

# Phishing/Spam Email Analysis

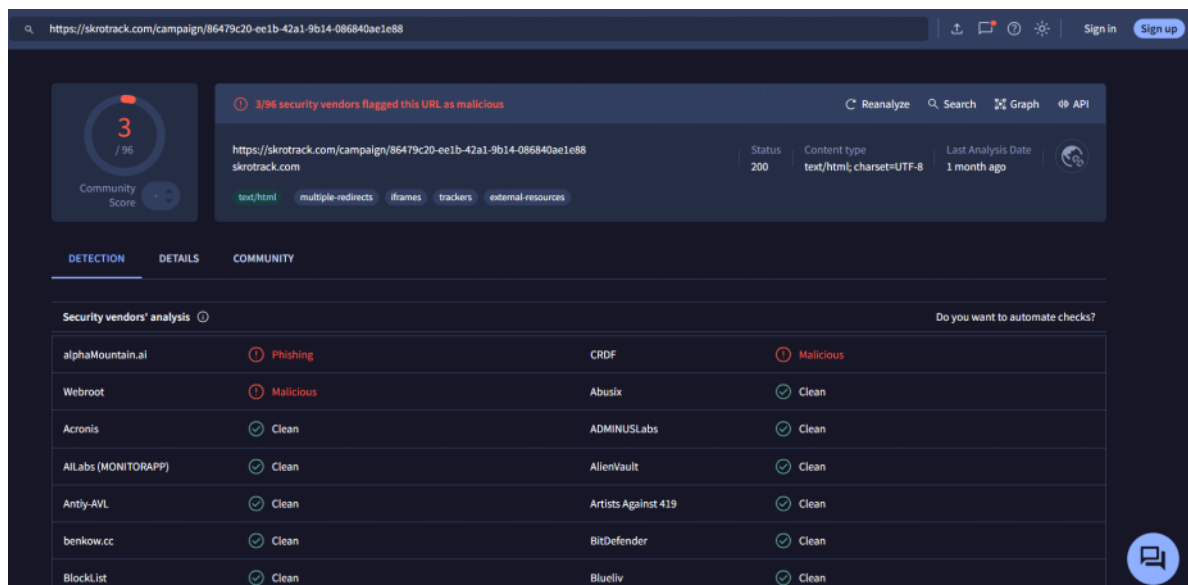
December 25, 2024 1:23 AM

## Using FREE web applications to analyze phishing emails.

- Open the email and check subject, sender information and email content.
- Questions to ask yourself:
  - Was I waiting for this email?
  - Is this email from who I was expecting it to be?
  - Is there any suspicious attachments or links that will redirect me?
    - If so: spot the link and copy it by right clicking on the link and selecting "Copy link".



- Open <https://www.virustotal.com/> and paste the link/url previously copied.
  - **VirusTotal** is an online service that analyzes files and URLs for viruses, malware, and other security threats by scanning them with multiple antivirus engines. It provides a detailed report on potential risks and safety of the submitted items.
  - You can also upload documents so it can be scanned for malware.
- Note: 3 engines spotted it as malicious or phishing.



Security vendors' analysis	Result
alphaMountain.ai	Phishing
Webroot	Malicious
Acronis	Clean
AL Labs (MONITORAPP)	Clean
Antiy-AVL	Clean
benkow.cc	Clean
Blocklist	Clean
CRDF	Malicious
Abusix	Clean
ADMINUS Labs	Clean
AlienVault	Clean
Artists Against 419	Clean
BitDefender	Clean
Blueliv	Clean

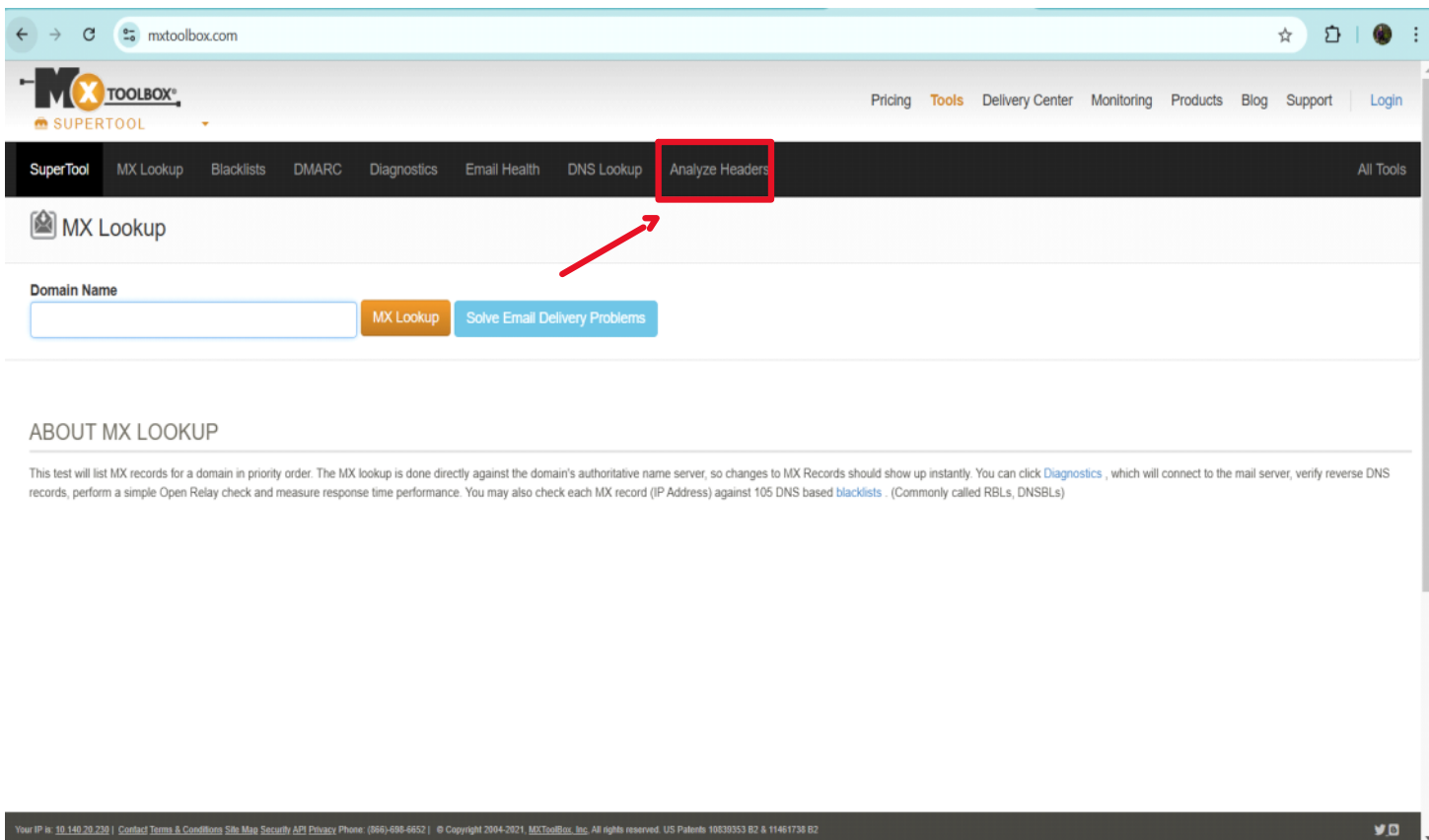
**For a more thorough analysis of the link** you can use tools like [www.joesandbox.com](https://www.joesandbox.com/), virtual machines or Sandbox applications(Windows Sandbox...), so you can access the link and further investigate.

- Make sure it is done in a controlled and contained environment. Consulting a Specialist is recommended.

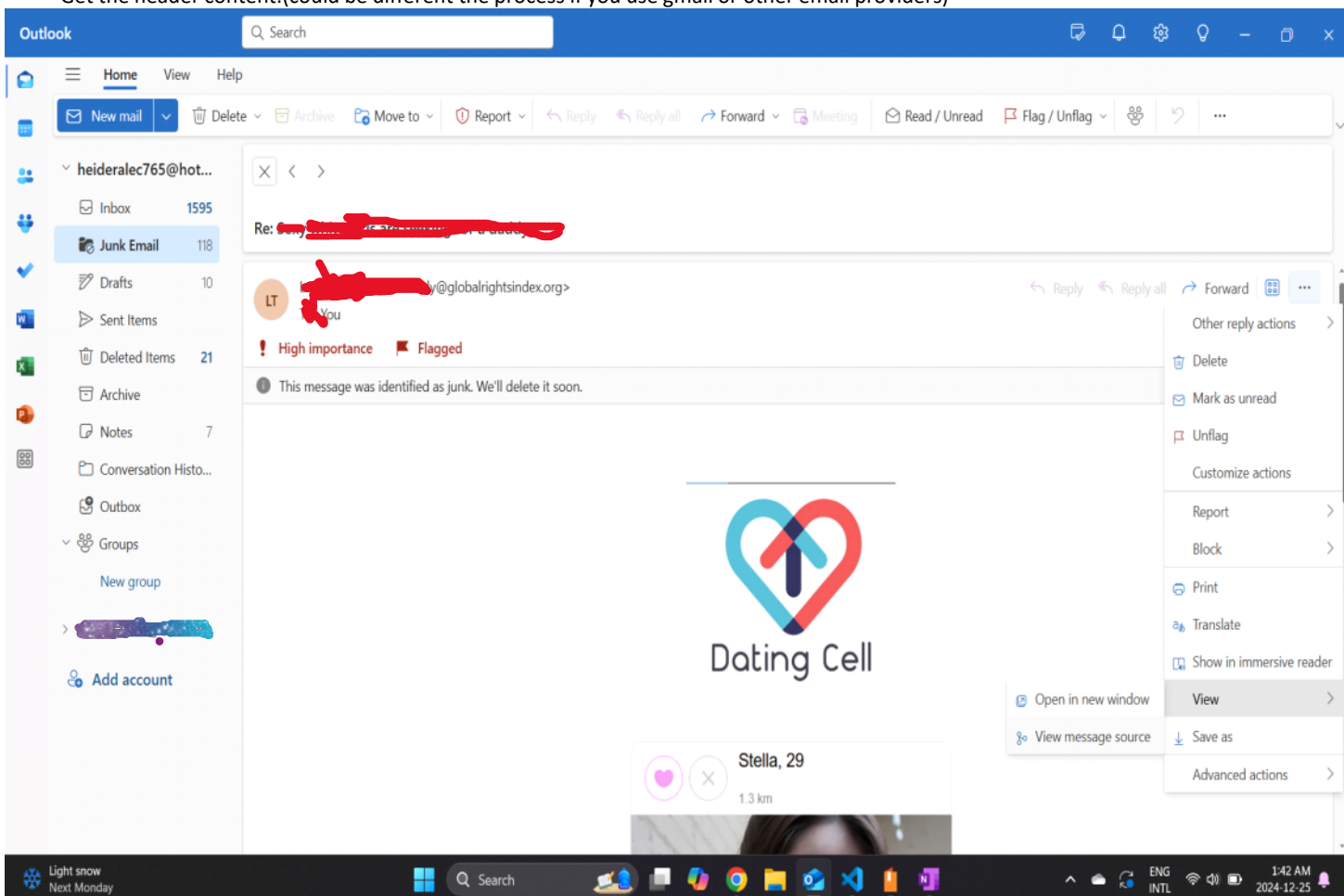
## Get information and investigate:

- MXToolBox
  - Provides various tools which can be used for email investigation.
- Goals:

- Verify the legitimacy of the email,
- Check if email is configured with the security mechanisms(SPF,DKIM and DMARC)
- Get more information from the email header.



- Get the header content.(could be different the process if you use gmail or other email providers)



- Copy the header and paste it to the website .

**Email Header Analyzer**

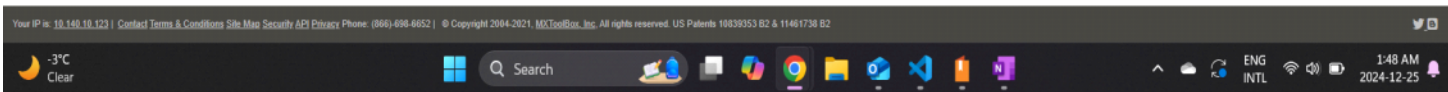
Paste Header:

```
CH3PR22MB4907.namprd22.prod.outlook.com with HTTPS; Fri, 22 Nov 2024 22:53:22 +0000
Received: from DUZPR01CA0057.eurprd01.prod.exchangelabs.com
(2603:10a6:10:469::6) by LV8PR22MB5314.namprd22.prod.outlook.com
(2603:10b6:408:1ce::6) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8158.27; Fri, 22 Nov
2024 22:53:15 +0000
Received: from DB5PEPF00014B8B.eurprd02.prod.outlook.com
(2603:10a6:10:469:cafe::bf) by DUZPR01CA0057.outlook.office365.com
(2603:10a6:10:469::6) with Microsoft SMTP Server (version=TLS1_2,
cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.8182.17 via Frontend
```

Analyze Header

## ABOUT EMAIL HEADERS

This tool will make email headers human readable by parsing them according to RFC 822. Email headers are present on every email you receive via the Internet and can provide valuable diagnostic information like hop delays, anti-spam results and more. If you need help getting copies of your email headers, [just read this tutorial](#).



- To be **DMARC compliant**, an email must pass both of the following checks:
  1. **SPF (Sender Policy Framework) Check:**
    - SPF is a system that checks if the email is coming from a server authorized to send emails on behalf of the domain in the "From" address.
  2. **DKIM (DomainKeys Identified Mail) Check:**
    - DKIM ensures that the email's content has not been altered in transit and that it was sent by a legitimate sender authorized to use the domain's private key.
- This email is not DMARC Compliant, which could indicate suspicious activity.
- Right below you can see the path/servers the email passed by to get to me and the time taken.

**Header Analyzed**

Email Subject: Re: [redacted]

Copy/Paste Warning  
Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our [Email Deliverability tool](#)

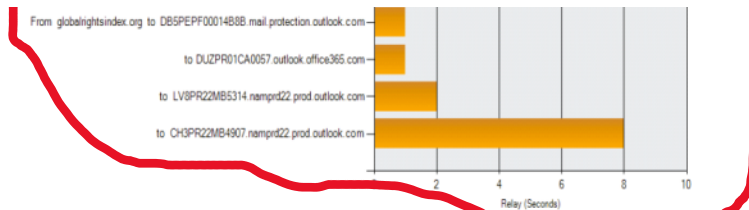
**Delivery Information**

- ✖ DMARC Compliant (No DMARC Record Found)
  - ✔ SPF Alignment
  - ✔ SPF Authenticated
  - ✖ DKIM Alignment
  - ✖ DKIM Authenticated

**Relay Information**

Received	8 seconds
Delay:	

From: globalsignindex.org to: DB5PEPF00014B8B.mail.protection.outlook.com  
to: DUZPR01CA0057.outlook.office365.com  
to: LV8PR22MB5314.namprd22.prod.outlook.com



- This table shows with more details regarding the path/hops taken by the email.
  - Notice that one of the domains involved on hop '1' and '4' where found on blacklist databases.

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	globalrightsindex.org 23.239.4.87	DB5PEPF00014B8B.mail.protection.outlook.com 10.167.8.199	Microsoft SMTP Server	11/22/2024 10:53:14 PM	✗
2	0 seconds	DB5PEPF00014B8B.eurprd02.prod.outlook.com 2603:10a6:10:469:cafe::bf	DUZPR01CA0057.outlook.office365.com 2603:10a6:10:469::6	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	11/22/2024 10:53:14 PM	✓
3	1 Second	DUZPR01CA0057.eurprd01.prod.exchangelabs.com 2603:10a6:10:469::6	LV8PR22MB5314.namprd22.prod.outlook.com 2603:10b6:408:1ce::6	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	11/22/2024 10:53:15 PM	✓
4	7 seconds	LV8PR22MB5314.namprd22.prod.outlook.com ::1	CH3PR22MB4907.namprd22.prod.outlook.com	HTTPS	11/22/2024 10:53:22 PM	✗

- Here are the contents found on the header, this is easier to view.(

## Headers Found

Header Name	Header Value
Authentication-Results	spf=pass (sender IP is 23.239.4.87) smtp.mailfrom=globalrightsindex.org; dkim=none (message not signed) header.d=none; dmarc=bestguesspass action=none header.from=globalrightsindex.org; compauth=pass reason=109
Received-SPF	Pass (protection.outlook.com: domain of globalrightsindex.org designates 23.239.4.87 as permitted sender) receiver=protection.outlook.com; client-ip=23.239.4.87; helo=globalrightsindex.org; pr=M
X-IncomingTopHeaderMarker	OriginalChecksum: AC7979BA326FB801C78690CFD26FDC75BBE134A78AF50266769299016DA418B0; UpperCasedChecksum: F0A1CA2A824821B0C8D0C72D784AA2BBD8AA67FCF3D77CEE726EAE01BE164F; SizeAsReceived: 461; Count: 12
From	Lets [REDACTED] today <Noreply@globalrightsindex.org>
Subject	Re: [REDACTED]
To	heidalec765@hotmail.com
Content-Transfer-Encoding	7bit
Content-Type	text/html; charset=UTF-8
Date	Fri, 22 Nov 2024 23:52:53 +0100
Message-Id	<nLsjTBJG-1zKI-NJZY-x77C-4d67-b406-4RBdB970srFJM@c@BN1PEPF00005FFD.namprd05.prod.outlook.com>
x-Liar	email@11_323467>
X-IncomingHeaderCount	12
Return-Path	infobot@globalrightsindex.org
X-MS-Exchange-Organization-ExpirationStartTime	22 Nov 2024 22:53:14 8762 (UTC)
X-MS-Exchange-Organization-ExpirationStartTimeReason	OriginalSubmit
X-MS-Exchange-Organization-ExpirationInterval	1:00:00:00.0000000

- With the information found on the header I started my search.
  - Info acquired:

Info	Tools
System is up	ping tool
Sender is hosted or tunneling traffic through Linode/Akamai cloud services	Whois and tracert tools
Domain was registered through	Whois(Cisco Talos Intelligence)

<a href="https://www.ovhcloud.com/">https://www.ovhcloud.com/</a>	
IP addresses linked to the domain (check picture below).	Nslookup tool

```

PS C:\Users\Heider> nslookup globalrightsindex.org
Server:  node-1w7jr9n24twqzs2cg5ed4tjl3.ipv6.telus.net
Address:  2001:568:ff09:10c::67

Non-authoritative answer:
Name:     globalrightsindex.org
Addresses: 2606:4700:10::6816:355a
           2606:4700:10::6816:345a
           2606:4700:10::ac43:1dab
           104.22.53.90
           104.22.52.90
           172.67.29.171

```