the IP address. However, the lack of previous activity does not necessarily indicate trustworthiness because attackers frequently switch up IPs and domains.

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**: post@abssmartkraft.no is a non-standard and suspicious domain name.

5. Conclusion & Recommendations

5.1 Conclusion

I consider this email to be a proven phishing effort based on a thorough examination of the email header, authentication issues, and third-party threat intelligence scans. The purpose of the email was to fool users into clicking on a possibly harmful link that was located on devicetechie.site. There are red flags associated with phishing infrastructure on the domain and IP in question.

5.2 Recommendations

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

Report Prepared by: Olatunji Taoheed Lawal

Cybersecurity Analyst