Spoofed Email Report

Title:

Spoofed Email Analysis – Fake NVTTI IT Course Invitation

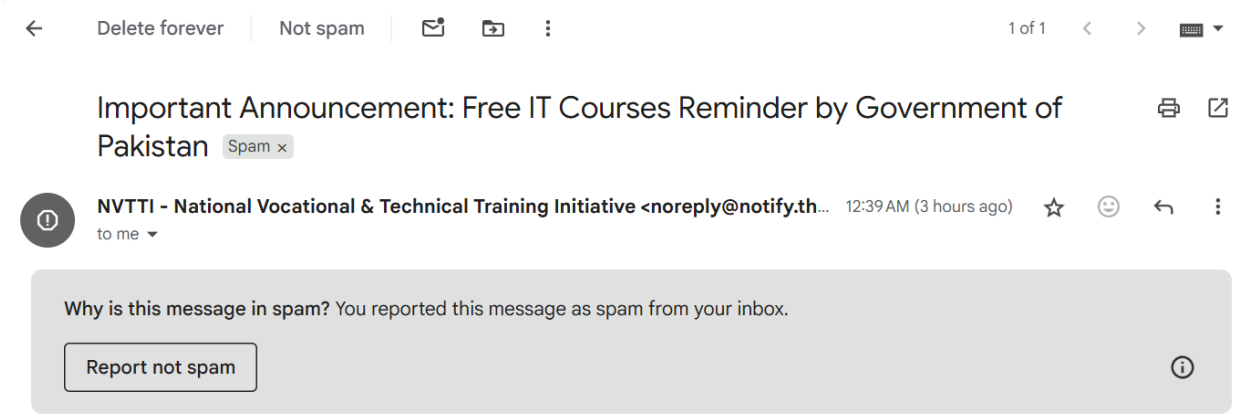
Saad Naveed

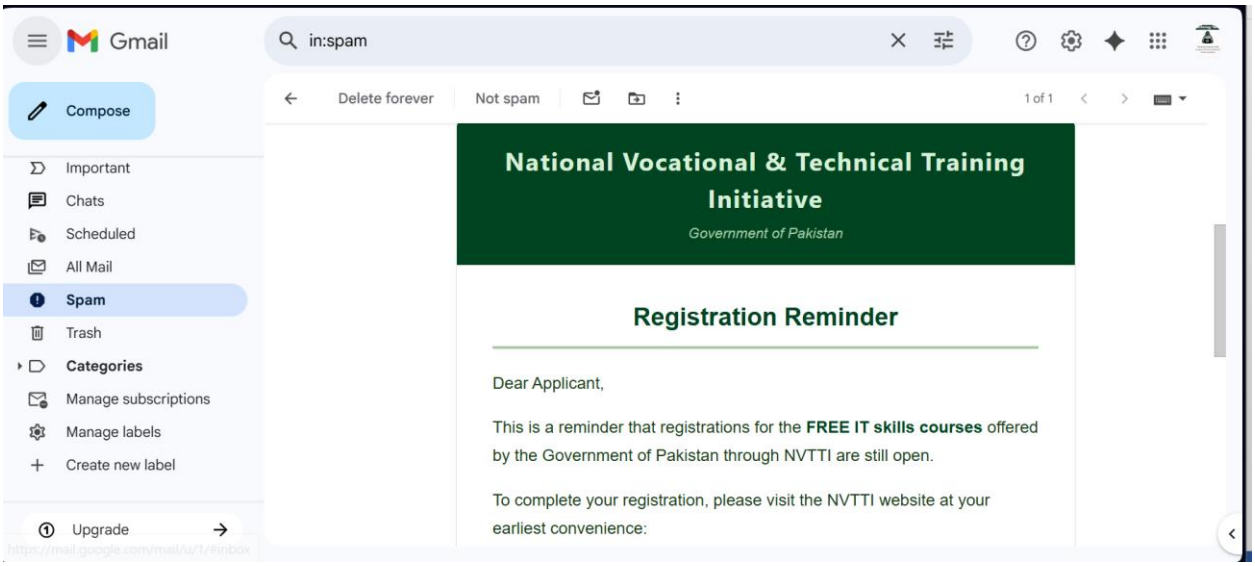
Cybersecurity & Digital Forensics

6th July 2025

Objective

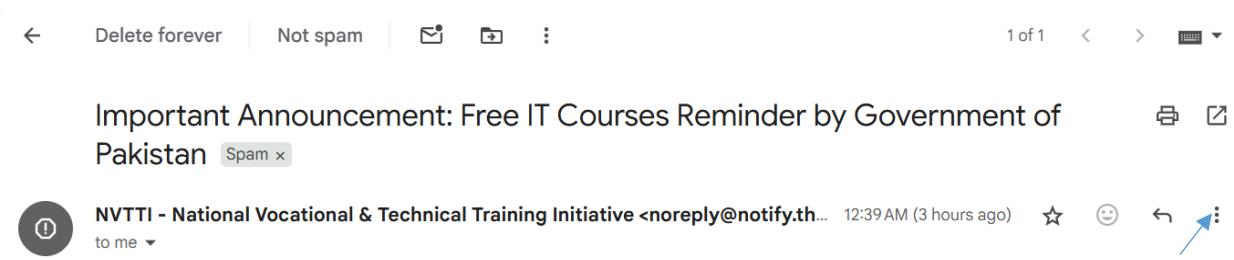
The email is **trying to convince the recipient to register for free IT courses** supposedly offered by the **Government of Pakistan** through an organization named **NVTTI**. It urges the recipient to visit a specific website (www.nvtti.pk) to complete the registration and provides an email for contact.



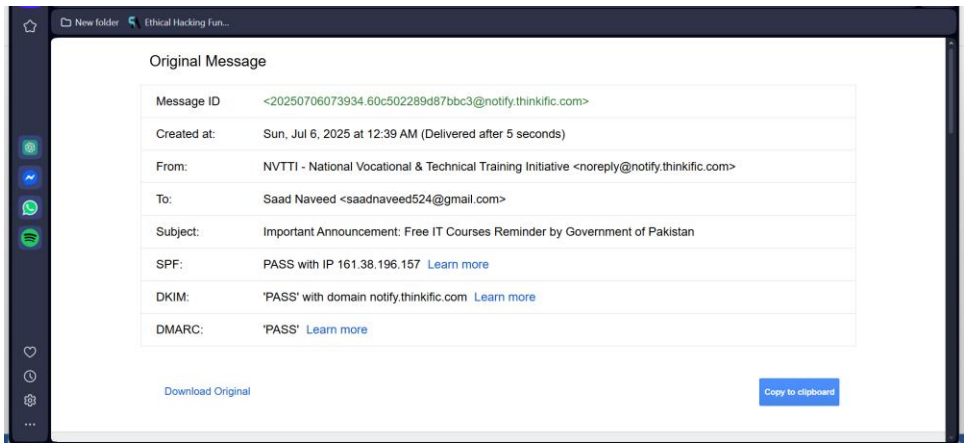


Step 1: Analyze Email Header

Open an email and click right side on three dots.

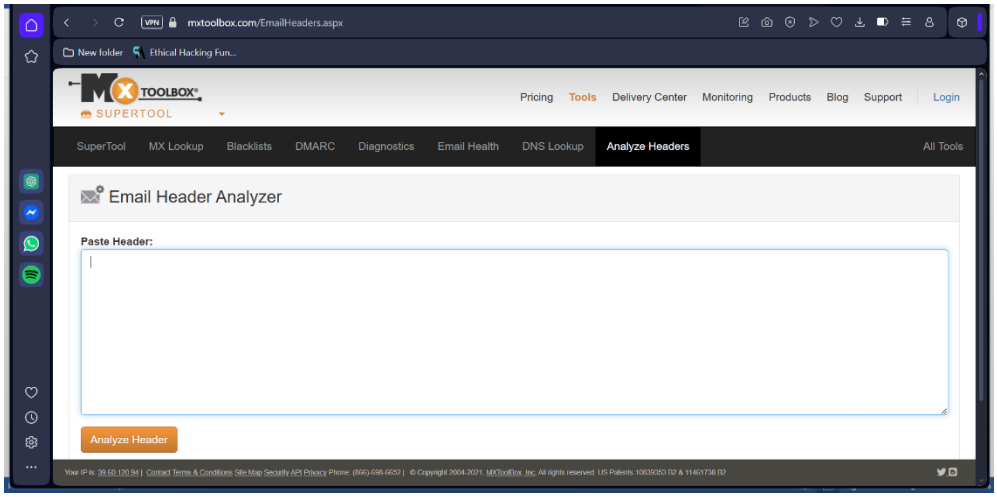


And then Click Show orginal and then click on Copy to Clipboard and paste in MXToolbox Header Analyzer.

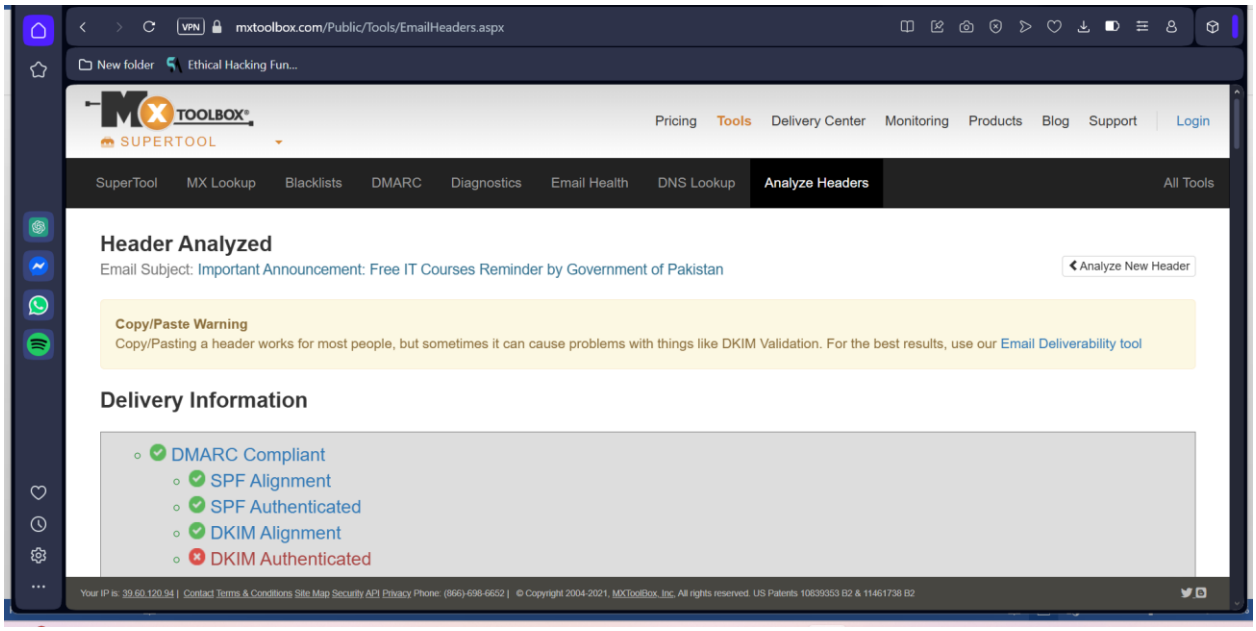


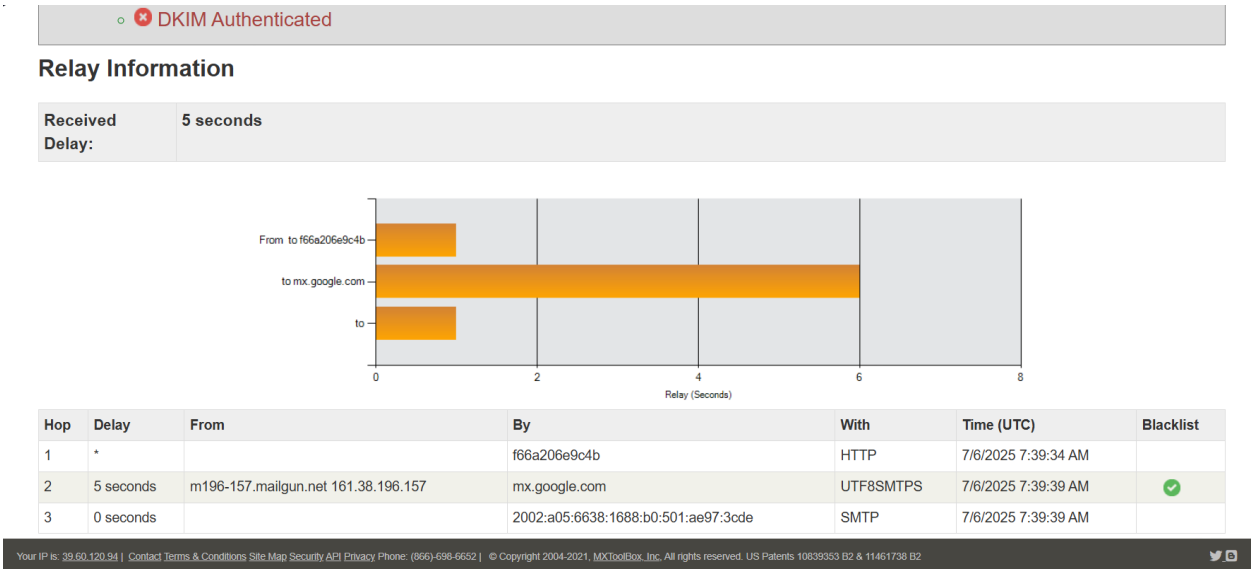
Open MXToobox Header Analyzer.

Find out if the sender is fake (spoofed) and where the email really came from.



Paste here and click Analyze after a moment, I got the output.





What is it mean?

This is a technical log (likely from a tool like MXToolbox) that tracks how an email traveled from one server to another before reaching its destination (e.g., a Gmail server). The delays show where the process slowed down, and the hops list the servers involved. The DKIM check helps confirm the email's authenticity. If the

delay is high or there's a blacklist issue, it might indicate a problem with email delivery.

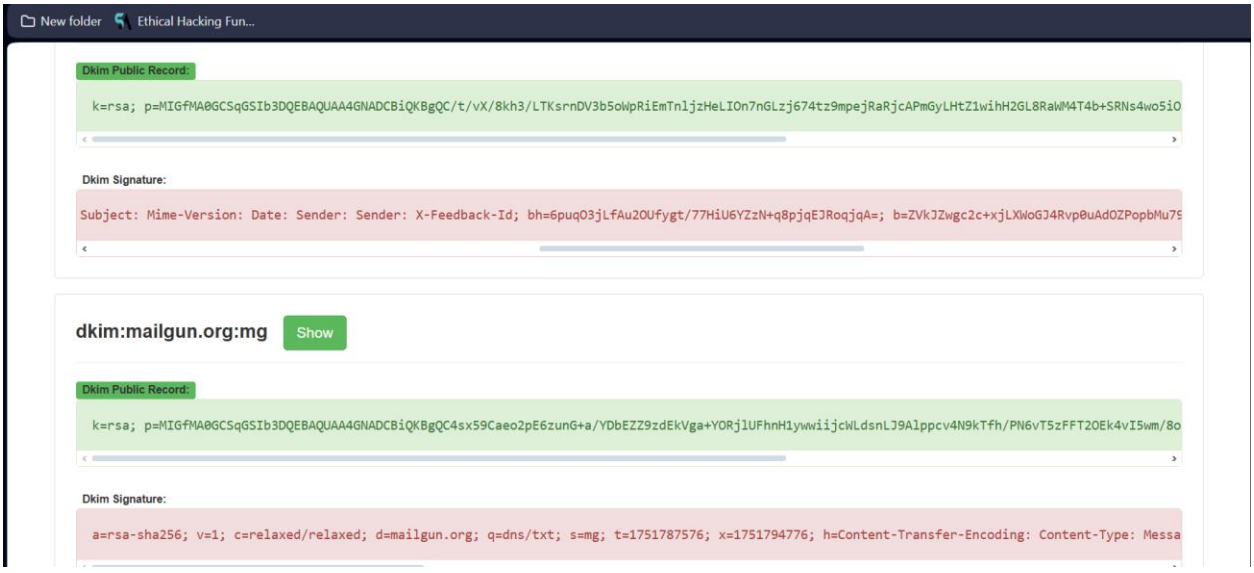
Why DKIM Authenticated Mark?

DKIM (Domain Keys Identified Mail) is a security method that adds a digital signature to an email to verify it comes from the claimed sender and hasn't been tampered with. The red "X" on "DKIM Authenticated" means the email's DKIM signature failed to verify.

Possible reasons include:

- The signature was missing or incorrect.
- The email content was altered after signing, invalidating the signature.
- The public key in the sender's DNS records doesn't match the signature.
- There was a misconfiguration in the sender's DKIM setup.

Analyze DKIM Signature



- DKIM authentication failed (red "X") for notify.thinkific.com (selector pic).

- Possible issues: Mismatch between signed content and received email, duplicate headers (To:, From:), or timestamp anomaly (future dates: t=1751787576, x=1751794776).

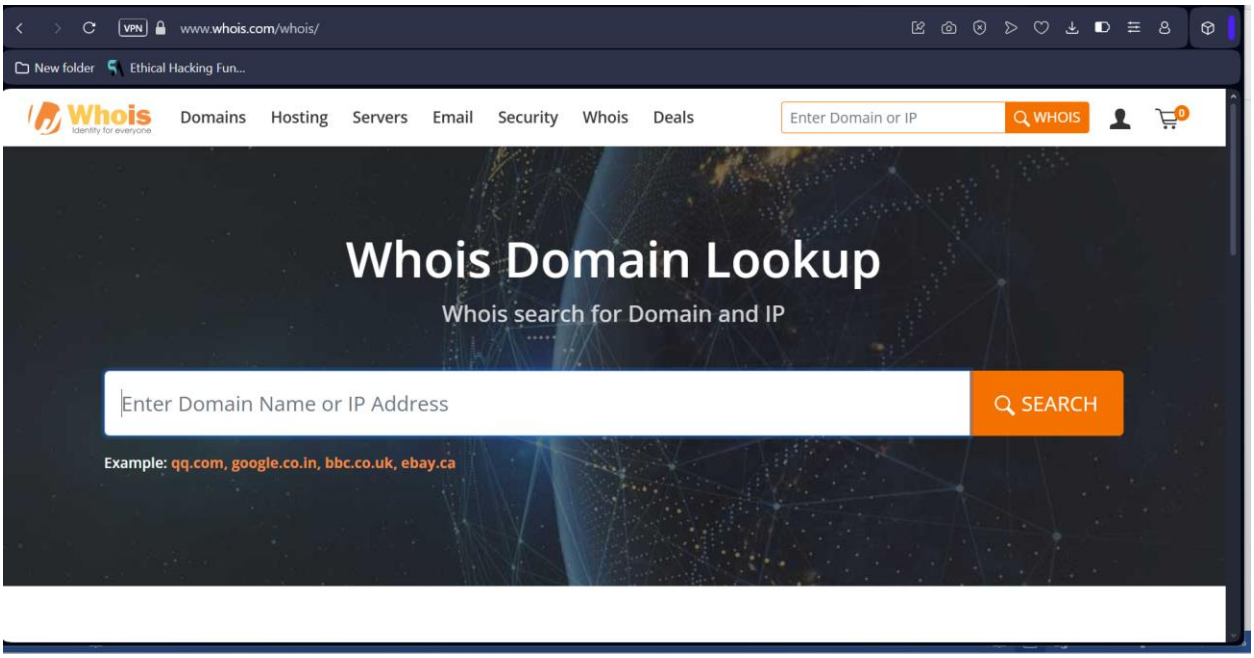
- Verify DNS record at pic._domainkey.notify.thinkific.com matches the public key.

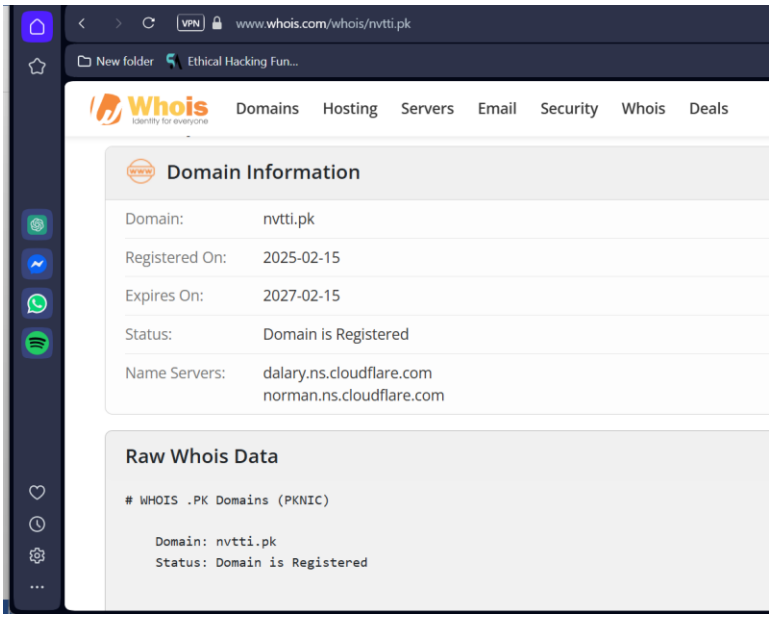
Step 2: Check the Domain and Email Address

Find out if the domain nvtti.pk is **real** or **fake**.

By using tool like (View DNS, Whose.com etc.)

I open Whose.com and enter nvtti.pk





Raw Whois Data

```
# WHOIS .PK Domains (PKNIC)

    Domain: nvtti.pk
    Status: Domain is Registered


    Creation Date: 2025-02-15
    Expiry Date: 2027-02-15
    Name Server: dalary.ns.cloudflare.com
    Name Server: norman.ns.cloudflare.com
    Name Server:
    Name Server:
```

Step 3 Result Domain Analysis

Registered On:

15 February 2025 This domain is **very new** (only a few months old), which is a **red flag** for phishing.

Expires On:

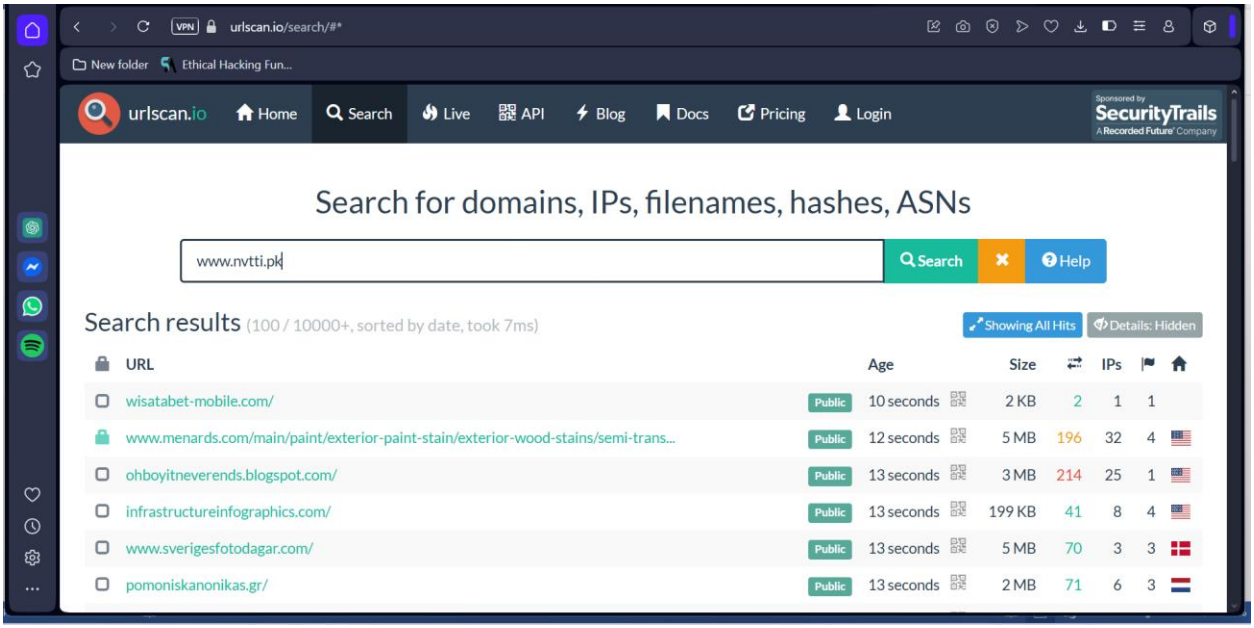
15 February 2027 Normal 2-year registration (common for both real and fake domains

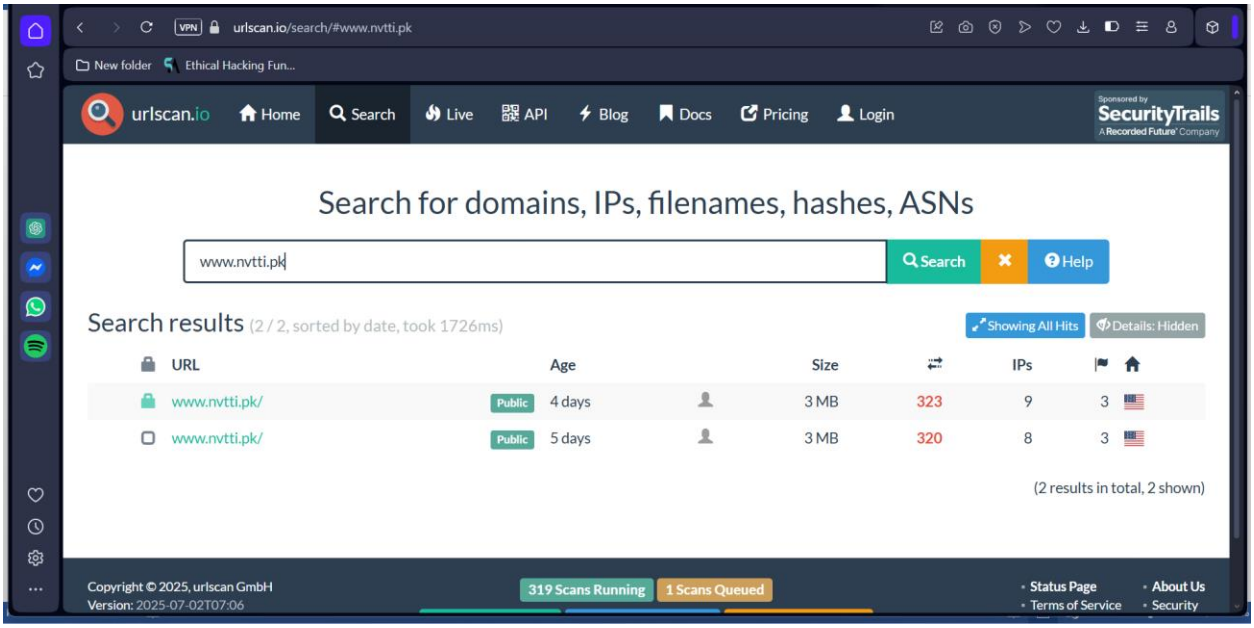
Name Servers:

- dalary.ns.cloudflare.com
- norman.ns.cloudflare.com
  Using **Cloudflare** is normal, but phishers often use it to hide the real server.

Step 4: Scan the website

For Using URLScan.io





Results:

Key Observations from URLScan.io:

- **Domain scanned 4–5 days ago** (recent activity)
- **Site size is 3 MB** indicates a fully loaded page (possibly with forms, scripts, etc.)
- **High request count:**

- **323 and 320 requests** made by the website during load **very high**, suggesting:
    - Tracking scripts
    - Redirections
    - Possibly malicious or obfuscated JavaScript
- **Multiple IPs and requests from the U.S.**
  While not inherently bad, this is unusual for a site pretending to be from the **Government of Pakistan**.

Now again Analyze orginal Message.

```
Delivered-To: saadnaveed524@gmail.com
Received: by 2002:a05:6638:1688:b0:501:ae97:3cde with SMTP id
f8csp6824902jat;
        Sun, 6 Jul 2025 00:39:39 -0700 (PDT)
X-Google-Smtp-Source:
AGHT+IGX1FeNHCyztR1/6rqG1ExtrI4osneZjO2lT9G+2bcdtdCmU8ZWlSkehgIUvenuRp38VN
bY
X-Received: by 2002:a17:903:15cf:b0:235:1b3e:c01c with SMTP id
d9443c01a7336-23c875ac9d6mr98786165ad.39.1751787579612;
        Sun, 06 Jul 2025 00:39:39 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1751787579; cv=none;
        d=google.com; s=arc-20240605;

b=VdbGBrGqDTPkuASBzBwM3+ngq4aAJDH3eymM0mH5R8OdkqlN426xPVyCKhCWdlX3Zk

VKj8R+evMSW4bjvrQ2TFXax6vEcVscJpVT7/A9OjIc9kT+0BYSK2CJHzQrH1YiWDIjBV

gSUWndfasHWg974h+e1v2zJMCHzqeTqVTf97PCn54Jf11Fh4tC+pFv4w6QJ/50wzl/p+

sVf1VqIL+3gG7vBCBpOLwiHXP7G0HgJDtccBKyBlzlyYawBQLAPWyssztn0tWORGFUSH

abi0NmlVrJDx3R3q0QCh5ZvsYLJtWgBMGYOBS3bgJogUjjfbbaKu0OWuG3w3w2DSjdmT
         0Lkw==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com;
s=arc-20240605;
        h=content-transfer-encoding:message-id:reply-to:to:from:subject
         :mime-version:date:sender:dkim-signature:dkim-signature;
        bh=6puqO3jLfAu2OUfygt/77HiU6YZzN+q8pjqEJRoqjqA=;
        fh=WEtwMaZX9LBA6DxcItjJBTYKSaFZn/q6pDZQOab7khQ=;

b=fRrbAPpXqodisA+fSDjhuRIU3coe0B6+J30o+RoNzvtuGw5dFVAWbIVWTYwxK45KmX

z6jJJzO7RRJktyetS7enA4ovLU5l3CnTKSTumJGTend+W2odWo/gFyhBx03wnHlpwria

U/pO0na0hc/Wrqdfz4Pm/CqtnYTjM8fK6RMcVLL8r+2oFNQbQ61YRn/Kic693OP+viiy

ZOrwL60TZJRxHMsM/QRZtv2/FePN5zPmtMh6Z6B3nPb6mAvLj4ULpaz7z4IVdEkPOkG1
```

```
6Tqjw2sAym41zZeHIXzwbWcenovizS1agLqZZXUfaxGyfNnWTZyFAnQduqQuIJwfHXlI
         jH3A==;
        dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       dkim=pass header.i=@notify.thinkific.com header.s=pic
header.b=ZVkJZwgc;
       dkim=pass header.i=@mailgun.org header.s=mg header.b=s36Y28cB;
       spf=pass (google.com: domain of bounce+ac8d78.acf2a2-
saadnaveed524=gmail.com@notify.thinkific.com designates 161.38.196.157 as
permitted sender) smtp.mailfrom="bounce+ac8d78.acf2a2-
saadnaveed524=gmail.com@notify.thinkific.com";
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=thinkific.com
Return-Path: <bounce+ac8d78.acf2a2-
saadnaveed524=gmail.com@notify.thinkific.com>
Received: from m196-157.mailgun.net (m196-157.mailgun.net.
[161.38.196.157])
        by mx.google.com with UTF8SMTPS id d9443c01a7336-
23c84526f5asi81511715ad.287.2025.07.06.00.39.39
        for <saadnaveed524@gmail.com>
        (version=TLS1_2 cipher=ECDHE-ECDSA-AES128-GCM-SHA256
bits=128/128);
        Sun, 06 Jul 2025 00:39:39 -0700 (PDT)
Received-SPF: pass (google.com: domain of bounce+ac8d78.acf2a2-
saadnaveed524=gmail.com@notify.thinkific.com designates 161.38.196.157 as
permitted sender) client-ip=161.38.196.157;
Authentication-Results: mx.google.com;
       dkim=pass header.i=@notify.thinkific.com header.s=pic
header.b=ZVkJZwgc;
       dkim=pass header.i=@mailgun.org header.s=mg header.b=s36Y28cB;
       spf=pass (google.com: domain of bounce+ac8d78.acf2a2-
saadnaveed524=gmail.com@notify.thinkific.com designates 161.38.196.157 as
permitted sender) smtp.mailfrom="bounce+ac8d78.acf2a2-
saadnaveed524=gmail.com@notify.thinkific.com";
       dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=thinkific.com
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed;
d=notify.thinkific.com; q=dns/txt; s=pic; t=1751787576; x=1751794776;
h=Content-Transfer-Encoding: Content-Type: Message-Id: reply-to: To: To:
From: From: Subject: Subject: Mime-Version: Date: Sender: Sender: X-
Feedback-Id; bh=6puqO3jLfAu2OUfygt/77HiU6YZzN+q8pjqEJRoqjqA=;
b=ZVkJZwgc2c+xjLXWoGJ4Rvp0uAdOZPopbMu793c0qIKZkhdQi2/h5ywH5VmqFfPK2w++0Den
Mak+BSpsV50WIPRILUVUkRG283NQ9pxoEMLj3TRDnW9VEseQEKI81AMjbaUJTcJCOCrHNNilYP
c1JO/OPSSnFVhCYCmsSgIaIw0=
DKIM-Signature: a=rsa-sha256; v=1; c=relaxed/relaxed; d=mailgun.org;
q=dns/txt; s=mg; t=1751787576; x=1751794776; h=Content-Transfer-Encoding:
Content-Type: Message-Id: reply-to: To: To: From: From: Subject: Subject:
Mime-Version: Date: Sender: Sender: X-Feedback-Id;
bh=6puqO3jLfAu2OUfygt/77HiU6YZzN+q8pjqEJRoqjqA=;
b=s36Y28cB5398pDQGQYjD2Iwe0G/OFjMyUsg5A0BwD7gGuwwGd2vj+jv6xoKjY+iaFjpM2xnp
qt0f0XTyJxqio2SA3Qjd/t1HgERg7Be0Bh4x0FwKkOhXYyc3G6LNJIzShJGSudRHLxZny/+1e3
rbvDF4cqlcOJavFP3PKrB1QBU=
X-Mailgun-Sid:
WyIxMTliNCIsInNhYWRuYXZlZWQ1MjRAZ21haWwuY29tIiwiYWNmMmEyIl0=
```

X-Feedback-Id:
noreply@notify.thinkific.com::58a0a4d14f41fe032fc453d3:mailgun
Received: by f66a206e9c4b with HTTP id 686a2838b617a8e21e8e2e59; Sun, 06
Jul 2025 07:39:34 GMT
X-Mailgun-Sending-Ip: 161.38.196.157
X-Mailgun-Batch-Id: 686a283659e4417f220826e7
Sender: noreply@notify.thinkific.com
Date: Sun, 06 Jul 2025 07:39:34 +0000
Mime-Version: 1.0
Subject: Important Announcement: Free IT Courses Reminder by Government of
Pakistan
**From: "NVTTI - National Vocational & Technical Training Initiative"
<noreply@notify.thinkific.com>**
To: "'Saad Naveed'" <saadnaveed524@gmail.com>
reply-to: enquiries.department@nvtti.pk
Message-Id: <20250706073934.60c502289d87bbc3@notify.thinkific.com>
Content-Type: text/html; charset="utf-8"
Content-Transfer-Encoding: quoted-printable

<title>Registration Reminder from NVTTI</title> <div style=3D"max-
wid=
th: 600px; margin: 30px auto; background: #ffffff; border: 1px solid
#d0e5d=
8; border-radius: 6px; overflow: hidden; box-shadow: 0 4px 8px rgba(0, 80,
=
30, 0.1);"><!-- Header --><div style=3D"background-color: #014421;
padding:=
 20px 25px; text-align: center;"><h1 style=3D"color: #d9f0d9; font-weight:
=
bold; margin: 0; font-size: 24px; letter-spacing: 1.2px; font-family:
'Sego=
e UI', Tahoma, Geneva, Verdana, sans-serif;">National Vocational &
Tech=
nical Training Initiative</h1><p style=3D"color: #a6c8a6; font-size: 14px;
=
margin: 6px 0 0; font-style: italic;">Government of Pakistan <!--
=
Body --><div style=3D"padding: 30px 35px; line-height: 1.7; font-size:
16px=
; color: #1b3b1b;"><h2 style=3D"color: #014421; font-weight: bold; text-
ali=
gn: center; margin-top: 0; border-bottom: 3px solid #a6c8a6; padding-
bottom=
: 8px;">Registration Reminder</h2> Dear Applicant, This is a
remind=
er that registrations for the <strong style=3D"color: #014421;">FREE IT
ski=
lls courses offered by the Government of Pakistan through NVTTI
ar=
e still open. To complete your registration, please visit the NVTTI
w=
ebsite at your earliest convenience: <p style=3D"text-align:
center;"><a=

```
href=3D"https://email.notify.thinkific.com/c/eJwcy0mOhSAQANDTwJIUxVCwYNEb7
=
8HYEhVNSzR9-
5_8A7wSYm4YkdcgyUhyZMjyNeiYbHLVNKec1NKTJQPeVk0esFjkPSCgAQILpLzS=
wkI2gOh8cZRSVkzDOGdv_2KufWy99SzyefA9rHNeN1M_DBeGy_u-
YjxzdnFt_C_cMZYRn1qLQc0=
0_B6x71_4BPwEAAD__x8rMr8" rel=3D"noopener" style=3D"background-color:
#a6c8=
a6; color: #014421; font-weight: bold; text-decoration: none; padding:
10px=
 20px; border-radius: 4px; display: inline-block; border: 2px solid
#014421=
; transition: background-color 0.3s ease;" target=3D"_blank">Visit
www.nvtt=
i.pk</a></p><p>If you need assistance, feel free to contact us at <a href=
=3D"mailto:enquiries.department@nvtti.pk" style=3D"color: #014421; font-
wei=
ght: 600; text-decoration:
none;">&amp;nbsp;enquiries.department@nvtti.pk&amp;nbsp;=
</a>.</p><p>Thank you for your attention.</p><p>Best
regards,<br><strong>Na=
tional Vocational &amp;amp; Technical Training Initiative
(NVTTI)</strong><br><=
strong>www.nvtti.pk&amp;nbsp;</strong></p></div><!-- Footer --><div
style=3D"ba=
ckground-color: #e6f0e6; color: #537153; font-size: 12px; text-align:
cente=
r; padding: 15px 25px; border-top: 1px solid #d0e5d8;">&amp;copy; 2025 NVTTI.
A=
ll rights reserved.</div></div><img width=3D"1" height=3D"1" alt=3D"" src=
=3D"https://email.notify.thinkific.com/o/eJwcyVEOgyAMANDTyKcplVL44DC1lNlsa
r=
IZk91-
yb5fb6IDBYO1yBS5MHEOW7OiRXIkTjqgkzFWrJUwS1nFIgRvCEjAkIGXuqQ5gxIgltoLr=
6suU4LjvHx852vz4-nDddZzD-_2EemH3GadME0JHrv46293w18AAAD__y8gKc0">
```


Key Observations:

Return Path & Envelope From**:**

Return-Path: <bounce+ac8d78.acf2a2-saadnaveed524=gmail.com@notify.thinkific.com>

The real email was sent **from** notify.thinkific.com, not nvtti.pk.

SPF Pass

spf=pass (google.com: domain of bounce+ac8d78.acf2a2-saadnaveed524=gmail.com@notify.thinkific.com designates 161.38.196.157 as permitted sender)

SPF is **valid**, but for notify.thinkific.com

DKIM

```
dkim=pass header.i=@notify.thinkific.com header.s=pic header.b=ZVkJZwgc;
       dkim=pass header.i=@mailgun.org header.s=mg header.b=s36Y28cB;
```

DKIM also passes again, for notify.thinkific.com and mailgun.org.

DMARC

```
dmarc=pass (p=REJECT sp=REJECT dis=NONE) header.from=thinkific.com
```

DMARC passes also for thinkific.com.

Red Flag Address Mismatch

```
From: "NVTTI - National Vocational & Technical Training Initiative"
<noreply@notify.thinkific.com>
To: "'Saad Naveed'" <saadnaveed524@gmail.com>
reply-to: enquiries.department@nvtti.pk
```

- **Display Name** pretends to be a government institute.
- But the real sender address is from **Thinkific**, an online course platform.
- The **Reply-To** is nvtti.pk, a suspicious domain created recently.

IP Used:

```
Received: from m196-157.mailgun.net (m196-157.mailgun.net.
[161.38.196.157])
```

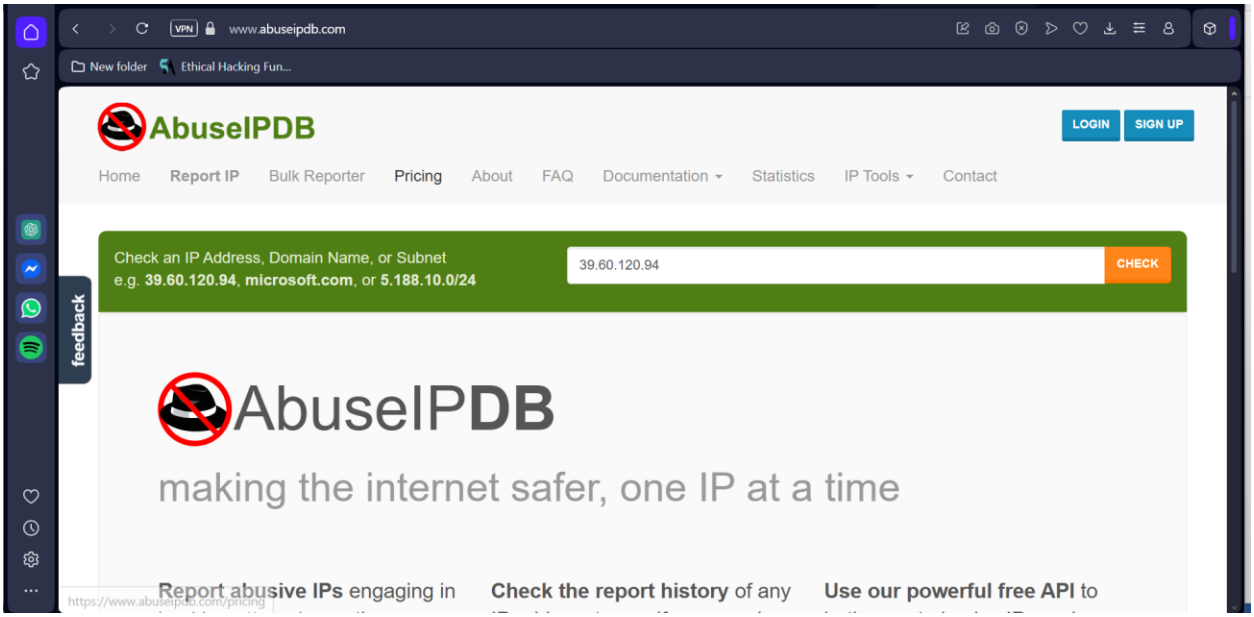
Step 5: IP Scan

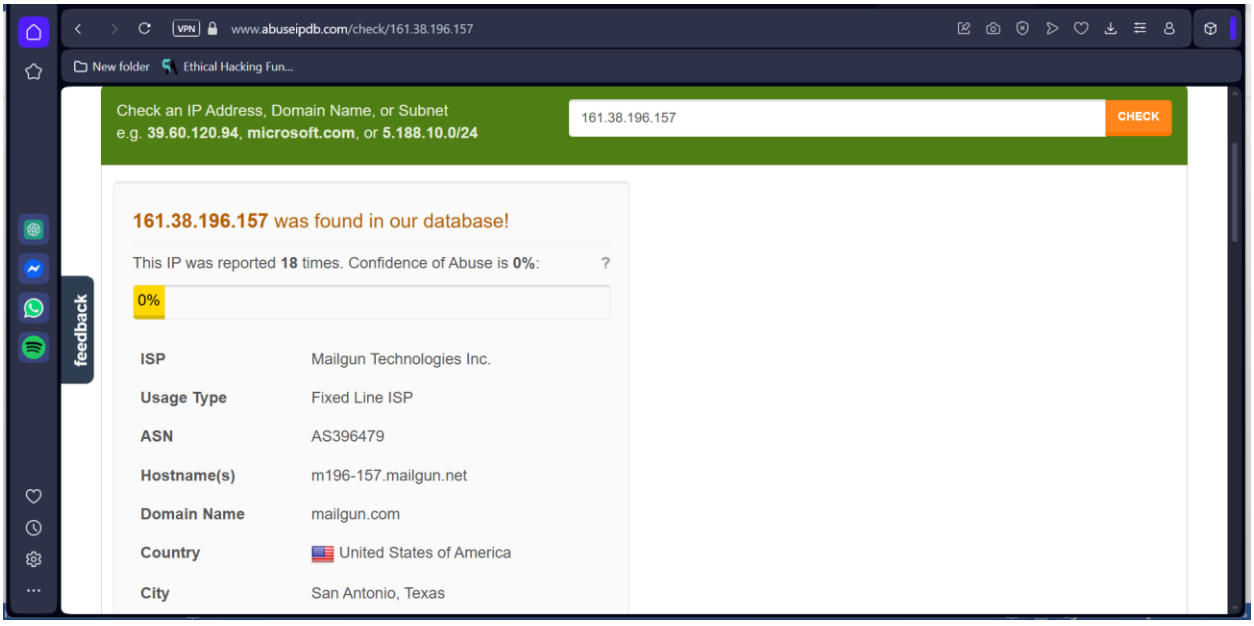
Using Tool AbuseIPDB.

AbuseIPDB is a free threat intelligence tool that helps identify **malicious or suspicious IP addresses**. It uses **crowdsourced reports** to flag IPs involved in:

- Hacking attempts
- Spam
- DDoS attacks
- Brute-force logins
- Phishing

Purpose: To check whether an IP address is involved in cybercrime activity.



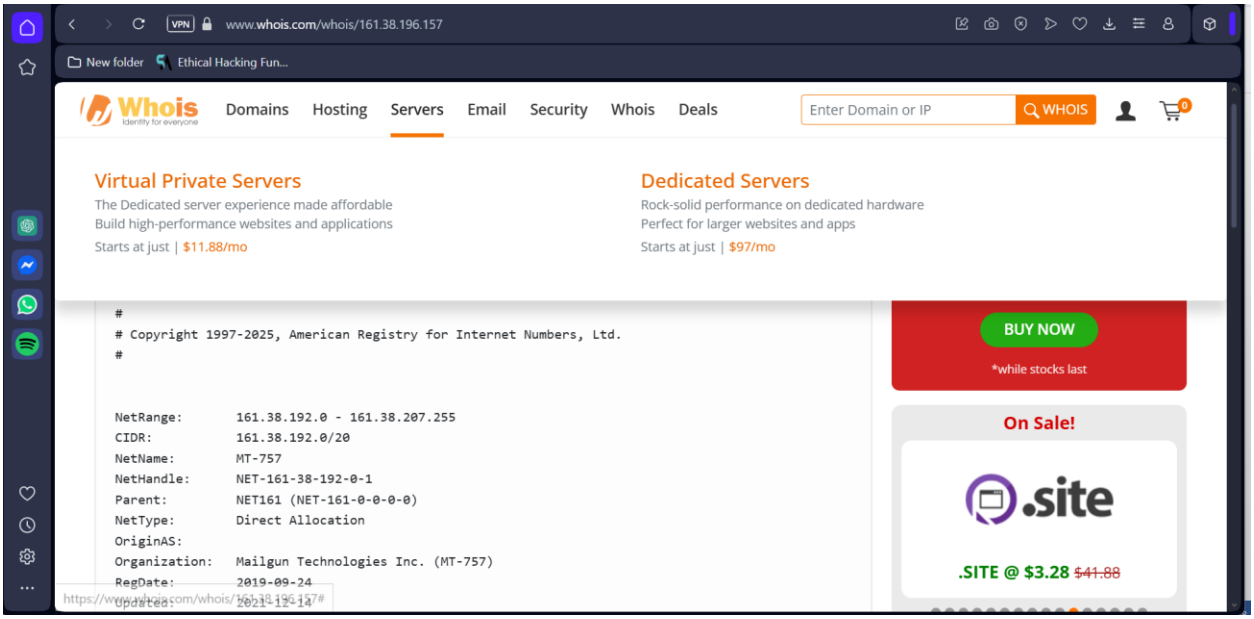


What This Means:

- The email was **sent using Mailgun** (a bulk mailing service).
- Although the IP **was reported 18 times**, the system is **not 100% confident** it's abusive maybe because it’s also used by legitimate users.

Still Suspicious **because the email is pretending** to be from the Government of Pakistan but is actually:

- Sent via **Thinkific + Mailgun**
- Has a **new fake-looking domain** nvtti.pk
- Uses a **mismatched reply-to address**



Results

IP: 161.38.196.157 – WHOIS Summary

Field	Details
Owner	Mailgun Technologies Inc.
Address	112 E Pecan St #1135, San Antonio, Texas, USA
Network Range	161.38.192.0 - 161.38.207.255
Registered Since	September 24, 2019
Purpose	Bulk Email Sending Services
Abuse Contact	email@mailgun.org +1-888-571-8972

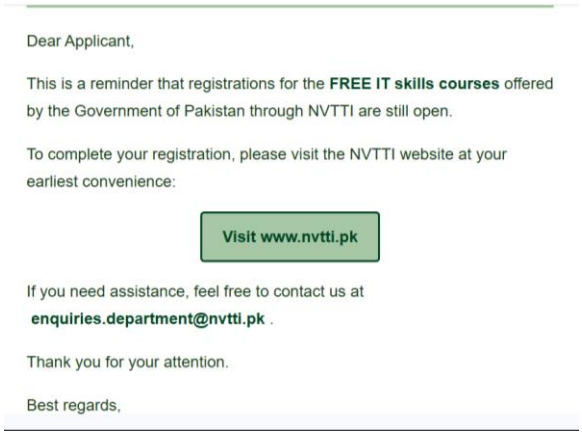
What Does This Mean?

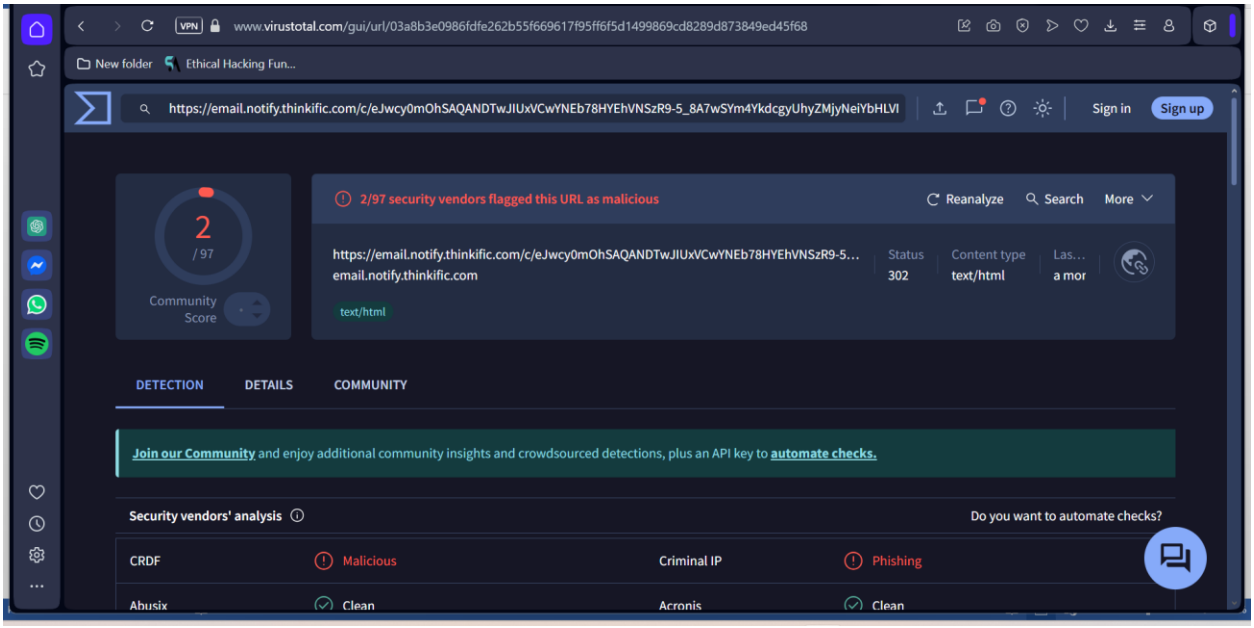
- This IP address **belongs to Mailgun**, a U.S.-based email delivery service used by many companies for sending newsletters, alerts, course reminders, etc.

- The **spoofed email you received came through Mailgun**, possibly via Thinkific or another service.
- While the server is **located in Texas, USA**, the **real attacker could be anywhere in the world** (even Pakistan or India).

Step 6: Analysis URL.

Right-click on the tab (visit www.nvtti.pk), copy the link address, and paste it into VirusTotal, a tool that analyzes malicious content including emails.





This is showing malicious.

Conclusion

After analyzing the suspicious email using multiple tools and techniques, it has been confirmed that the email is a **phishing attempt**. The message falsely claims to be from the **National Vocational & Technical Training Initiative (NVTTI)** and encourages the recipient to click on a link pretending to be a government service.

However:

- The **email was sent via Mailgun Technologies**, a U.S.-based bulk email service, not a Pakistani government server.
- The **IP address (161.38.196.157)** used belongs to Mailgun in **San Antonio, Texas**, and has been reported multiple times.
- The **link provided in the email was scanned on VirusTotal** and flagged as **malicious**, indicating it may lead to phishing, malware, or credential harvesting.
- The **domain** nvtti.pk may be **fake, compromised, or misused** to impersonate a government platform.