

# 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 MN2PR19MB6312.namprd19.prod.outlook.com with HTTPS; Thu, 3 Nov 2022 04:56:17
3 +0000
4 Received: from AM7PR02CA0005.eurpr02.prod.outlook.com (2003:10a:6:20b:100::15)
5 by MN2PR19MB3966.namprd19.prod.outlook.com (2003:10b:6:20B:1e8:10) with
6 Microsoft SMTP Server (version=TLS_1_2,
7 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5791.16; Thu, 3 Nov
8 2022 04:56:16 +0000
9 Received: from 10.128.0.5:587048.eop-eur05.prod.protection.outlook.com
10 (2003:10a:6:20b:100::14) by MN2PR19MB6312.namprd19.prod.outlook.com
11 (2003:10a:6:20b:100::15) with Microsoft SMTP Server (version=TLS_1_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=dturn.de; dkim=none (message not signed)
16 header.dnone;dmarc=none action=none
17 header.from=appj.serenitepure.fr;compauth=fail reason=001
18 Received: from dturn.de (57.128.69.202) by
19 (2003:10a:6:20b:100::14) with Microsoft SMTP Server (version=TLS_1_2,
20 cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.5791.29 via Frontend Transport; Thu, 3 Nov 2022 04:56:15 +0000
21 X-IncomingTopHeaderMarker:
22 OriginalChecksum:9F309EACB003DF9CDCAFE3B21313DDB1E3B982D325FC1E8548F8F8B8C2F79;UpperCasedChecksum:444711FD0B0E2E8A44517602CD0F014385C88FC05F6FC7556D018F36EEF4F216;SizeAsReceived:969;Count:19
23 +0000
24 X-IncomingHeaderMarker:
25 Subject: =?UTF-8?B?3J+Ui=?= Zonnepanelen voor een goede prijs
26 From: <zonnepanelen installateur> <zonnepanelen@appj.serenitepure.fr>
27 To: <zonnepanelen installateur> <zonnepanelen@appj.serenitepure.fr>
28 Reply-To: <zonnepanelen installateur> <news@chakandisha.com>
29 To: phishing@pt
30 In-Reply-To: -----x98avdmffvobke75+wbtbr-lm==_er/_rw-81-7cpfrbgjnl-142022132846@rxiqmmq5n0a1.fichi-fixzag.dturn.de
31 List-Unsubscribe-Post: List-Unsubscribe=One-Click
32 X-Report-Abuse: abuse@serenitepure.fr
33 Feedback-ID: e.serenitepure.fr
34 Content-Type: text/html; charset="utf-8"
35 Content-Transfer-Encoding: base64
36 Date: Thu, 3 Nov 2022 04:56:15 +0000
37 X-mid: YmlnYnVnMU8o3RtyWslzYGKg2y5gSR2g4Povdx2Um0SAsIHMxNDc3OTYxNQ
38 X-Sender: news@chakandisha.com
39 X-UID: esmfr-4710-6fa7afdb9514e11e374e301e549cfb3
40 Feedback-ID: 4710:esmfr
41 X-idnvc: 2+782C19ZD99NwKTp9PFRxrxrdcMgzEicf9a43276aa0
42 Message-ID: <0.0.0.0.1DEFA49AC12CE.37AA@dturm.de>
43 X-IncomingHeaderCount: 19
44 X-MS-Header-Path: return@dturm.de
45 X-MS-Header-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: 1:00:00:00.000000
50 X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit
51 X-MS-Exchange-Organization-Network-Message-Id:
52 fff65d2e-4d4b-4d8d-b4f1-08da0bd57bce
53 X-EOAttributedMessage: 0
54 X-MS-Exchange-Organization-MessageId: 04df9e7f-e9f6-4aef-b435-aaaaaaaaaaaa:0
55 X-MS-Exchange-Organization-MessageDirectionality: Incoming
56 X-MS-PublicTrafficType: Email
57 X-MS-TrafficTypeDiagnostic: VI1EUR0805FT048:EE_|MN2PR19MB3966:EE_
58 X-MS-Exchange-Organization-AuthSource:
59 VI1EUR0805FT048.eop-eur05.prod.protection.outlook.com
```

utf-8 ( 3 mail 13% 59:1

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 grammer, 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