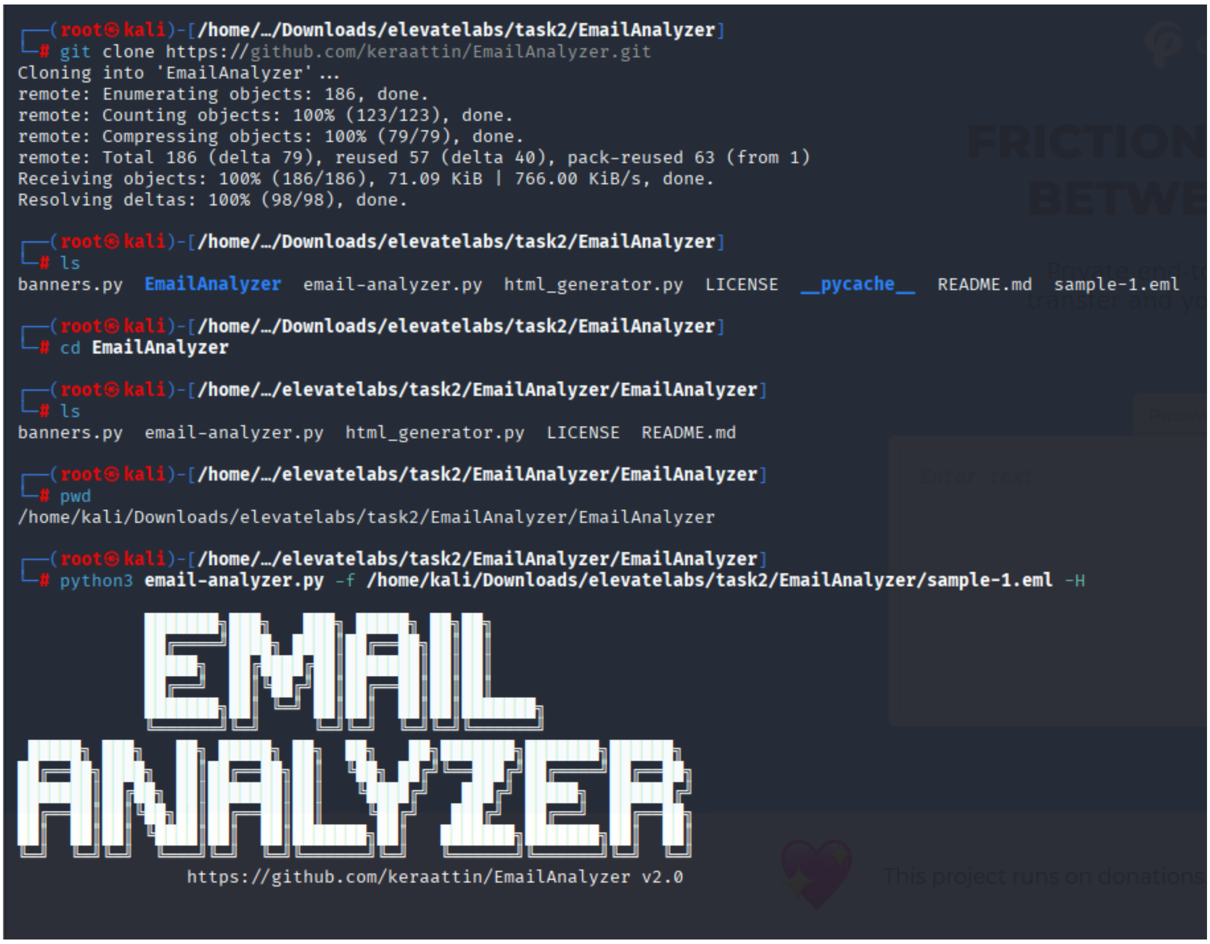
HARSH GUPTA
ELEVATE LABS CYBERSECURITY INTERNSHIP

TASK DAY-2: **<u>Analyze a Phishing Email Sample. Objective: Identify phishing characteristics in a suspicious email sample. Tools: Email client or saved email file (text), free online header analyzer. Deliverables: A report listing phishing indicators found .</u>**

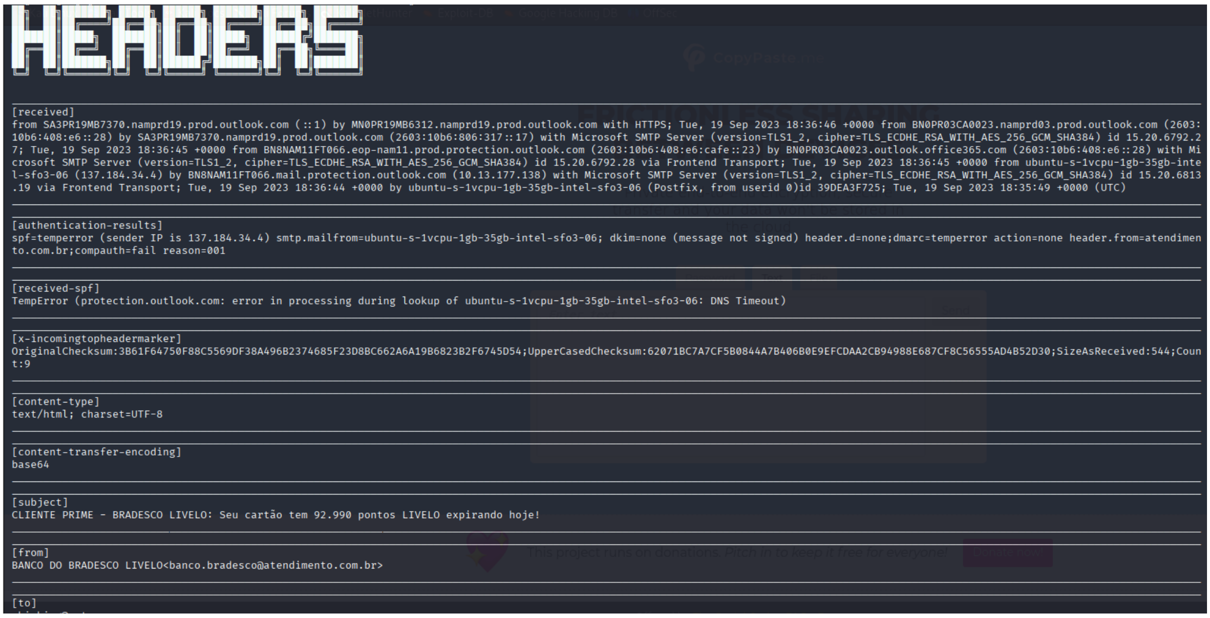
Step 1: Obtain a Sample Phishing Email

For this task I am using https://github.com/rfpeixoto/phishing_pot/blob/main/email/sample-1.eml as an sample email.

Step 2: Analyze the Email Using EmailAnalyzer Tool in Kali Linux



```
┌──(root㉿kali)-[/home/…/Downloads/elevatelabs/task2/EmailAnalyzer]
└─# git clone https://github.com/keraattin/EmailAnalyzer.git
Cloning into 'EmailAnalyzer'...
remote: Enumerating objects: 186, done.
remote: Counting objects: 100% (123/123), done.
remote: Compressing objects: 100% (79/79), done.
remote: Total 186 (delta 79), reused 57 (delta 40), pack-reused 63 (from 1)
Receiving objects: 100% (186/186), 71.09 KiB | 766.00 KiB/s, done.
Resolving deltas: 100% (98/98), done.

┌──(root㉿kali)-[/home/…/Downloads/elevatelabs/task2/EmailAnalyzer]
└─# ls
banners.py  EmailAnalyzer  email-analyzer.py  html_generator.py  LICENSE  __pycache__  README.md  sample-1.eml

┌──(root㉿kali)-[/home/…/Downloads/elevatelabs/task2/EmailAnalyzer]
└─# cd EmailAnalyzer

┌──(root㉿kali)-[/home/…/elevatelabs/task2/EmailAnalyzer/EmailAnalyzer]
└─# ls
banners.py  email-analyzer.py  html_generator.py  LICENSE  README.md

┌──(root㉿kali)-[/home/…/elevatelabs/task2/EmailAnalyzer/EmailAnalyzer]
└─# pwd
/home/kali/Downloads/elevatelabs/task2/EmailAnalyzer/EmailAnalyzer

┌──(root㉿kali)-[/home/…/elevatelabs/task2/EmailAnalyzer/EmailAnalyzer]
└─# python3 email-analyzer.py -f /home/kali/Downloads/elevatelabs/task2/EmailAnalyzer/sample-1.eml -H

      EMAIL
ANALYZER
                https://github.com/keraattin/EmailAnalyzer v2.0
```



```
HEADERS

[received]
from SA3PR19MB7370.namprd19.prod.outlook.com (::1) by MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Tue, 19 Sep 2023 18:36:46 +0000 from BN0PR03CA0023.namprd03.prod.outlook.com (2603:
10b6:408:e6::28) by SA3PR19MB7370.namprd19.prod.outlook.com (2603:10b6:806:317::17) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.2
7; Tue, 19 Sep 2023 18:36:45 +0000 from BN8NAM11FT066.eop-nam11.prod.protection.outlook.com (2603:10b6:408:e6:cafe::23) by BN0PR03CA0023.outlook.office365.com (2603:10b6:408:e6::28) with Mi
crosoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.28 via Frontend Transport; Tue, 19 Sep 2023 18:36:45 +0000 from ubuntu-s-1vcpu-1gb-35gb-inte
l-sfo3-06 (137.184.34.4) by BN8NAM11FT066.mail.protection.outlook.com (10.13.177.138) with Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6813
.19 via Frontend Transport; Tue, 19 Sep 2023 18:36:44 +0000 by ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (Postfix, from userid 0)id 39DEA3F725; Tue, 19 Sep 2023 18:35:49 +0000 (UTC)

[authentication-results]
spf=temperror (sender IP is 137.184.34.4) smtp.mailfrom=ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06; dkim=none (message not signed) header.d=none;dmarc=temperror action=none header.from=atendimen
to.com.br;compauth=fail reason=001

[received-spf]
TempError (protection.outlook.com: error in processing during lookup of ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06: DNS Timeout)

[x-incomingtopheadermarker]
OriginalChecksum:3B61F64750F88C5569DF38A496B2374685F23D8BC662A6A19B6823B2F6745D54;UpperCasedChecksum:62071BC7A7CF5B0844A7B406B0E9EFCDAA2CB94988E687CF8C56555AD4B52D30;SizeAsReceived:544;Coun
t:9

[content-type]
text/html; charset=UTF-8

[content-transfer-encoding]
base64

[subject]
CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!

[from]
BANCO DO BRADESCO LIVELO<banco.bradesco@atendimento.com.br>

[to]
```

After python3 email-analyzer.py -f ../phishing_sample.eml -H -d -l -a

- -f specifies the filename
- -H extracts headers
- -d extracts digests
- -l extracts links
- -a extracts attachments

DISCREPANCIES FOUND IN THE EMAIL HEADER ARE

1. Header Fields Reviewed

- From
- Return-Path
- Received headers (including originating IP addresses)
- Authentication-Results (SPF, DKIM, DMARC)
- Subject
- Message-ID
- Date
- X-Sender-IP
- X-MS-Exchange-Organization-AuthSource
- X-MS-Exchange-Organization-AuthAs
- X-SID-PRA

2. Analysis Summary & Discrepancies Found

A. From and Return-Path Mismatch: Strong Indicator of Spoofing

- **Observation:**
    - The From: address is BANCO DO BRADESCO LIVELO<banco.bradesco@atendimento.com.br>. 1
    - The Return-Path: is root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06. 1
- **Discrepancy Indicator:** This is a significant discrepancy. The From: address attempts to impersonate "BANCO DO BRADESCO LIVELO" from the atendimento.com.br domain, which is unlikely to be the official domain for Bradesco Livelo. Crucially, the Return-Path (where bounces would go) points to root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06, a generic server name. This mismatch is a classic sign of email spoofing, where the sender's apparent identity is faked.

B. Sender IP Address and Origin: Suspicious Source

- **Observation:**
    - The email originates from ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 with IP address 137.184.34.4. 1
    - This IP is also confirmed by [x-sender-ip]: 137.184.34.4. 1
- **Discrepancy Indicator:** An email purporting to be from a financial institution like "BANCO DO BRADESCO LIVELO" should originate from their official mail servers, not a generic ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 server. This indicates an unauthorized or compromised host sending the email, a strong sign of a malicious sender. The X-MS-Exchange-Organization-AuthAs: Anonymous further confirms that the sender was not authenticated by Microsoft's mail system as a legitimate user. 1

C. Authentication Results (SPF, DKIM, DMARC): Failures and Missing Signatures

- **Observation:**
    - spf=temperror (sender IP is 137.184.34.4) smtp.mailfrom=ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06; 1
    - dkim=none (message not signed) header.d=none; 1
    - dmarc=temperror action=none header.from=atendimento.com.br;compauth=fail reason=001 1

- **Discrepancy Indicator:**
    - **SPF (Sender Policy Framework):** The temperror for SPF means the receiving server encountered a temporary error while trying to validate the sender's IP against the SPF record for ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06. Even if it were to pass, ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 is not atendimento.com.br, indicating a fundamental mismatch.
    - **DKIM (DomainKeys Identified Mail):** dkim=none (message not signed) indicates the email was not digitally signed by the purported sending domain, atendimento.com.br. This is a significant red flag for email authenticity.
    - **DMARC (Domain-based Message Authentication, Reporting & Conformance):** The dmarc=temperror action=none and compauth=fail reason=001 show that the DMARC check failed, meaning the email did not align with the atendimento.com.br domain's authentication policy. This is a critical indicator of a forged sender.

D. Subject Line: Phishing Lure

- **Observation:**
    - [subject]: CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje! 1
- **Discrepancy Indicator:** The subject line uses urgency ("expirando hoje!") and mentions a well-known financial institution ("BRADESCO LIVELO") and loyalty program points ("92.990 pontos LIVELO"). This is a common tactic in phishing emails to create a sense of urgency and trick recipients into clicking malicious links or revealing credentials.

E. Message-ID and X-MS-Exchange-Organization-AuthAs: Further Anomalies

- **Observation:**
    - [message-id]: <20230919183549.39DEA3F725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06> 1
    - [x-ms-exchange-organization-authas]: Anonymous 1
- **Discrepancy Indicator:** The Message-ID further confirms the origin from the generic ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 server. The AuthAs: Anonymous indicates that the sender was not authenticated as a legitimate user by the receiving Microsoft mail system, reinforcing the suspicious nature of the email's origin.

The online tool which I used for email to analyze email header text is https://mxtoolbox.com/Public/Tools/EmailHeaders.aspx?huid=db5d475d-7bfa-4112-b0cd-861909b50924

This report provides practical steps and user-friendly tips to help you avoid falling victim to phishing emails, using the analyzed sample as a real-world example. The email in question attempted to impersonate a trusted brand (Bradesco Livelo), used urgent language, and failed multiple security checks. By following the guidance below, you can protect yourself and your organization from similar threats.

---

1. How to Spot and Avoid Phishing Emails

A. Always Check the Sender's Email Address Carefully

- **Look for mismatches:** The sender in the sample used banco.bradesco@atendimento.com.br instead of an official bank domain (like @bradesco.com.br).
- **Be wary of lookalike domains:** Attackers often use domains that look similar to real ones (e.g., atendimento.com.br vs. bradesco.com.br).

B. Inspect the Return-Path and Technical Headers

- **Return-Path mismatch:** In this sample, the return-path was root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06, not a legitimate corporate address.
- **Tip:** If you know how, view the email headers and check if the return-path matches the sender's domain.

C. Watch for Urgent or Threatening Language

- **Example from sample:** The subject line said, "Seu cartão tem 92.990 pontos LIVELO expirando hoje!" ("Your card has 92,990 Livelo points expiring today!")
- **Tip:** Phishing emails often try to scare you into acting quickly. Pause and verify before clicking.

D. Look for Poor Grammar and Spelling

- **Tip:** Professional organizations rarely send emails with spelling or grammatical mistakes. If you spot errors, be suspicious.

E. Hover Over Links (But Don't Click!)

- **Tip:** Hover your mouse over any links to see the actual URL. If it doesn't match the company's official website, don't click.

F. Be Cautious with Attachments

- **Tip:** Never open unexpected attachments, especially from unknown senders. They may contain malware.

G. Check for Authentication Results

- **Technical users can check headers for:**
    - **SPF, DKIM, and DMARC:** In the sample, all failed or were missing. This is a red flag.
    - **Tip:** If your email client warns you about authentication failures, take it seriously.

H. Use Multi-Factor Authentication (MFA)

- **Tip:** Even if your credentials are stolen, MFA can prevent attackers from accessing your accounts.

I. Keep Software and Security Tools Updated

- **Tip:** Regularly update your operating system, browser, and antivirus software to protect against known threats.

J. When in Doubt, Verify!

- **Tip:** If you receive an email that seems suspicious, contact the organization directly using a trusted phone number or website—not the contact information in the email.

2. Practical Tips and Tricks

Tip/Trick	**How It Helps You Stay Safe**
Double-check sender address	Prevents falling for lookalike or spoofed domains
Hover over links	Reveals hidden, malicious URLs
Don’t trust urgent emails	Prevents rushed, risky actions
Don’t open unknown files	Avoids malware and ransomware
Use MFA	Adds a layer of security even if passwords are stolen
Report suspicious emails	Helps your IT team protect others in your organization

Tip/Trick	**How It Helps You Stay Safe**
Educate yourself	Awareness is your best defense against phishing

3. What To Do If You Suspect a Phishing Email

1. Do not click any links or download attachments.
2. Do not reply to the sender.
3. Report the email to your IT or security team.
4. Delete the email from your inbox and trash.
5. If you clicked a link or entered information, change your passwords immediately and inform IT.

4. Bonus: Technical Steps for Advanced Users

- **View full email headers** in your email client to check for mismatches and authentication failures.
- **Use online header analyzers** (like MXToolbox) to spot red flags.
- **Check the sender's IP address** using tools like whois or ipinfo.io to see if it matches the claimed organization.