

# Task - 2

## Identifying phishing mails

**Step 1:** Download an email from your mail vendor, preferably in .eml format, for analysing the headers in the mail.

**Step 2:** Read through the contents, and understand what the mail is about, so that you get an idea whether the content is actually credible.

```
1 Received: from MN2PR19MB3966.namprd19.prod.outlook.com ([::1] by
2 MN2PR19MB3966.namprd19.prod.outlook.com with HTTPS; Thu, 3 Nov 2022 04:56:17
3 +0000
4 Received: from AM7PR02CA0005.eurprd02.prod.outlook.com (2603:10a6:20b:100::15)
5 by MN2PR19MB3966.namprd19.prod.outlook.com (2603:10a6:20b:100::10) with
6 Microsoft SMTP Server (version=TLS1_2,
7 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5769.16; Thu, 3 Nov
8 2022 04:56:16 +0000
9 Received: from V1EUR05FT048.eop-eur05.prod.protection.outlook.com
10 (2603:10a6:20b:100::14) by AM7PR02CA0005.outlook.office365.com
11 (2603:10a6:20b:100::15) with Microsoft SMTP Server (version=TLS1_2,
12 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5791.22 via Frontend
13 Transport; Thu, 3 Nov 2022 04:56:15 +0000
14 Authentication-Results: spf=none (sender IP is 57.128.69.202)
15 smtp.mailfrom=dturm.de; dkim=none (message not signed)
16 header.d=none; dmarc=none action=none
17 header.from=appjjj.serenitepure.fr;compauth-fail reason=001
18 Received-SPF: None (protection.outlook.com: dturm.de does not designate
19 permitted sender hosts)
20 Received: from dturm.de (57.128.69.202) by
21 V1EUR05FT048.mail.protection.outlook.com (10.233.243.188) with Microsoft
22 SMTP Server id 15.20.5791.20 via Frontend Transport; Thu, 3 Nov 2022 04:56:15
23 +0000
24 X-IncomingTopHeaderMarker:
25 OriginalChecksum:9F3896A6AACB083DF9CDCAFE3B21313D0B1E3B982DA325FC1E8548F8F8B2C2F79;UpperCasedChecksum:444711F080E2E8A44517602CD0F014385C8BF005F6C75560D18F36EEF4F216;SizeAsReceived:969;Count:19
26 Subject: =?UTF-8?B?3j3Ujw==? Zonnepanelen voor een goede prijs
27 From: "Zonnepanelen installateur" <zonnepaneel@appjjj.serenitepure.fr>
28 Sender: "Zonnepanelen installateur" <zonnepaneel@appjjj.serenitepure.fr>
29 Reply-To: "Zonnepanelen installateur" <news@eichakandisha.com>
30 To: phishing@p0t
31 In-Reply-To: <-----f98avdmffv08ke75wtbdr+l=====er/zw-81-7cprfbgjn1-1420221328460rxgmq5n0a1.fichi-fixzag.dturm.de>
32 List-Unsubscribe-Post: List-Unsubscribe=One-Click
33 X-Report-Abuse: abuse@e.serenitepure.fr
34 Feedback-ID: e.serenitepure.fr
35 Content-Type: text/html; charset=utf-8
36 Content-Transfer-Encoding: 7bit
37 Date: Thu, 3 Nov 2022 04:56:15 +0000
38 X-Mid: YmInYmNkU0B0b3RtWl9mZy0Kz2y5qSR2g4Povdx2Um0SAsIHMxNdc30TYxWQ
39 X-Sender: <news@e.serenitepure.fr>
40 X-UID: esmfr-4710-6fa7afdb9514e11c374e301e549caf3
41 Feedback-ID: 4710:esmfr
42 x-ldnv: 2-g782C1Y2D09NwKtp9PFRwXrXdcMgZE1cf9a43276aa0
43 Message-ID: <0.6.0.0.1D0EF489A5C12CE.37AA@dturm.de>
44 X-IncomingHeaderCount: 19
45 Return-Path: return@dturm.de
46 X-MS-Exchange-Organization-ExpirationStartTime: 03 Nov 2022 04:56:15.5649
47 (UTC)
48 X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit
49 X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000
50 X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
51 X-MS-Exchange-Organization-Network-Message-Id:
52 f165ed2e-6d4b-4b6f-b4fe-08dabdb7bcea
53 X-EOPAttributedMessage: 0
54 X-EOPTenantAttributedMessage: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0
55 X-MS-Exchange-Organization-MessageDirectionality: Incoming
56 X-MS-PublicTrafficType: Email
57 X-MS-TrafficTypeDiagnostic: V1EUR05FT048:EE_|MN2PR19MB3966:EE_
58 X-MS-Exchange-Organization-AuthSource:
59 V1EUR05FT048.eop-eur05.prod.protection.outlook.com
60 sample=100.eml
```

Here is what I analysed from this eml file (Refer to the attached .eml file for a better reference):

- Inconsistent use of emails through out the mail, the sender and the reply to mail is not the same.
- No authentication protocols is enforced, (SPF,DKIM,DMARC,compauth) all of them failed, and the email vendor has flagged this, and put them into it's spam folder.
- The sender IP is not associated with the organisation name specified but is associated with a RIPE Network Coordination.
- The url is just http instead of a https, organisations are very much insisted to use HTTPS on hosting their websites. The domain name is nowhere near to the sender.

- And the dutch used in this file, when translated, gives us a content which grabs the reader's attention using emotions, but uses incorrect language grammar, including the incorrect spellings.

Go through the given analysis, this will give us a clear red flag on why this email is not to be trusted and the link given has so many redirections.

- Hareekshith AS