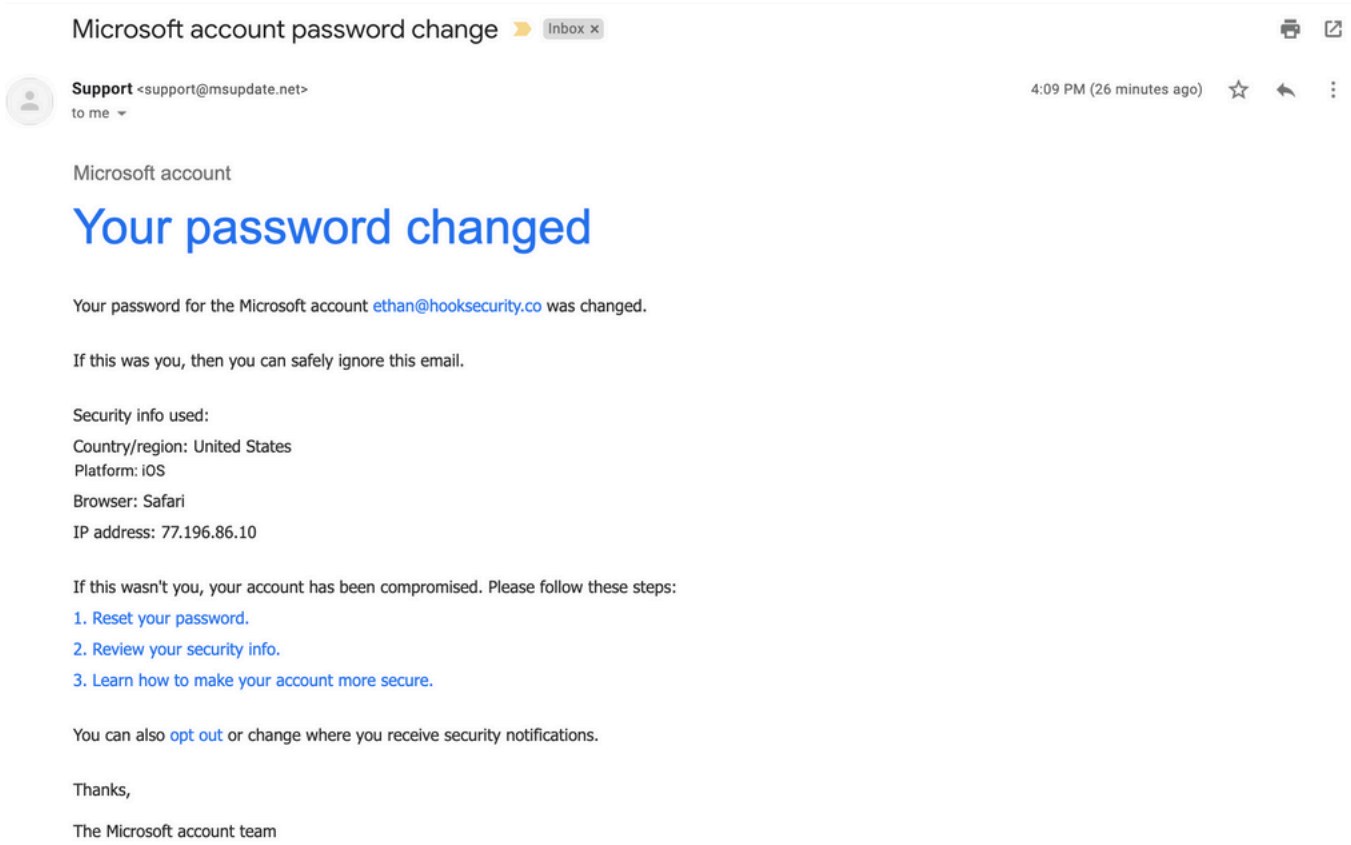
Email Phishing Analysis

Introduction:

Phishing is a trick where attackers pretend to be someone you know or trust, trying to steal your personal information. They might send you fake emails with bad links or attachments that can harm your computer. Email phishing is very common, and in this project, we will look at how to spot a phishing email and how to stay safe from it.

Phishing Email Analysis

Let's take a sample phishing email and analyze it step by step to understand how we can catch these fake emails. Here is the sample :



Microsoft account password change Inbox ×

Support <support@msupdate.net>
to me

4:09 PM (26 minutes ago)

Microsoft account

Your password changed

Your password for the Microsoft account ethan@hooksecurity.co was changed.

If this was you, then you can safely ignore this email.

Security info used:
Country/region: United States
Platform: iOS
Browser: Safari
IP address: 77.196.86.10

If this wasn't you, your account has been compromised. Please follow these steps:
1. Reset your password.
2. Review your security info.
3. Learn how to make your account more secure.

You can also opt out or change where you receive security notifications.

Thanks,

The Microsoft account team

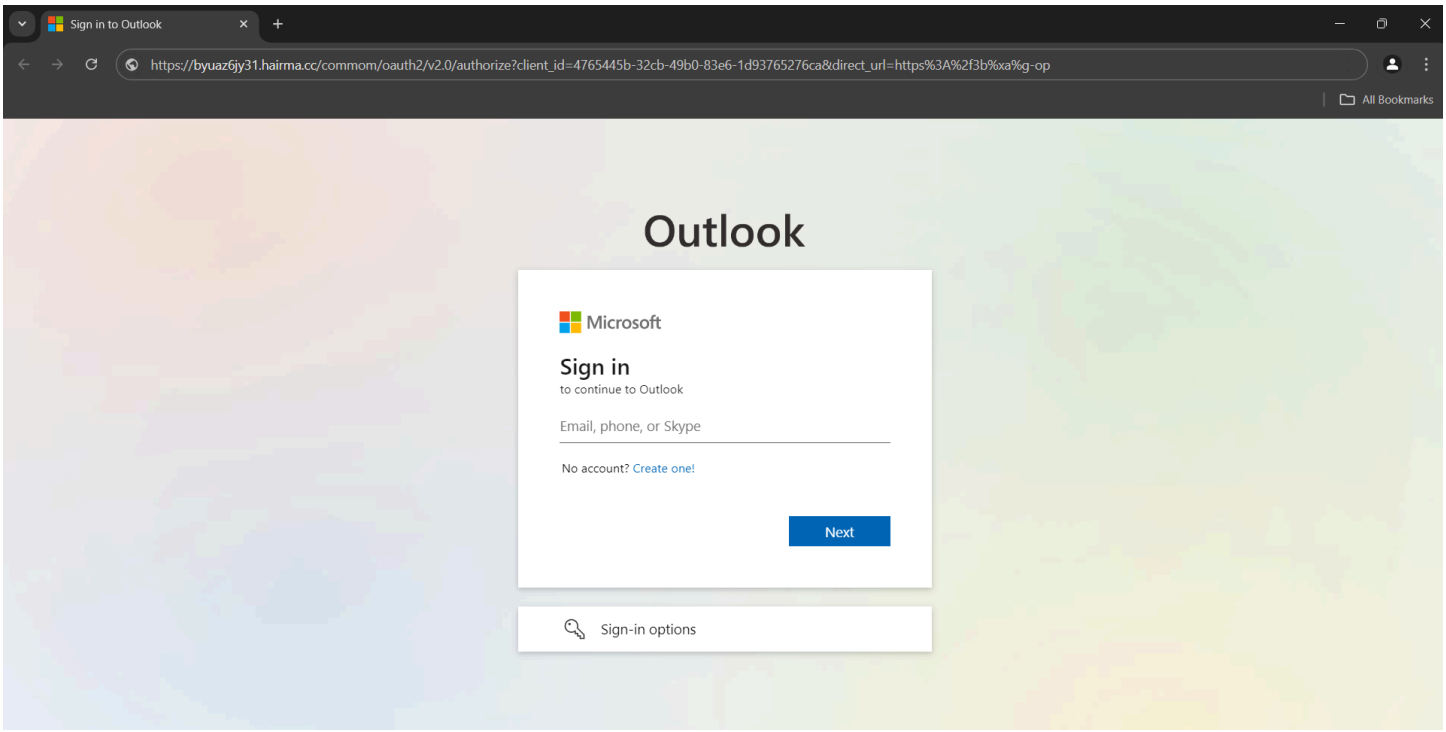
The above looks like a legitimate email but not actually . But how can we find ioc?

Step 1) Check for Attachments and Suspicious Content :

Attachments: Always check if there are any attached files, links, or images. These might be dangerous and contain harmful backdoors.

Content: Phishing emails often use urgent or scary messages to make you click on a link or open a file. If it seems too urgent or strange, it might be a phishing attempt.

when i clicked the hyperlink it actually redirected to a page that looks exactly like a legitimate page , given below:

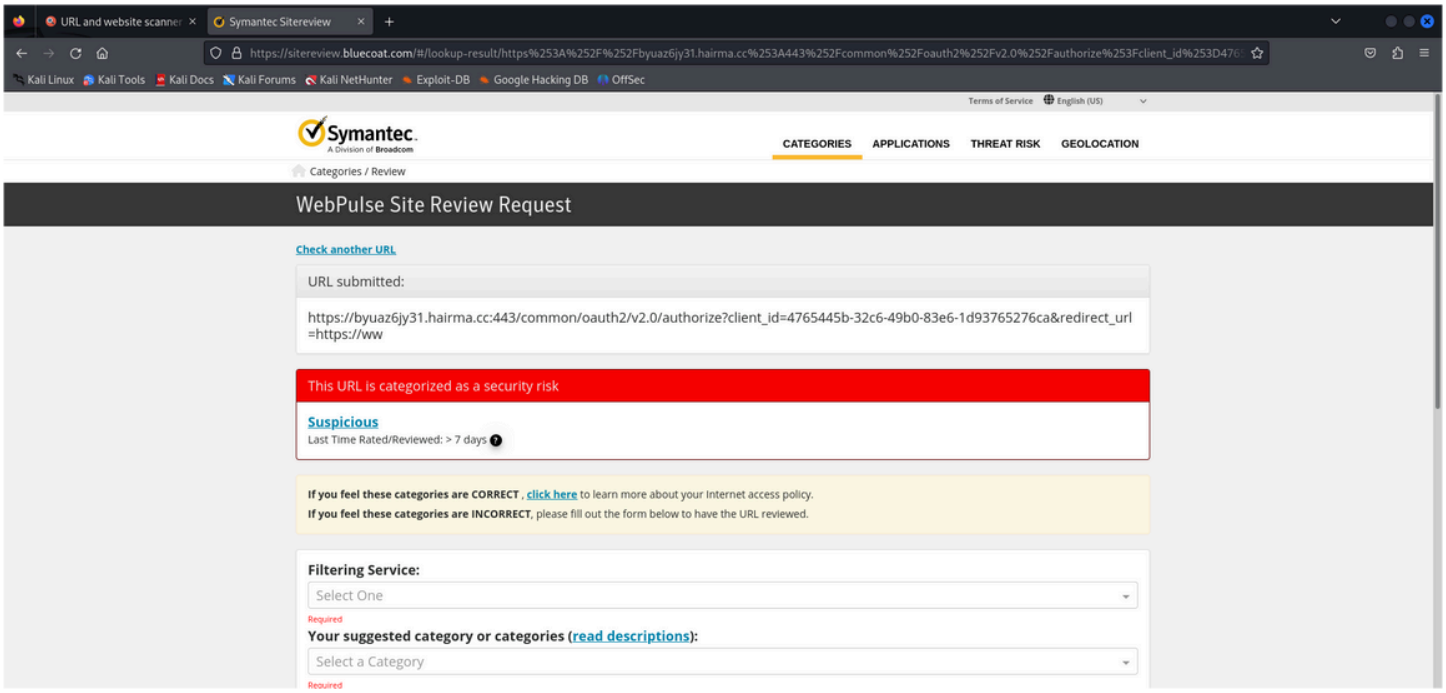


But , there is a twist look at the url , the domain in the url doesnt belongs to microsoft instead it looks different , this is an important ioc one should notice.

▢ Step 2) Analyze the Links (URLs)

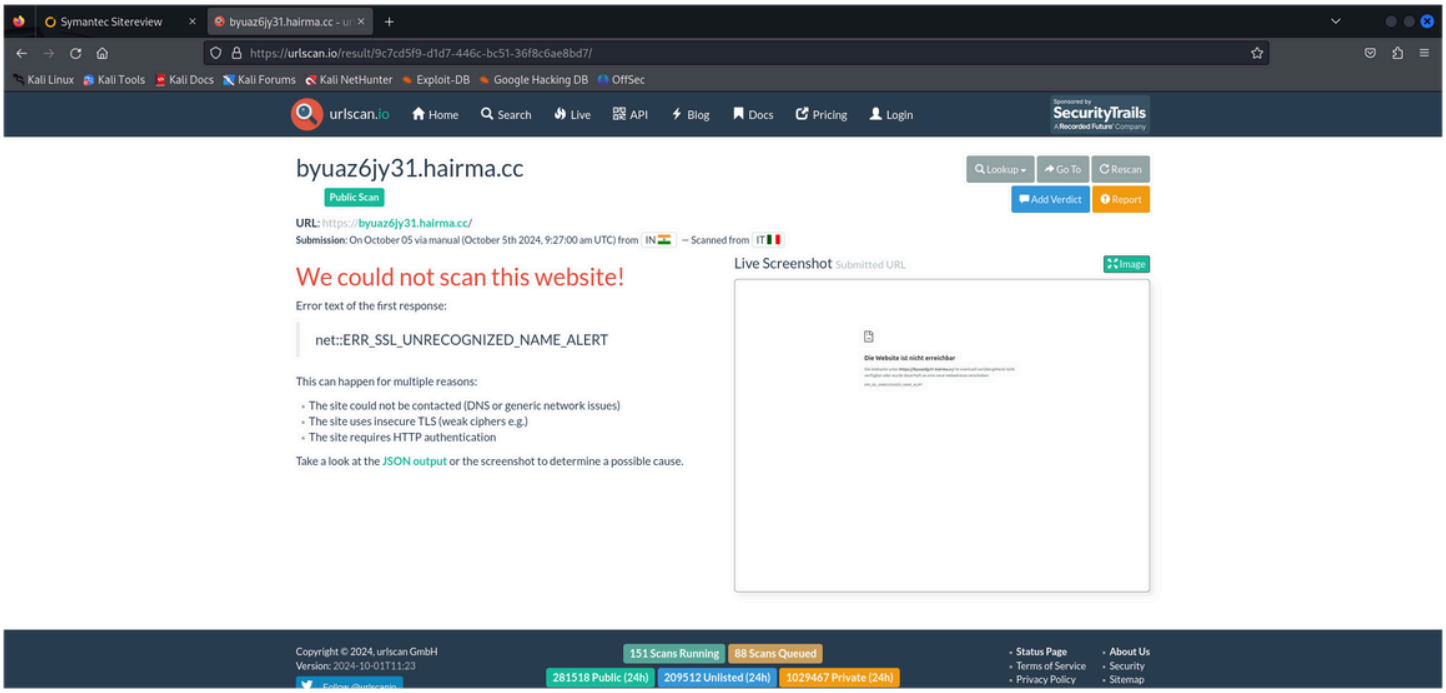
Phishing emails often include links that seem harmless but actually lead to fake websites. Here's how to check if a link is safe:

Symantec Site Review: This tool helps you check if a website is safe to visit.



you can clearly see the url is Suspicious therfore its not the real one. We can also search with other tools as well.

URLscan.io: This tool scans links to see if they are connected to any bad activities or phishing scams.



The above result states that the url is no longer available & it has been taken down because it has been categorized as phishing.

▢ Step 3) Analyze the Email Header

The email header contains important details about where the email came from. Here's how to check if an email is phishing:

Export the Email as an EML File: To examine the email properly, you need to download it in **EML format**. Here's how to do it:

Gmail: Open the email → Click on the "More" button (three dots) → Select "Download message" (it will save as a .eml file).

Outlook: Open the email → Click "File" → Select "Save As" → Choose the .eml format.

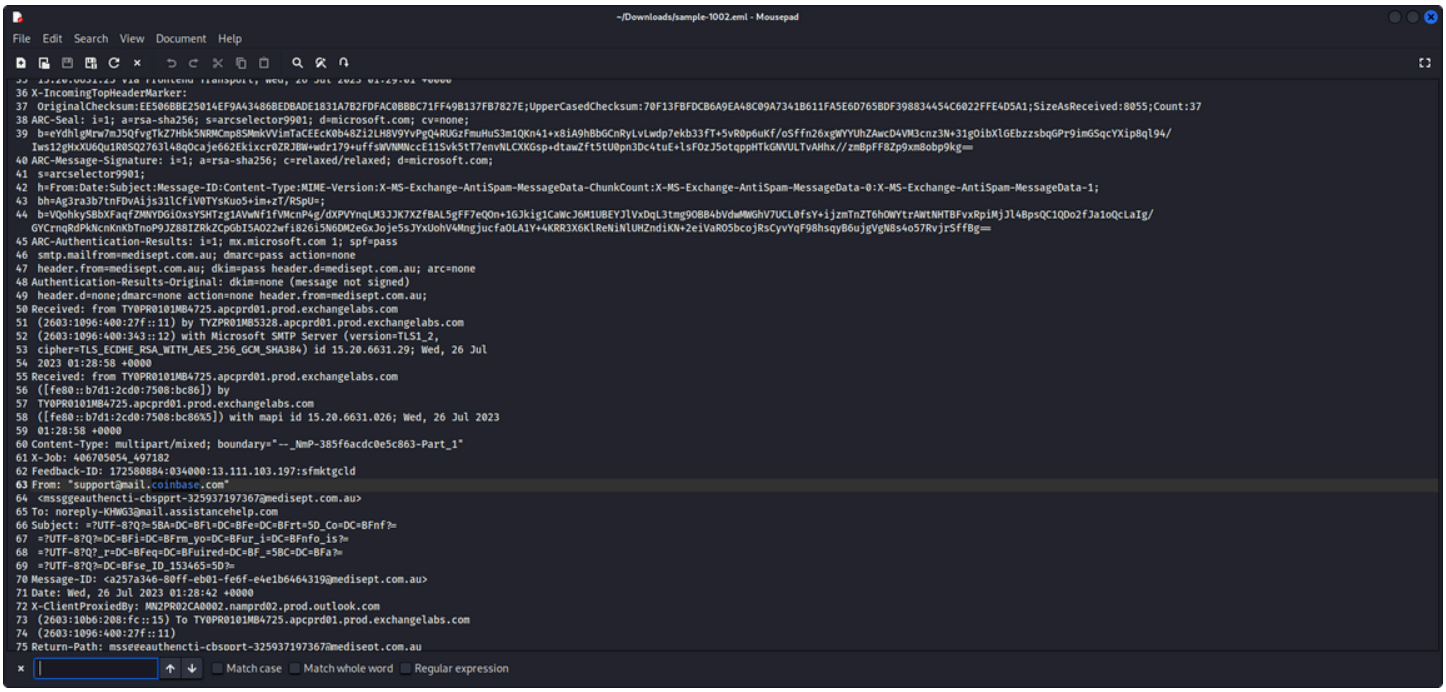
The .eml format looks like :

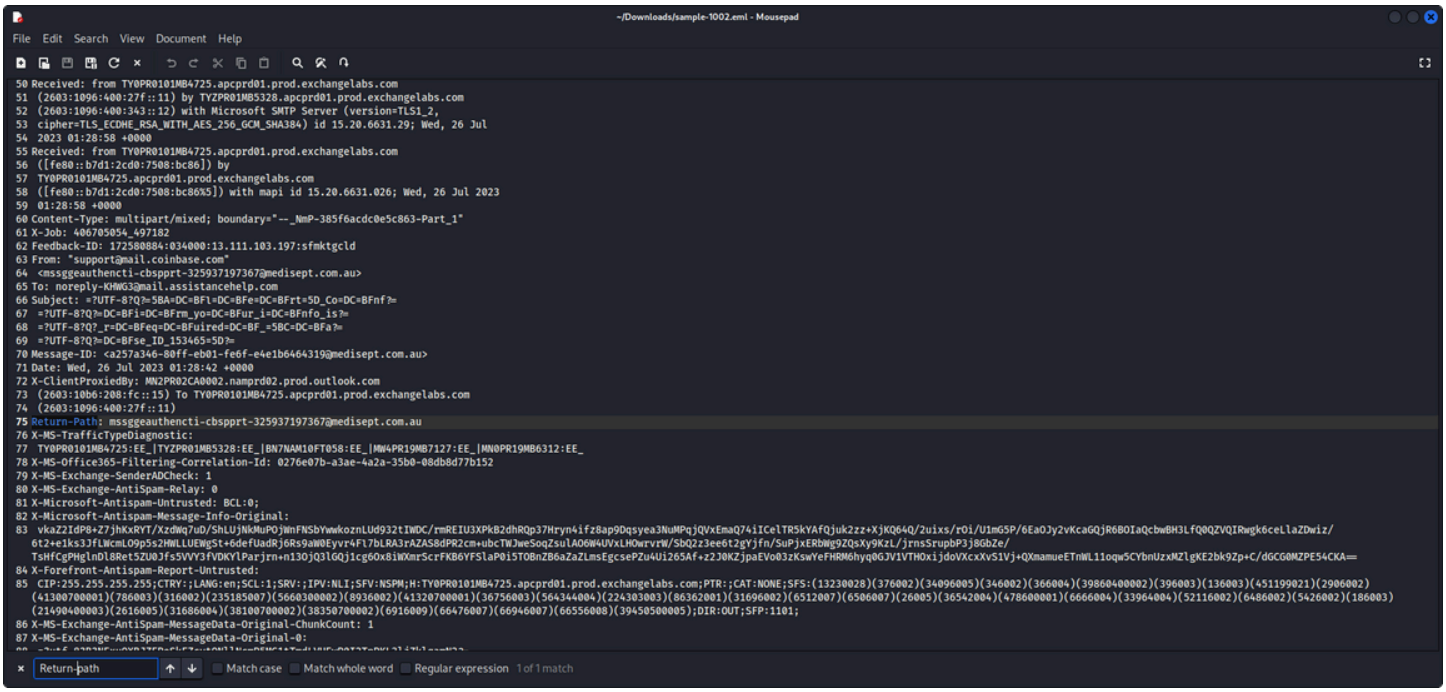
```
Received: from BN8NAM11FT066.eop-nam11.prod.protection.outlook.com
 (2603:10b6:408:e6:cafe::23) by BN0PR03CA0023.outlook.office365.com
 (2603:10b6:408:e6::28) with Microsoft SMTP Server (version=TLS1_2,
 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.28 via Frontend
 Transport; Tue, 19 Sep 2023 18:36:45 +0000
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=atendimento.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)
Received: from ubuntu-s-1vcpu-1gb-35gb-intel-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
X-IncomingTopHeaderMarker:
 OriginalChecksum:3B61F64750F88C5569DF38A496B2374685F23D8BC662A6A19B6823B2F6745D54;UpperCasedChecksum:62071BC7A7CF5B0844A7B406B0E9EFCDAA2CB94988E687CF8C56555AD4B52D30;SizeAsReceived:544;Count:9
Received: by ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (Postfix, from userid 0)
        id 39DEA3F725; Tue, 19 Sep 2023 18:35:49 +0000 (UTC)
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: phishing@pot
Message-Id: <20230919183549.39DEA3F725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06>
Date: Tue, 19 Sep 2023 18:35:49 +0000 (UTC)
X-IncomingHeaderCount: 9
Return-Path: root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06
X-MS-Exchange-Organization-ExpirationStartTime: 19 Sep 2023 18:36:44.2236
 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
```

- [ ] **Check the SPF Status:** Look at the email's SPF status. If it says “Fail” or “None,” it might be a phishing email.

- [ ] **Compare "From" and "Return-Path":**

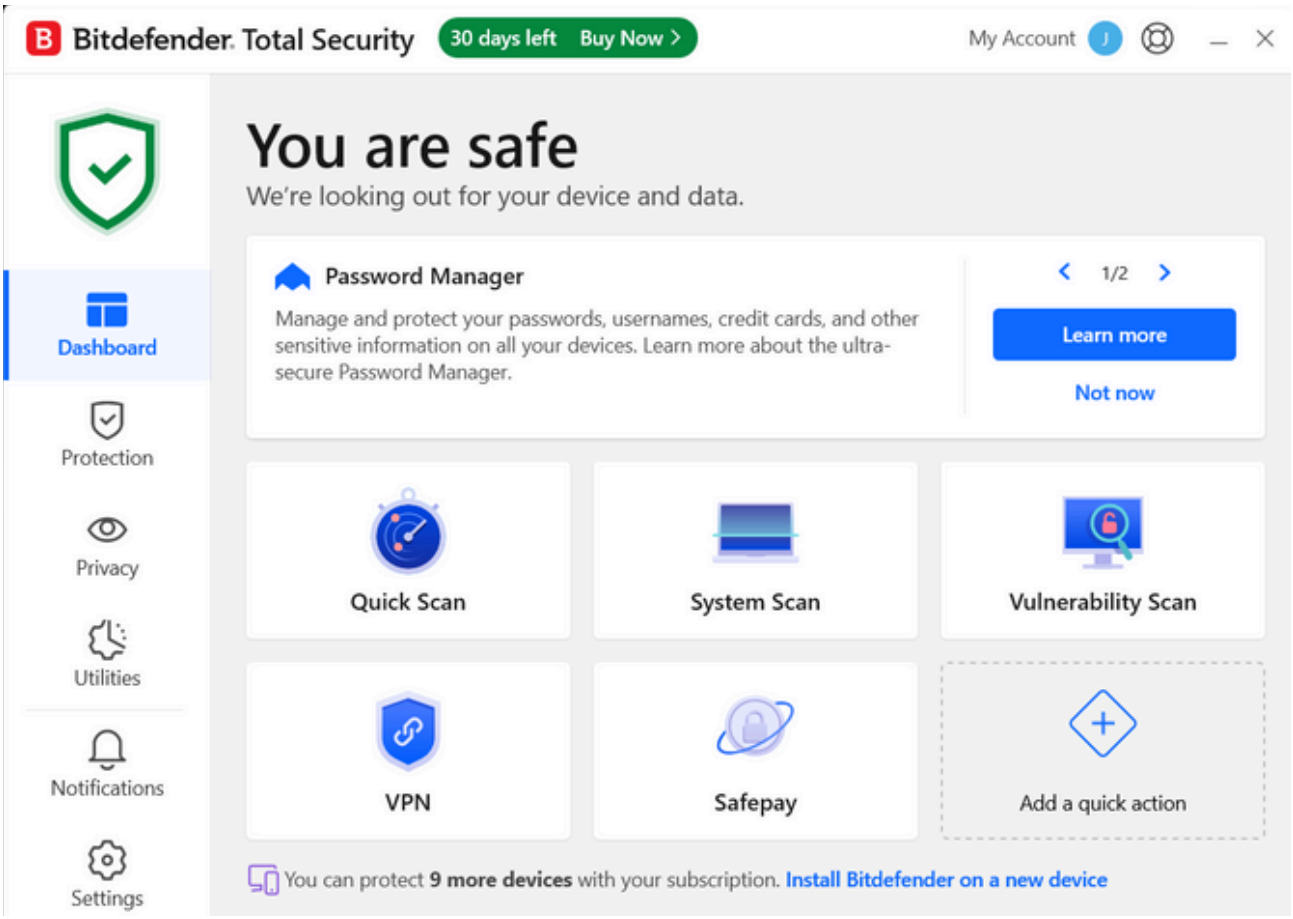
Look at the email sender (the "From" address). Then, check the "Return-Path" to see if it’s the same. If it’s different or strange, it could be phishing.





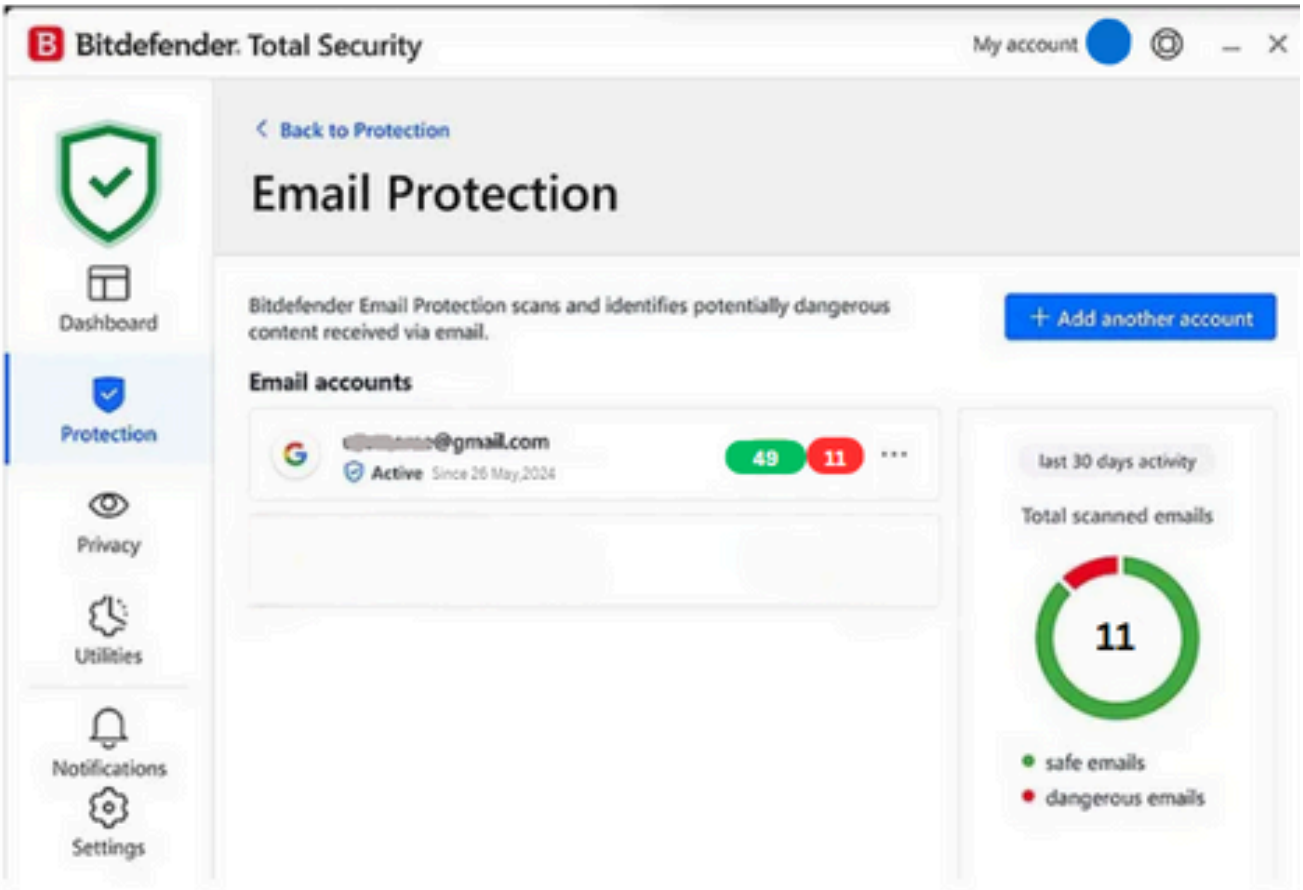
you can see the return path and from differs here , hence it doesnt really goes back to the address mentioned in the from field (the address might be spoofed) ,instead it goes to the address actually in the return path field .

▢ Step 4) Using an Email Filtering Tool: Bitdefender :

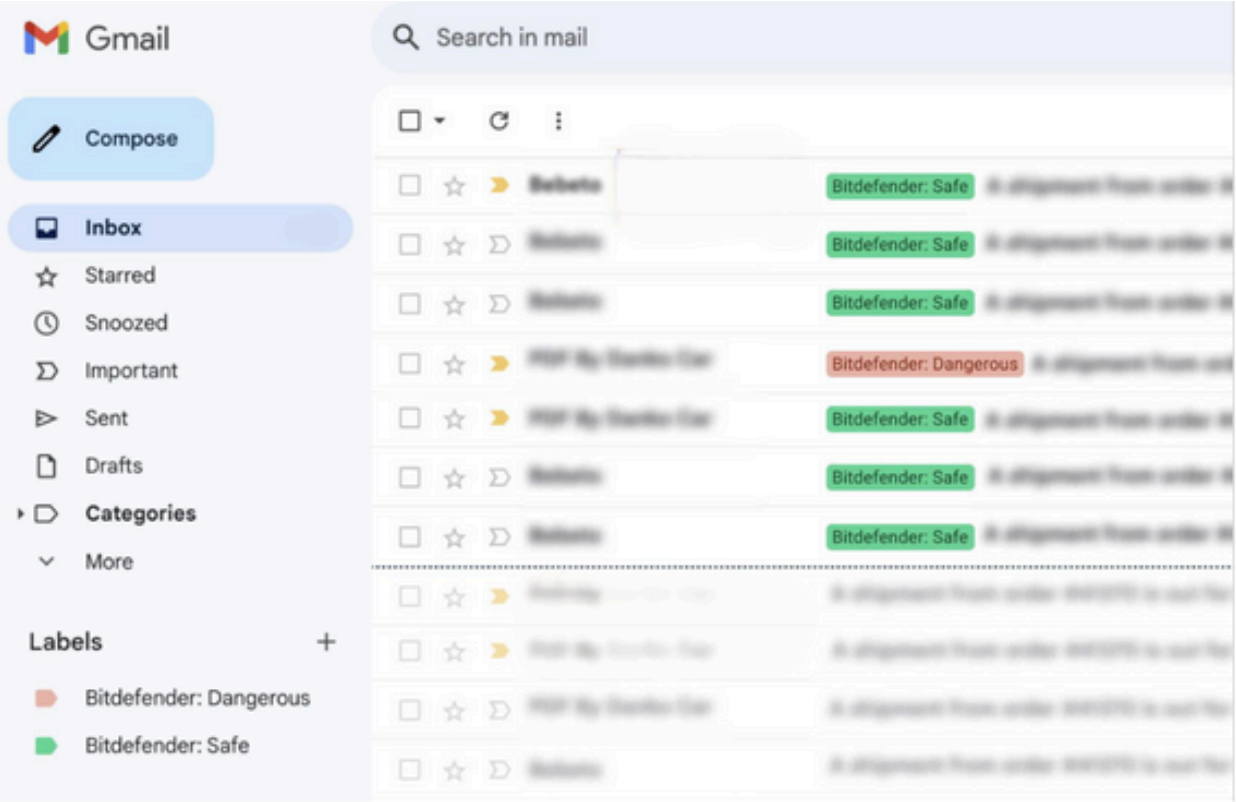


Bitdefender is a tool that helps protect you from phishing emails. Here's how it works:

- **Bitdefender Email Protection:** Go to the Protection tab in Bitdefender, then Email Protection and add your Gmail account, Bitdefender will start scanning the emails.



If a phishing email comes, Bitdefender will show a red alert, indicating the threat. The green shield indicates that your system is secure.



After configuring bitdefender gmail looks like the above indicating the security status of the email so it will be very easy even for a normal people.

▢ Conclusion:

This project showed how to analyze phishing emails by checking attachments, links, and email headers. Tools like **Symantec Site Review**, **URLscan.io**, and **Bitdefender** help protect against phishing attacks. By using these methods, you can stay safe and avoid falling for phishing scams.