Email Header Analysis for Phishing Attack

There are some factors that we should look out for while checking out if an email is a phishing email or not these factors include:

- The sense of urgency the Email portrays
- The email not been addressed to the receiver directly (your name not been mentioned but instead they addressed you as “user”)
- Generic reference to an undefined system (The exact reason for the notification will not be stated, instead the will just give a generic description)
- Statement of threat, for example: if you don’t click on the link your account will be blocked
- At the end of any phishing email there are always phishing links attached to the emails which can also be hidden under a button.

Phishing emails can also be known through email headers.

The highlighted spot on the email header above is the date the email is sent, and Gmail format is usually day, month, year, hour, minutes, and seconds. It’s good to also look out for these, if there is any mistake in arrangement the email might be a phishing attack.

The highlighted spot on the email header above is the destination the email was sent from. it is important to check if this email is same with the return path email, if there is any difference the email might be a phishing attack.

```
rLfXqkUhSQUUcVFOTOKjJ6DdbcAraH2TvhD+MrcnVpCG6HVBmwPCJ3qUIwtp1xABku1STRC6SzUIS
YRVweSmmXmfSz1qk84i0PjWsHXTzp91UVRXw==
Received: from dap-notification-email-gateway-7dd7b579f8-622dv (172.24.32.73) by NG-OJT-EX-RE002.mtn.com.ng
(172.30.152.149) with Microsoft SMTP Server id 15.2.1748.10; Wed, 14 May 2025 14:54:09 +0100
Date: Wed, 14 May 2025 13:54:09 +0000
From: <donotrespond@mtn.com>
To: <Imafidonjoseph9@gmail.com>
Message-ID: <700582836.94093.1747230849927@dap-notification-email-gateway-7dd7b579f8-622dv>
Subject: Your Product Purchase Payment Link
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_Part_94092_1702220154.1747230849927"
Return-Path: donotrespond@mtn.com
Received-SPF: PermError (NG-OJT-EX-RE002.mtn.com.ng: domain of donotrespond@mtn.com used an invalid SPF
mechanism)
```

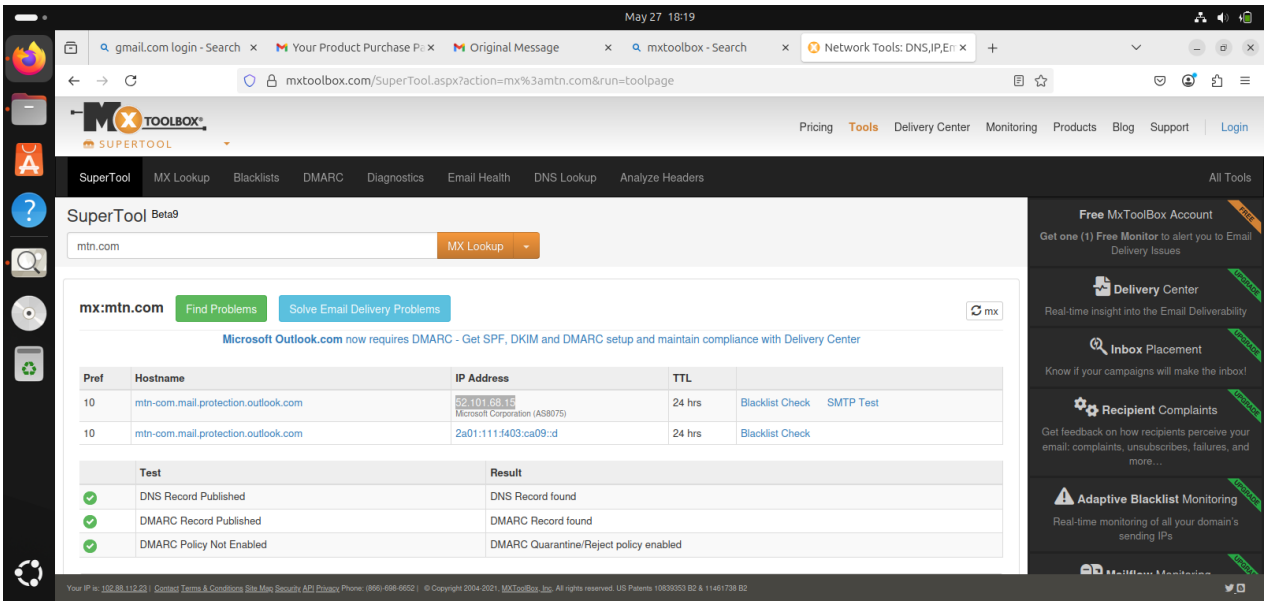
The highlighted spot on the email header above is the return path email, which means any response back to the email will be sent back to the mail in particular so it is important to compare this email with the email it was sent from, if there is any change the email might be a phishing attack.

```
rLfXqkUhSQUUcVFOTOKjJ6DdbcAraH2TvhD+MrcnVpCG6HVBmwPCJ3qUIwtp1xABku1STRC6SzUIS
YRVweSmmXmfSz1qk84i0PjWsHXTzp91UVRXw==
Received: from dap-notification-email-gateway-7dd7b579f8-622dv (172.24.32.73) by NG-OJT-EX-RE002.mtn.com.ng
(172.30.152.149) with Microsoft SMTP Server id 15.2.1748.10; Wed, 14 May 2025 14:54:09 +0100
Date: Wed, 14 May 2025 13:54:09 +0000
From: <donotrespond@mtn.com>
To: <Imafidonjoseph9@gmail.com>
Message-ID: <700582836.94093.1747230849927@dap-notification-email-gateway-7dd7b579f8-622dv>
Subject: Your Product Purchase Payment Link
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_Part_94092_1702220154.1747230849927"
Return-Path: donotrespond@mtn.com
Received-SPF: PermError (NG-OJT-EX-RE002.mtn.com.ng: domain of donotrespond@mtn.com used an invalid SPF
mechanism)
```

The highlighted spot on the email header above is the message ID and this is what identify this email in particular so two emails sent must not have same ID, if two emails have same ID it might be a phishing attack.

```
wMSsWMZmKz8t+QjKvHdc8N+6Y4lWd2LUPqOTvbXKNRg1nQUXW4u6adFzwWCIqDPM1VZaek7GQNQwh
rLfXqkUhSQUUcVFOTOKjJ6DdbcAraH2TvhD+MrcnVpCG6HVBmwPCJ3qUIwtp1xABku1STRC6SzUIS
YRVweSmmXmfSz1qk84i0PjWsHXTzp91UVRXw==
Received: from dap-notification-email-gateway-7dd7b579f8-622dv (172.24.32.73) by NG-OJT-EX-RE002.mtn.com.ng
(172.30.152.149) with Microsoft SMTP Server id 15.2.1748.10; Wed, 14 May 2025 14:54:09 +0100
Date: Wed, 14 May 2025 13:54:09 +0000
From: <donotrespond@mtn.com>
To: <Imafidonjoseph9@gmail.com>
Message-ID: <700582836.94093.1747230849927@dap-notification-email-gateway-7dd7b579f8-622dv>
Subject: Your Product Purchase Payment Link
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="----=_Part_94092_1702220154.1747230849927"
Return-Path: donotrespond@mtn.com
Received-SPF: PermError (NG-OJT-EX-RE002.mtn.com.ng: domain of donotrespond@mtn.com used an invalid SPF
mechanism)
```

The highlighted spot on the email header above is the domain of the sender, this domain can be taken to a website like MxToolbox.com to analyze If the email is spoofed, this can also determine if he email is a phishing attack or not.



The image above is a Practical example of a domain been Analyze on the MxToolbox.com website, the highlighted spot is the domain IP address, it is also important to check if the domain IP address match that on the email header, if it doesn't match it might be that it's a phishing attack, but this is not always a qualification for an email to be a phishing attack.

	Test	Result
✓	DNS Record Published	DNS Record found
✓	DMARC Record Published	DMARC Record found
✓	DMARC Policy Not Enabled	DMARC Quarantine/Reject policy enabled

This signify the protocol the domain is using. this should also be looked out for while analyzing if an email is a phishing attack.