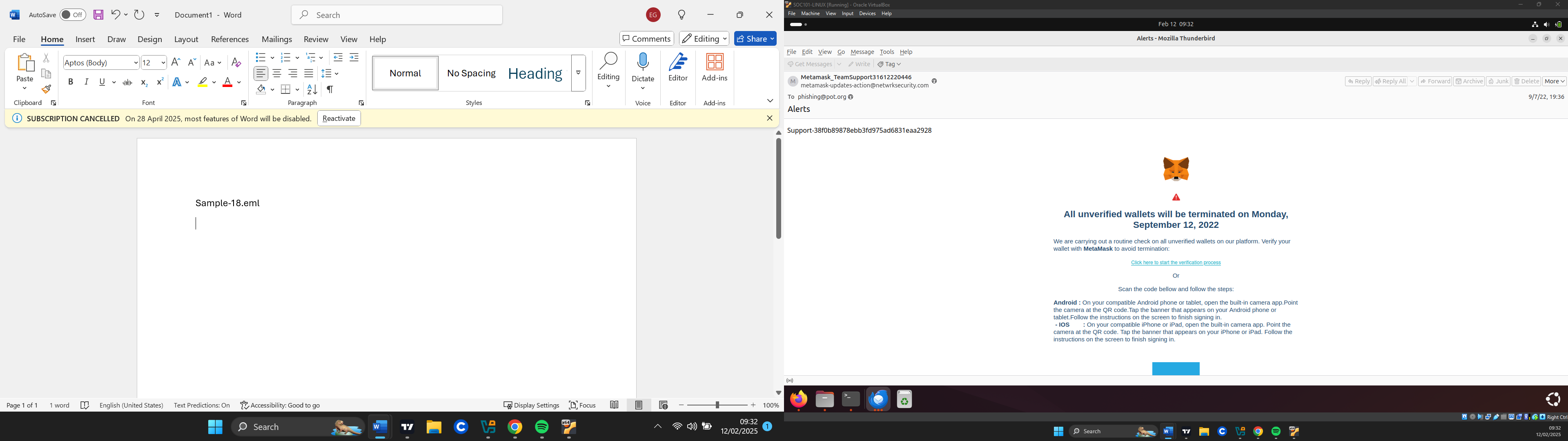
Sample-18.eml



HEADERS:

**Date/ Time**: Wed, 7 Sep 2022 / 21:36:59 +0200

**Subject**: Alerts

**To**: phishing@pot

**From**: metamask-updates-action@netwrksecurity.com

**Reply to**: -

|  |  |
| --- | --- |
|  |  |

**Return-Path**: metamask-updates-action@netwrksecurity.com

**Sender IP**: 94.231.103.45

**Resolved host**: websmtp-out1.simply.com

**Message – ID:** “<cYXojTcIMuRgMo3OaSdh1AdBl1vEakIefZlXkuw@netwrksecurity[.]com>”

URLS

With the help of the eioc.py script we extracted the following URL

-(“hxxps[://]420[.]bio/NtRIA”)

ATTACHMENTS

**-**

EMAIL DESCRIPTION

The email shows to be related to MetaMask, a crypto wallet. It appears to be from their support team warning that all unverified wallets will be terminated, due to a routine check on Monday, September 12, 2022 which is 5 days after the email was received.

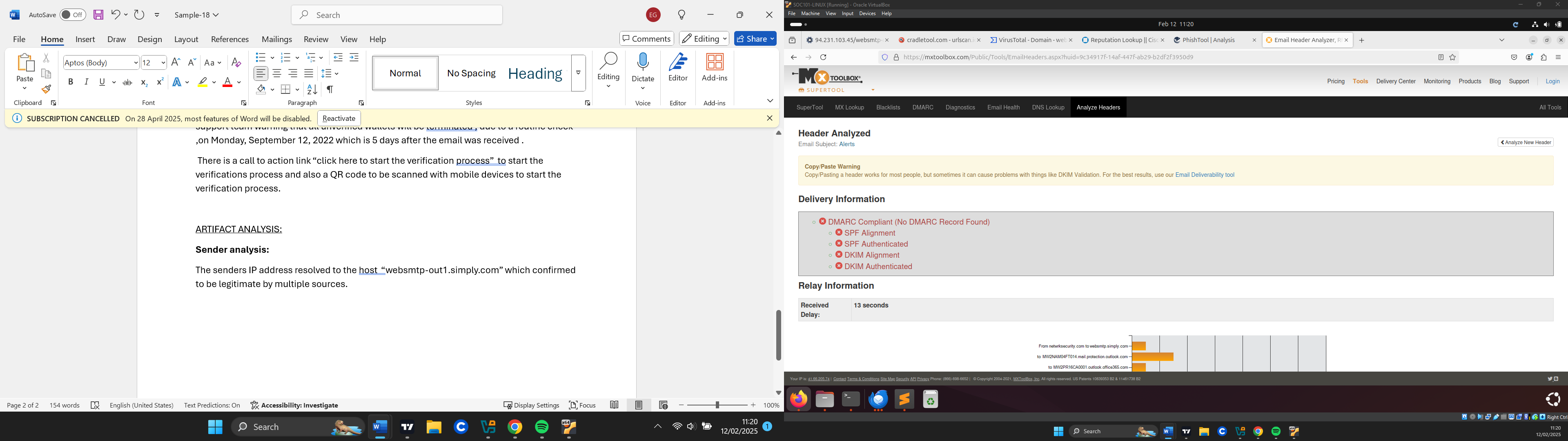
There is a call to action link “click here to start the verification process” to start the verifications process and also a QR code to be scanned with mobile devices to start the verification process.

ARTIFACT ANALYSIS:

**Sender analysis:**

The senders IP address resolved to the host “websmtp-out1.simply.com” which confirmed to be legitimate by multiple sources.

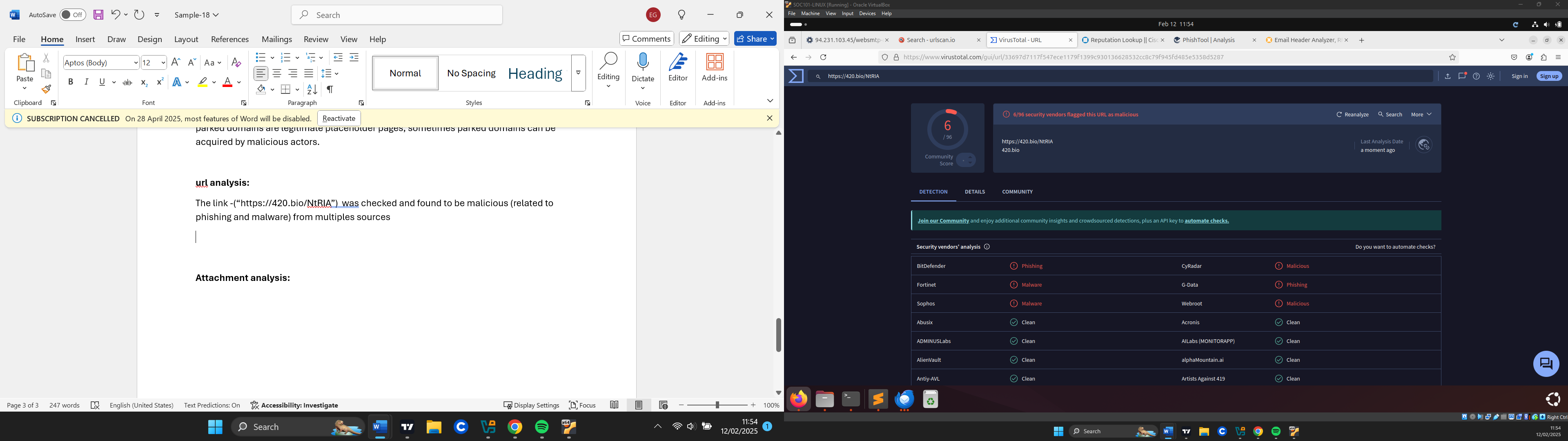
The email header, however, failed all email authentication methods signifying that the email is spoofed and suspicious.



Since it could be possibly spoofed, we checked the reputation of the sender domain “netwrksecurity.com” and could be an example of typo squatting since we expect “networksecurity”. The domain appears to be legitimate but a parked site. While most parked domains are legitimate placeholder pages, sometimes parked domains can be acquired by malicious actors.

**URL analysis:**

The link(“hxxps[://]420[.]bio/NtRIA”) was checked and found to be malicious (related to phishing and malware) by multiple vendors.



**Attachment analysis:**

**-**

VERDICT

Due to the email failing all authentication methods which is a strong indication of being spoofed and also the associated link being malicious, it is safe to say that this email is a phishing attempt and also quishing. (QRcode Phishing)

DEFENSE ACTIONS

I blocked the spoofed Ip address used to send the phishing email.

To ensure users never visit the malicious site, I have blocked the URL (“hxxps[://]420[.]bio/NtRIA”)