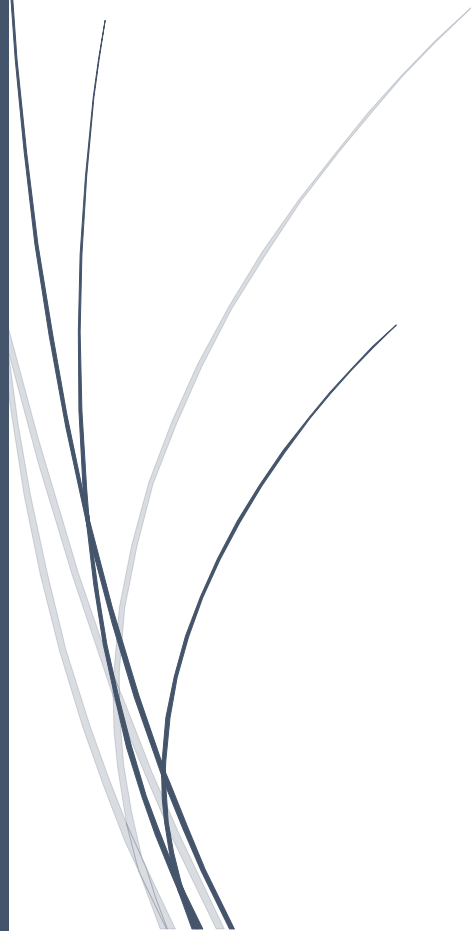
8/5/2025

Analysis of Phishing Emails

Using MX Tools, VirusTotal



@SRCybersecurity

Task 2: Analyse a Phishing Email Sample.

Objective: Identify phishing characteristics in a suspicious email sample.

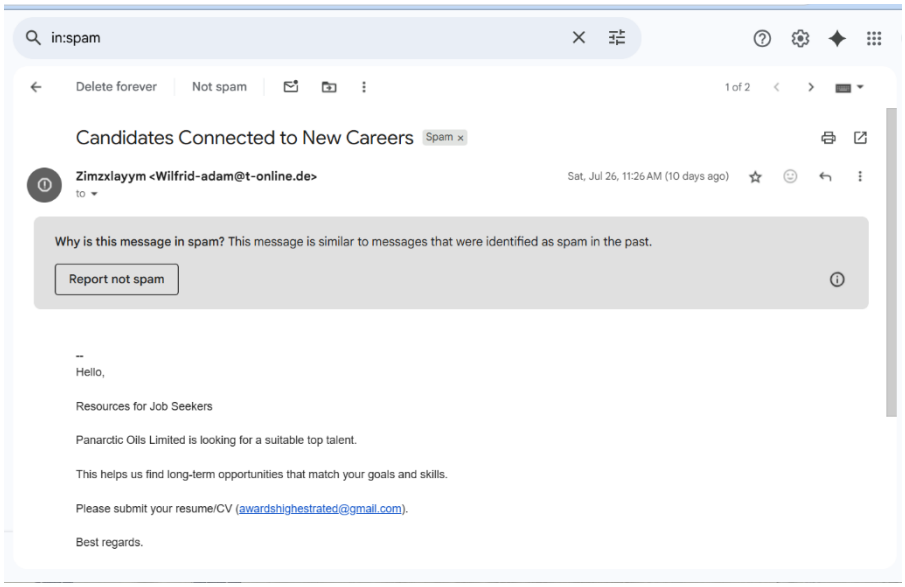
Tools: MX Lookup, VirusTotal.

1.Obtain a sample phishing email (many free samples online).

Email Body Summary:

A fake job alert pretending to be a recruiter,

- Urging: To apply for new job role by giving a limited time to become a talented top applicant.
- No phishing alert was triggered.
- Message was sent by "Unknown".
- Urging the user to send CV "To Apply".



2.Examine sender's email address for spoofing.

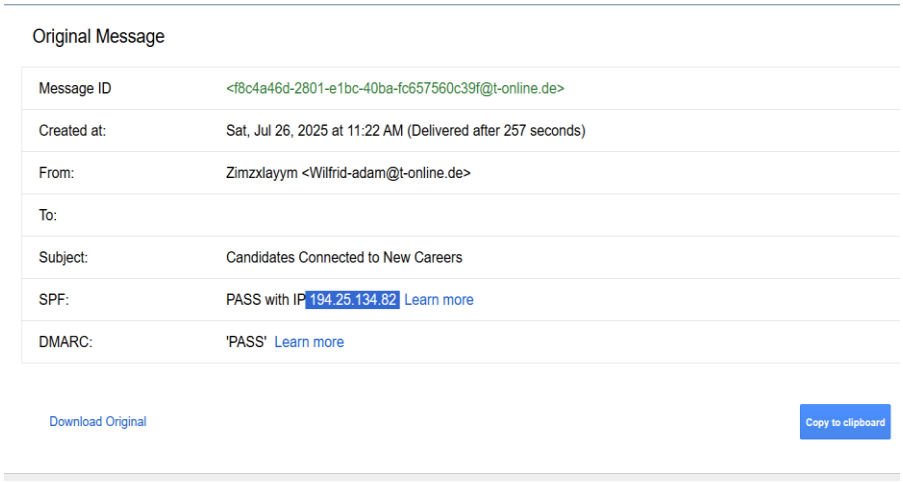
- Not found

3.Check email headers for discrepancies (using online MX Lookup).

- Deliverables: A report listing phishing indicators found

- **Full email id of sender?**

  - 194.25.134.82



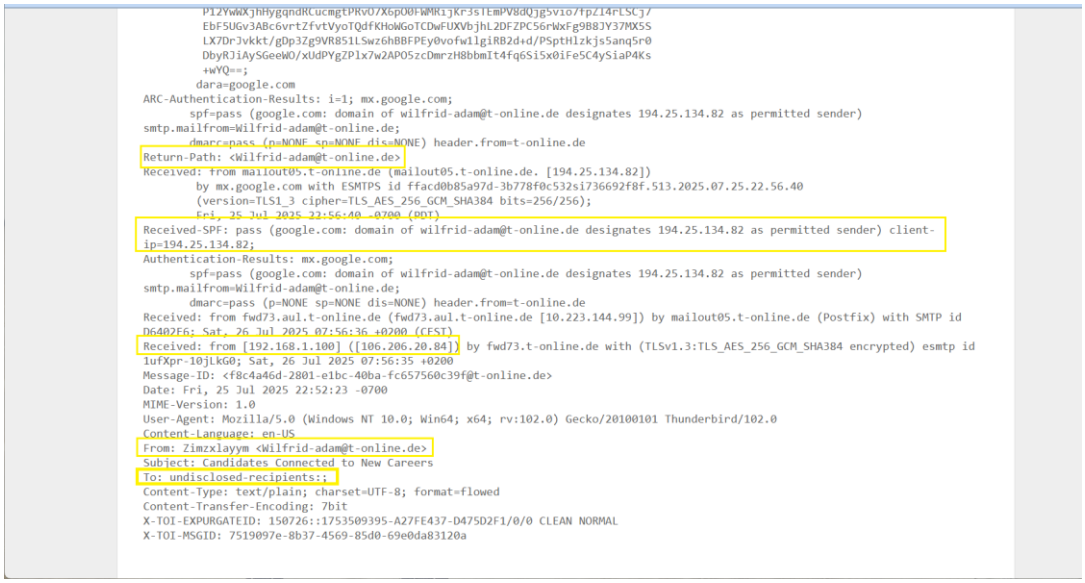
Original Message

Message ID	<f8c4a46d-2801-e1bc-40ba-fc657560c39f@t-online.de>
Created at:	Sat, Jul 26, 2025 at 11:22 AM (Delivered after 257 seconds)
From:	Zimzxlayym <Wilfrid-adam@t-online.de>
To:	
Subject:	Candidates Connected to New Careers
SPF:	PASS with IP 194.25.134.82 Learn more
DMARC:	'PASS' Learn more

Download Original

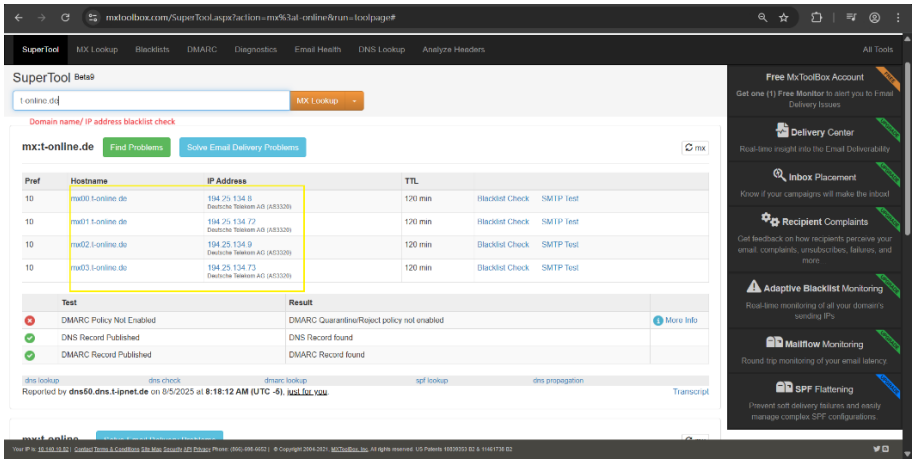
Copy to clipboard

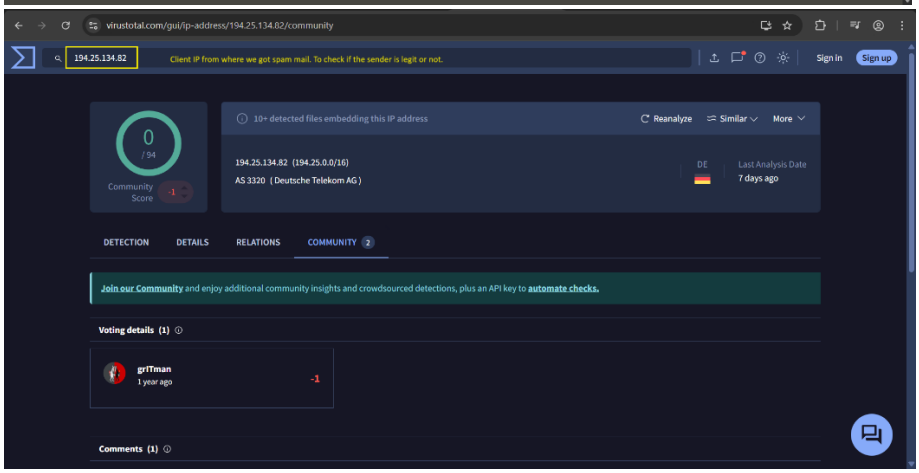
- **What domain is used to send this mail? (Return path/ From)**
  - wilfrid-adam@t-online.de



```
          P12YwWXjhHygqndRCucmgtPRvO7X6pO0FWMRijKr3sIEmPV8dQjg5v1o7fpZ14rLSCj7
          EbF5UGv3ABc6vrtZfvtVyoTQdfKHoWGoTCDwFUXVbjhL2DFZPC56rWxFg9B8JY37MX5S
          LX7DrJvkkt/gDp3Zg9VR851LSwz6hBBFPEy0vofw1lgiRB2d+d/PSptHlzkjs5anq5r0
          DbyRJiAySGeeWO/xUdPYgZPlx7w2APO5zcDmrzH8bbmIt4fq6Si5x0iFe5C4ySiaP4Ks
          +wYQ==;
         dara=google.com
ARC-Authentication-Results: i=1; mx.google.com;
       spf=pass (google.com: domain of wilfrid-adam@t-online.de designates 194.25.134.82 as permitted sender)
smtp.mailfrom=Wilfrid-adam@t-online.de;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=t-online.de
Return-Path: <Wilfrid-adam@t-online.de>
Received: from mailout05.t-online.de (mailout05.t-online.de. [194.25.134.82])
        by mx.google.com with ESMTPS id ffacd0b85a97d-3b778f0c532si736692f8f.513.2025.07.25.22.56.40
        (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
        Fri, 25 Jul 2025 22:56:40 -0700 (PDT)
Received-SPF: pass (google.com: domain of wilfrid-adam@t-online.de designates 194.25.134.82 as permitted sender) client-
ip=194.25.134.82;
Authentication-Results: mx.google.com;
       spf=pass (google.com: domain of wilfrid-adam@t-online.de designates 194.25.134.82 as permitted sender)
smtp.mailfrom=Wilfrid-adam@t-online.de;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=t-online.de
Received: from fwd73.aul.t-online.de (fwd73.aul.t-online.de [10.223.144.99]) by mailout05.t-online.de (Postfix) with SMTP id
D6402F6; Sat, 26 Jul 2025 07:56:36 +0200 (CEST)
Received: from [192.168.1.100] ([106.206.20.84]) by fwd73.t-online.de with (TLSv1.3:TLS_AES_256_GCM_SHA384 encrypted) esmtp id
1ufXpr-10jlkG0; Sat, 26 Jul 2025 07:56:35 +0200
Message-ID: <f8c4a46d-2801-e1bc-40ba-fc657560c39f@t-online.de>
Date: Fri, 25 Jul 2025 22:52:23 -0700
MIME-Version: 1.0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/20100101 Thunderbird/102.0
Content-Language: en-US
From: Zimzxlayym <Wilfrid-adam@t-online.de>
Subject: Candidates Connected to New Careers
To: undisclosed-recipients:;
Content-Type: text/plain; charset=UTF-8; format=flowed
Content-Transfer-Encoding: 7bit
X-TOI-EXPURGATEID: 150726::1753509395-A27FE437-D475D2F1/0/0 CLEAN NORMAL
X-TOI-MSGID: 7519097e-8b37-4569-85d0-69e0da83120a
```

- **Sender IP address blacklisted or not? (VirusTotal, MX Lookup)**
  - IP address is not flagged or blacklisted yet.



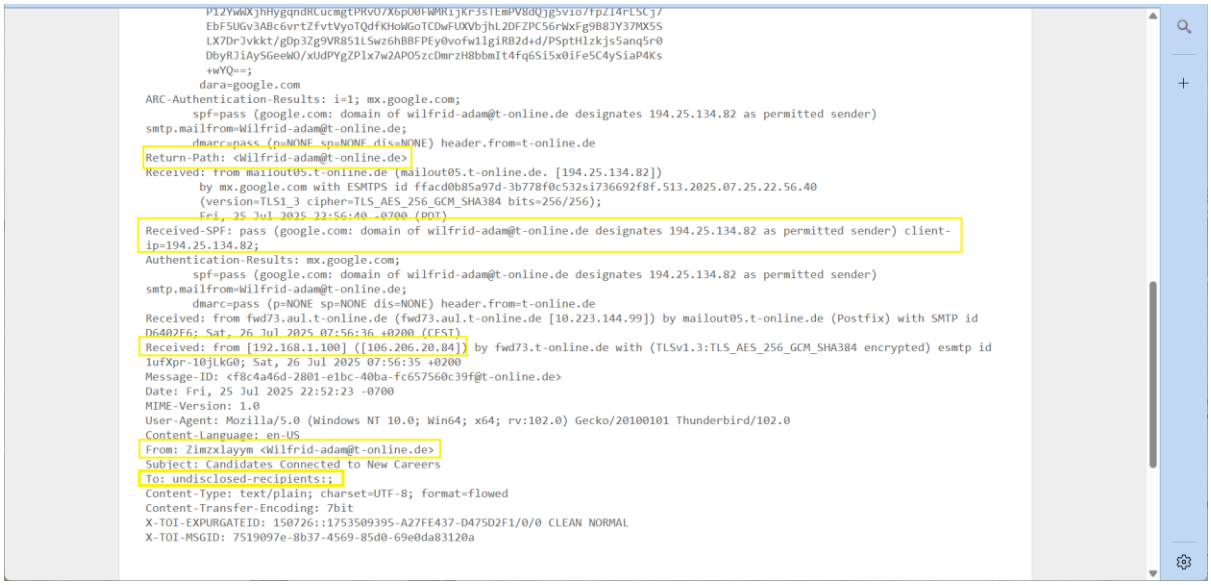


- **What is the status of SPF Authentication Result?**

Status	Description
pass	The sending IP is authorized by the domain's SPF record. This is a successful SPF check.
fail	The sending IP is not authorized to send on behalf of the domain. Usually triggers rejection or spam filtering.
softfail	The IP is probably not authorized. The domain's SPF record includes a ~all mechanism (soft fail). Treated as suspicious, but usually not rejected outright.
neutral	No explicit authorization result. The domain's SPF record uses? all. Mail may still be accepted.
none	The domain has no SPF record. No authentication was possible.

Status	Description
permerror	Permanent error in the SPF record (e.g. syntax error). SPF cannot be evaluated.
temperror	Temporary error (e.g. DNS lookup failure). SPF check could not complete. Retry may succeed later.

SPF (Sender Policy Framework) to authenticate sender mail exchange server Ip address to avoid spam. If the result is pass then it has designated client id or they might have used new legitimate email id and hasn't been blacklisted yet.



- **Is anything suspicious found in the email?**
  - Yes
  - Dkim Signature Error: No DKIM-Signature header found
  - Dkim Signature Error: There must be at least one aligned DKIM-Signature for the message to be considered aligned.

4.Identify suspicious links or attachments.

- Not Found

5.Look for urgent or threatening language in the email body.

- Yes**,** urging to apply for new job role by giving a limited time to become a talented top applicant.

6.Note any mismatched URLs (hover to see real link).

- No

7.Verify presence of spelling or grammar errors.

- Not many grammatical mistakes, but lacks authenticity of the job recruiter's id.

8.Summarize phishing traits found in the email.

- Using legitimate new email id that hasn't been blacklisted to avoid getting blocked or filtered. No Personalization, no name, user ID, or specific reference is used — shows it's a mass-mailed phishing attempt.

Conclusion:

This email shows clear signs of phishing:

- Not an authenticated sender identity

- Urgent content.

- Misleading content to gain personal information.

- Lack of personalization

- Signature failure (DKIM)

Action Recommended:

- Do NOT send your personal information (CV) in the given id in the email.

- Report the email to your IT/Security team or email provider.

- Mark it as "Phishing" or "Spam" in your email client.

THANK YOU

END