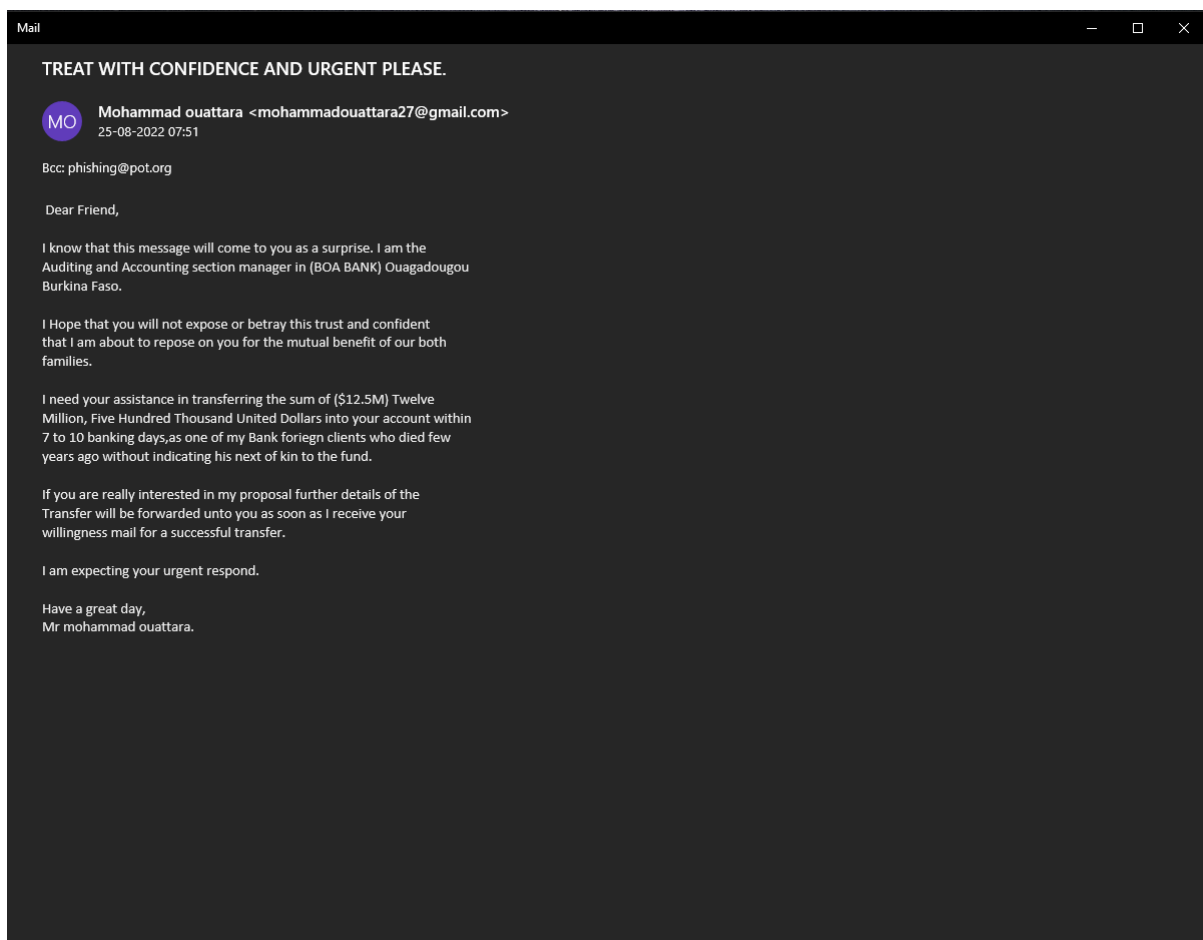


Name – Saimon Soren

Gmail – [saimonsoren200206@gmail.com](mailto:saimonsoren200206@gmail.com)

Task 2: **Identify phishing characteristics in a suspicious email sample.**

### Example of a phishing Mail –



For clarification, the sender of email is impersonating itself as an Auditing and Accounting section manager in (BOA) Bank of Africa Ouagadougou Burkina Faso and asking for a transfer of (\$12.5M) in the bank account.

So, first of all none of the banks sends such an email requesting for money transaction within a time period and no higher Authority would send an email personally to his customers.

No corporate sector sends email to his customers or employees with the heading (Dear Friend); mentioned in the screenshot above.

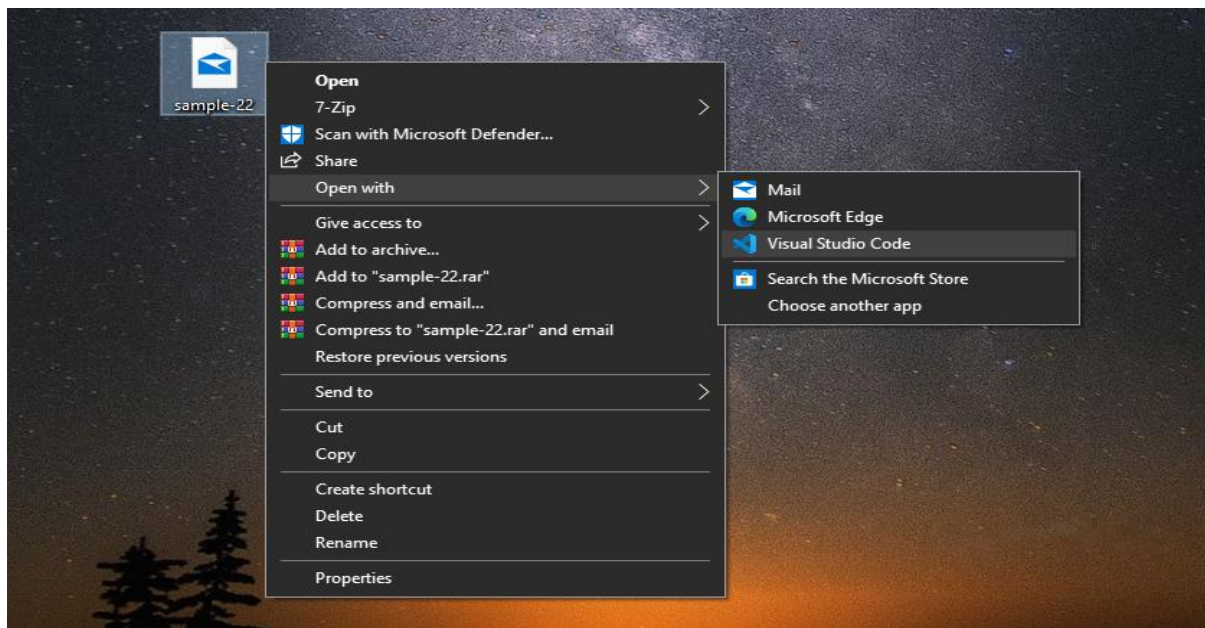
This email contains grammatical mistakes.

This email imposes psychological trait with the customer, which is totally unwanted in its behavior.

The email is proposing an emotional proposal with the victim to lure him/her into the phishing pot.

So, above are some of the characteristics based on the writing structure of the email.

Let's dive in to the technical part of the email –



To check the email header, we will copy the raw source for the email.

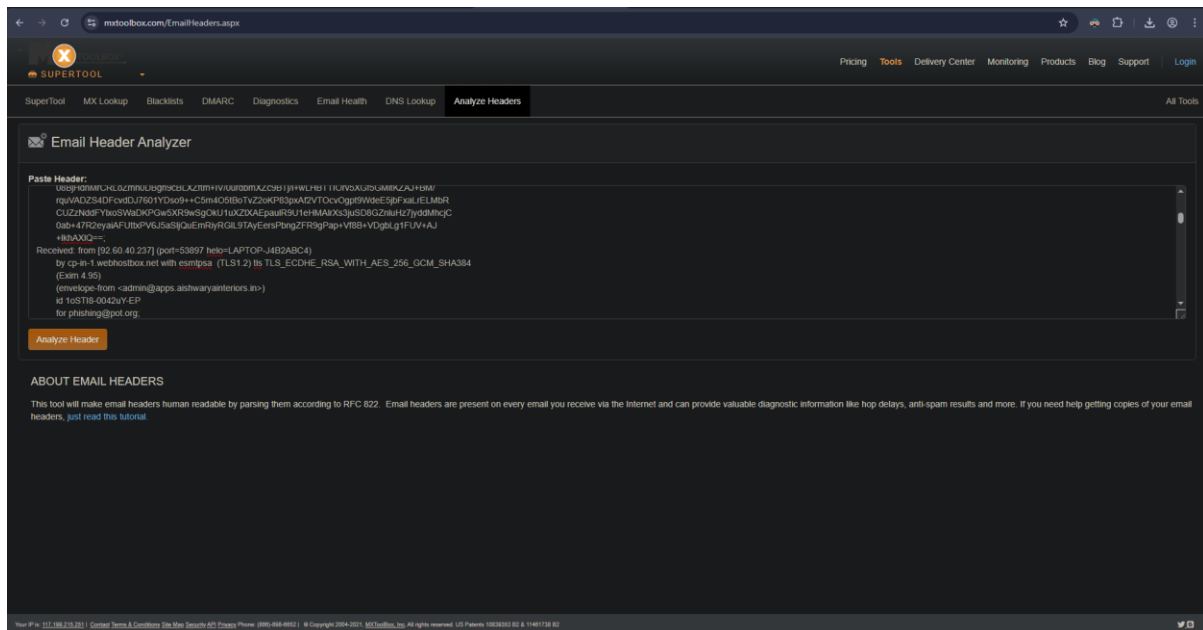
Below is the screenshot of the source-

```
C:\Users\Sandbox\Desktop > E:\sample-22.html
14 Authentication-Results: spr=none (sender IP is 192.185.51.139)
15 smtp.mailfrom=apps.aishwaryainteriors.in; dkim=pass (signature was verified)
16 header.d=apps.aishwaryainteriors.in;marc=faill action=reject
17 header.from=exodus.com;compauth=faill reason=000
18 Received-SPF: None (protection.outlook.com: apps.aishwaryainteriors.in does
19 not designate permitted sender hosts)
20 Received: from gateway24.webstewelcome.com (192.185.51.139) by
21 DB3EUR04F1012.mail.protection.outlook.com (10.152.25.209) with Microsoft SMTP
22 Server Id 15.20.5566.15 via Frontend Transport; Mon, 29 Aug 2022 01:10:19
23 +0000
24 X-IncomingTopHeaderMarker:
25 OriginalHostedCom-B55B931CE45B490B1577ACD4C47CEFB0C39E01A68EC47F6657F6318277ADCAEB;UpperCasedChecksum:A660266E3082971D1BF6A6B88DF2E850B24B43EF196E9E5CBA5F787E28327B3;SizeAsReceived:2611;Count:32
26 Received: from cm10.webstewelcome.com (cm10.webstewelcome.com [100.42.40.4])
27 by gateway24.webstewelcome.com (Postfix) with ESMTP Id 4881914680
28 for cphishing@pot.org; Sun, 28 Aug 2022 20:10:19 -0500 (CDT)
29 Received: from cp-in-1.webstewelcome.net ([183.21.58.10])
30 by csmtp with SMTP
31 Id ST10Q4z9wFESTao54Bx; Sun, 28 Aug 2022 20:10:19 -0500
32 X-Authority-Reason: ss-1
33 DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
34 d=apps.aishwaryainteriors.in; s=default; h=Content-Type:MIME-Version:Sender:
35 To:Message-Id:Subject:Date:From:Reply-To:Cc:Content-Transfer-Encoding:
36 Content-ID:Content-Description:Resent-Date:Resent-From:Resent-Sender:
37 Resent-To:Resent-Cc:Resent-Message-ID:In-Reply-To:References:List-Id:
38 List-Help:List-Unsubscribe:List-Subscribe:List-Post:List-Owner:List-Archive;
39 bh=QXus/oz764uQqIgt1u1uAUCjFPx1a/9xMBaOLs; b=JKczagKRM0Ccx3r+AOOLqPH
40 08Bj9dH9CRLozh0dgh0cBLKZftm+IV/burdh0Zc9BTj/1wLHBT10r+VXGFS6H1tKZA3+BN/
41 rquANDZ54DFcvdD7601YDso9+CSm4D51Bo1VZ20K83paf2Vt0Cv0pT9Mde5JbfXaLrELM6R
42 CUZ2nd6PVLx0s0m0P0wS0h0w0g0u0Z0X40paul0R010W010X30j0s0002u0u0z0jy00w0c0c
43 0ab+4782eyalAFUtt0V035a51j0u0mly0Ll0Tay0ers0bng2fR0g0apv0F0B+V0gh0g1f0v0A3
44 +lkHAKlQ==;
45 Received: from [92.68.40.237] (port=53897 helo=LAPTOP-34B2ABC4)
46 by cp-in-1.webstewelcome.net with esmtpsa (TLS1.2) tls TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
47 (Exim 4.95)
48 (envelope-from <cadefn@apps.aishwaryainteriors.in>)
49 id 1oST1B-0042Uv-EP
50 for phishing@pot.org;
```

The above screenshot will help us to recognize the email authenticity.

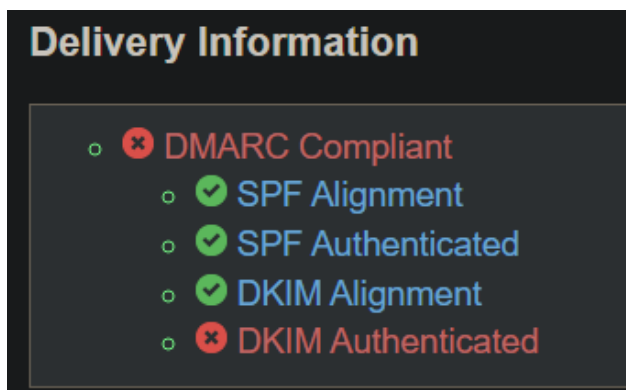
To check the email header for discrepancies I will use the mxtoolbox header checkup tool.

Copy and paste the email header to the tool for lookup:



Below are the results found from the email lookup:

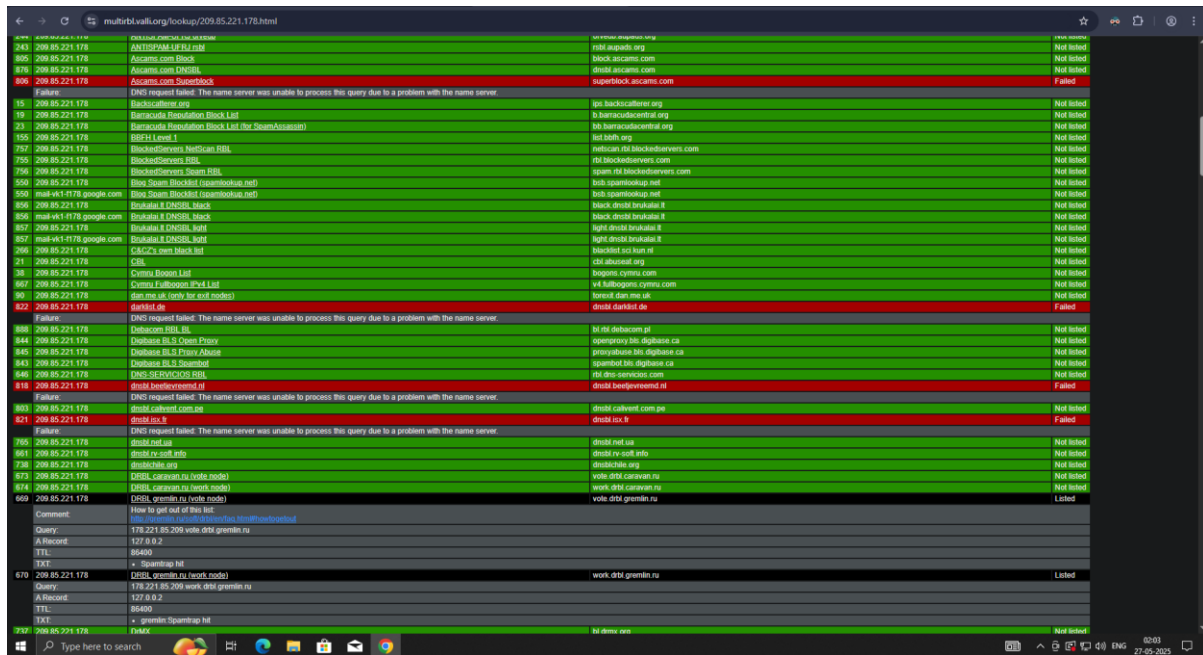
Headers Found	
Header Name	Header Value
Authentication Results	spf-pass (sender IP is 209.85.221.178) smtp.mailfrom=gmail.com; dkim-pass (signature was verified) header-d=gmail.com; dmarc-pass action=none header-from=gmail.com; compact=pass reason=100
Received-SPF	Pass (protection.outlook.com; domain of gmail.com designates 209.85.221.178 as permitted sender) receiver=protection.outlook.com; client-ip=209.85.221.178; helo=mail-v4-1178.google.com; pr=C
X-IncomingTopHeaderMarker	OriginalChecksum:3FC48B36A88B776CDE7569BC1C895B88CF34437A23A580C76C9C1C8D44;UpperCasedChecksum:598CE0981F0625AF54248C6368F4DE046CBAE34DA8894E4E6362DEB761;ScpaReceived:2450;Count:18
DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=gmail.com; s=20210112; h=to:subject:message-id:date:from:sender:reply-to:mime-version:to:cc:bm:dkim; bh=064bunGhwnU11YxSNMawD88VcOTJh4bhuWWhayBICbhuVZheabdlqyS2SD; SPf=pass; RPf=pass; MBZ=AWpaBZJr1h4WYRTWQb3hKZFNb1389505WKGbUbfLXF-1338pq14R9XOE; Mct=W12H5d5fccaTnGFQALRAC5fbc73QZ53epTRhuYTRKG; BU=Hb+vsomgDNLgYyLW4UHVBasfup4pYsdb83jbn5pZFWDTTtW5GPFpOgdl; URTUN; QuhA2HqYtZLuf; S9VY2246; 1972hGawUuCS9f+eodtrlyMnqVqgC-X; hYCA=
X-Google-DKIM-Signature	v=1; a=rsa-sha256; c=relaxed/relaxed; d=1e100.net; s=20210112; h=to:subject:message-id:date:from:sender:reply-to:mime-version; x-gm-message-state=to:cc:bm:dkim; bh=064bunGhwnU11YxSNMawD88VcOTJh4bhuWWhayBICbhuVZheabdlqyS2SD; SPf=pass; MBZ=AWpaBZJr1h4WYRTWQb3hKZFNb1389505WKGbUbfLXF-1338pq14R9XOE; Mct=W12H5d5fccaTnGFQALRAC5fbc73QZ53epTRhuYTRKG; BU=Hb+vsomgDNLgYyLW4UHVBasfup4pYsdb83jbn5pZFWDTTtW5GPFpOgdl; URTUN; QuhA2HqYtZLuf; S9VY2246; 1972hGawUuCS9f+eodtrlyMnqVqgC-X; hYCA=
X-Gm-Message-State	ACgBoo2ubRrTrFdmRqgK5W4g5WuhsJmMcCzV1mK0dZLGLdV9L; ulae5x4ch5CzQ2pBEM4CRMA8BIB9mmWd1=
X-Google-Spam-Source	AM6agR7fhuErOuPBFzVhA7JxTk1mmMbsdZ3oh7yz6R0Z3AcvaU7n9uGcCzhuvgCv7nWwCPheoO688Y=
X-Received	by 2002.a11.1650.0 b0 38c:9034:53 with SMTP id 77.20020a11f6500000000038c9034053m15762964w4 1661439110080; Thu, 25 Aug 2022 07:51:59 -0700 (PDT)
Reply-To	mohammadouattara53@gmail.com
Sender	nadeemkh@gmail.com
From	Mohammad ouattara <mohammadouattara27@gmail.com>
Date	Thu, 25 Aug 2022 07:51:49 -0700
X-Google-Sender-Auth	zZLnF0KGdQh386-uJfupX1gE8
Message-ID	<CAHEH-CRLv_Xb-WGyMn-QUCHMBtHfEY1tmaDOPR3XBo+4dXaQ@mail.gmail.com>
Subject	TREAT WITH CONFIDENCE AND URGENT PLEASE
To	undisclosed-recipients;
Content-Type	text/plain; charset="UTF-8"
Bcc	phishing@pot.org
X-IncomingHeaderCount	18
Return-Path	nadeemkh@gmail.com
X-MS-Exchange-Organization-ExpirationStartTime	25 Aug 2022 14:51:51.3407 (UTC)
X-MS-Exchange-Organization-ExpirationReason	OriginalSubmit
X-MS-Exchange-Organization-ExpirationTimeReason	1.00.00.00.00000000





This tool will check the IP of the sender's mail and see if it is blacklisted on the mailservers.

In the above screenshot I just put the IP into the field input and below is the screenshot provided for the blacklisted results:



Rank	IP	Domain	Status
1	209.85.221.178	asbl.xm.com	Not listed
2	209.85.221.178	asbl.xm.com	Not listed
3	209.85.221.178	asbl.xm.com	Not listed
4	209.85.221.178	asbl.xm.com	Not listed
5	209.85.221.178	asbl.xm.com	Not listed
6	209.85.221.178	asbl.xm.com	Not listed
7	209.85.221.178	asbl.xm.com	Not listed
8	209.85.221.178	asbl.xm.com	Not listed
9	209.85.221.178	asbl.xm.com	Not listed
10	209.85.221.178	asbl.xm.com	Not listed
11	209.85.221.178	asbl.xm.com	Not listed
12	209.85.221.178	asbl.xm.com	Not listed
13	209.85.221.178	asbl.xm.com	Not listed
14	209.85.221.178	asbl.xm.com	Not listed
15	209.85.221.178	asbl.xm.com	Not listed
16	209.85.221.178	asbl.xm.com	Not listed
17	209.85.221.178	asbl.xm.com	Not listed
18	209.85.221.178	asbl.xm.com	Not listed
19	209.85.221.178	asbl.xm.com	Not listed
20	209.85.221.178	asbl.xm.com	Not listed
21	209.85.221.178	asbl.xm.com	Not listed
22	209.85.221.178	asbl.xm.com	Not listed
23	209.85.221.178	asbl.xm.com	Not listed
24	209.85.221.178	asbl.xm.com	Not listed
25	209.85.221.178	asbl.xm.com	Not listed
26	209.85.221.178	asbl.xm.com	Not listed
27	209.85.221.178	asbl.xm.com	Not listed
28	209.85.221.178	asbl.xm.com	Not listed
29	209.85.221.178	asbl.xm.com	Not listed
30	209.85.221.178	asbl.xm.com	Not listed
31	209.85.221.178	asbl.xm.com	Not listed
32	209.85.221.178	asbl.xm.com	Not listed
33	209.85.221.178	asbl.xm.com	Not listed
34	209.85.221.178	asbl.xm.com	Not listed
35	209.85.221.178	asbl.xm.com	Not listed
36	209.85.221.178	asbl.xm.com	Not listed
37	209.85.221.178	asbl.xm.com	Not listed
38	209.85.221.178	asbl.xm.com	Not listed
39	209.85.221.178	asbl.xm.com	Not listed
40	209.85.221.178	asbl.xm.com	Not listed
41	209.85.221.178	asbl.xm.com	Not listed
42	209.85.221.178	asbl.xm.com	Not listed
43	209.85.221.178	asbl.xm.com	Not listed
44	209.85.221.178	asbl.xm.com	Not listed
45	209.85.221.178	asbl.xm.com	Not listed
46	209.85.221.178	asbl.xm.com	Not listed
47	209.85.221.178	asbl.xm.com	Not listed
48	209.85.221.178	asbl.xm.com	Not listed
49	209.85.221.178	asbl.xm.com	Not listed
50	209.85.221.178	asbl.xm.com	Not listed
51	209.85.221.178	asbl.xm.com	Not listed
52	209.85.221.178	asbl.xm.com	Not listed
53	209.85.221.178	asbl.xm.com	Not listed
54	209.85.221.178	asbl.xm.com	Not listed
55	209.85.221.178	asbl.xm.com	Not listed
56	209.85.221.178	asbl.xm.com	Not listed
57	209.85.221.178	asbl.xm.com	Not listed
58	209.85.221.178	asbl.xm.com	Not listed
59	209.85.221.178	asbl.xm.com	Not listed
60	209.85.221.178	asbl.xm.com	Not listed
61	209.85.221.178	asbl.xm.com	Not listed
62	209.85.221.178	asbl.xm.com	Not listed
63	209.85.221.178	asbl.xm.com	Not listed
64	209.85.221.178	asbl.xm.com	Not listed
65	209.85.221.178	asbl.xm.com	Not listed
66	209.85.221.178	asbl.xm.com	Not listed
67	209.85.221.178	asbl.xm.com	Not listed
68	209.85.221.178	asbl.xm.com	Not listed
69	209.85.221.178	asbl.xm.com	Not listed
70	209.85.221.178	asbl.xm.com	Not listed
71	209.85.221.178	asbl.xm.com	Not listed
72	209.85.221.178	asbl.xm.com	Not listed
73	209.85.221.178	asbl.xm.com	Not listed
74	209.85.221.178	asbl.xm.com	Not listed
75	209.85.221.178	asbl.xm.com	Not listed
76	209.85.221.178	asbl.xm.com	Not listed
77	209.85.221.178	asbl.xm.com	Not listed
78	209.85.221.178	asbl.xm.com	Not listed
79	209.85.221.178	asbl.xm.com	Not listed
80	209.85.221.178	asbl.xm.com	Not listed
81	209.85.221.178	asbl.xm.com	Not listed
82	209.85.221.178	asbl.xm.com	Not listed
83	209.85.221.178	asbl.xm.com	Not listed
84	209.85.221.178	asbl.xm.com	Not listed
85	209.85.221.178	asbl.xm.com	Not listed
86	209.85.221.178	asbl.xm.com	Not listed
87	209.85.221.178	asbl.xm.com	Not listed
88	209.85.221.178	asbl.xm.com	Not listed
89	209.85.221.178	asbl.xm.com	Not listed
90	209.85.221.178	asbl.xm.com	Not listed
91	209.85.221.178	asbl.xm.com	Not listed
92	209.85.221.178	asbl.xm.com	Not listed
93	209.85.221.178	asbl.xm.com	Not listed
94	209.85.221.178	asbl.xm.com	Not listed
95	209.85.221.178	asbl.xm.com	Not listed
96	209.85.221.178	asbl.xm.com	Not listed
97	209.85.221.178	asbl.xm.com	Not listed
98	209.85.221.178	asbl.xm.com	Not listed
99	209.85.221.178	asbl.xm.com	Not listed
100	209.85.221.178	asbl.xm.com	Not listed

So, as we can see the mail IP is blacklisted in the mail server; now it proves that the sender of the email is a scammer and performs malicious activity.