

Email Header Analysis Report

```
1 Delivered-To: themajoronearth@gmail.com
2 Received: by 2002:a92:bd02:0:0:0:0 with SMTP id c2csp3604485ile;
3 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
4 X-Google-Smtp-Source: ABdhPJxMrOAIW/tZAHoxAwoghq8F8fLpv1xou4CoJ8r9tPXaBGLDruGLq5PtDzenNW5arGU5A99
5 X-Received: by 2002:adf:9b92:: with SMTP id d18mr4483603wrc.170.1611643278636;
6 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
7 ARC-Seal: i=1; a=rsa-sha256; t=1611643278; cv=none;
8 d=google.com; s=arc-20160816;
9 b=hedJHzoAUpL4fSk43IZnla4IXMtoAw3SxcmgyefMYowCr5P8cUwV6ZZPNCjSjQX1Xe
10 5NTMZQ5klqjPo2Pt7XZbK2X9DZfKIqfqsZfW2IoGml/q9FiPvXlv/Ob7s7WL917Do+4y0
11 jRlfqFJ7RXWZaTKVUJk5FjyXR+PAsMterOHzbGZBb5PuWscs+kRzwJ+8ktN/vm7E9C6/
12 4md9RAKtLW3wpnsHarorYj0sz/xlhqLUSK7gvquKXo9QCvWdQOs4hllQ9G3LZMT5QMU
13 kvBZXstcdfuwQBI99LIhsORsiylE8r0qU0N39gI0IMupEXV7oQxAVGofic2dRgAP1jUe
14 lgAA==
15 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
16 h=date:message-id:mime-version:reply-to:errors-to:importance:from
17 :subject:to;
18 bh=GfMK2s9MDbqBDZeyMDCQoZLpa7Z72oNds1X0SgpgQDs=;
19 b=VlLJrpR1Dzc0LUdlnU4WvAn9c2tV54CNGDtba7AyTQmRXWjoPzpad25jlZ5e0t60dJ
20 bvqSxiY0ovvAisfUIPkcsGcPXnJyd8RfaGOWTJXOCCKwQh0dE2pxhEcoK5GCkAtVQTqd
21 Ebjj4vKGL/+e5E5KVan5X/KAKDJlEWxpJnpB9YLW1Fn07Lm/xAVpmfoFo8xw7xc82Urr
22 mXBeSoIfIE5/SOYr9Y/vvQaOX/fZpx3hXqgalEdw4Dq4JCUflDzI9x1wI+F7ckiCneci
23 GWdcoNBZCiE6T8DvFNbDK4Zap03JE62nfp6zUKm8NfYorfQTt3GVbr/iKxEqQ2G5WN
24 V1cw==
25 ARC-Authentication-Results: i=1; mx.google.com;
26 spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
27 Return-Path: <billjobs@microapple.com>
28
29
30 Received: from localhost (emkei.cz. [93.99.104.210])
31 by mx.google.com with ESMTPS id s16sil7017lmj.176.2021.01.25.22.41.18
32 for <themajoronearth@gmail.com>
33 (version=TLS1_2 cipher=ECDHE-ECDSA-CHACHA20-POLY1305 bits=256/256);
34 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
35 Received-SPF: fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) client-ip=93.99.104.210;
36 Authentication-Results: mx.google.com;
37 spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
38
39
40 Received: by localhost (Postfix, from userid 33)
41 id 1993E221F8; Tue, 26 Jan 2021 01:41:18 -0500 (EST)
42
43
44 To: themajoronearth@gmail.com
45 Subject: A Hope to CoCanada
46 From: "Bill" <billjobs@microapple.com>
47 X-Priority: 3 (Normal)
48 Importance: Normal
49 Errors-To: billjobs@microapple.com
50 Reply-To: negeja3921@pashter.com
51 MIME-Version: 1.0
52 Content-Type: multipart/mixed; boundary=BOUND_600FB98E0DCEE8.49207210
53 Message-Id: <20210126064118.1993E221F8@localhost>
54 Date: Tue, 26 Jan 2021 01:41:18 -0500 (EST)
```

1. Basic Information

Item	Detail
1. Delivered-To	themajoronearth@gmail.com
2. Date Sent	26 January 2021, 01:41:18 (EST)
3. Sender	"Bill" billjobs@microapple.com
4. Recipient	themajoronearth@gmail.com
5. Subject	A Hope to CoCanada
6. Reply-To	negeja3921@pashter.com
7. Return-Path	billjobs@microapple.com

```

1 Delivered-To: themajoronearth@gmail.com
2 Received: by 2002:a92:bd02:0:0:0:0 with SMTP id c2csp3604485ile;
3 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
4 X-Google-Smtp-Source: ABdhPJxMrOaiiW/tZAH0xAWohqg8F8fLpvlxou4CoJ8r9tPXaB6LDruGLq5PtDzenNW5arGU5A99
5 X-Received: by 2002:adf:9b92:: with SMTP id d18mr4483603wrc.170.1611643278636;
6 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
7 ARC-Seal: i=1; a=rsa-sha256; t=1611643278; cv=none;
8 d=google.com; s=arc-20160816;
9 b=hedJHzoAUpL4fSk43IZnla4IXMtoAw3SxCMgyeIMYowCr5P8cUwV6ZZPNCjsjQXlXe
10 5NtMZQ5k1qjPo2Pt7XZbK2X9DZfKIFqs2Fw2IoGm1/q9F1PvXlv/Ob7s7WL917Do+4y0
11 jRlfqFJ7RXWZaTKVUJk5FjyxR+PAsMterOHZbGZBb5PuWscS+kRzwJ+8ktN/vm7E9C6/
12 4md99RAKtLW3wpnsHarorYjo0sz/xlhqLUSK7gvquKXo9QCvWdQOs4h1lQ9G3LZMT5QMU
13 kvBZxtcDfufQBI99LHs0RsiylE8r0qU0N39gI0IMupEXV7oQxAVGofic2dRgAP1jUe
14 lgAA==
15 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
16 h=date:message-id:mime-version:reply-to:errors-to:importance:from
17 :subject:to;
18 bh=GfMK2s9MDbqBDZeyMDCQo2Lpa7Z72oNds1X0SgppqDs=;
19 b=VLLJpR1Dzc0LUdlnU4WvAn9c2tV54CNGDtba7AyTQmRXWjoPzpad25j1Z5eOt6oDJ
20 bvsXiiY0ovvVAisfUIPkcsGcPxnJyd8Rfag0WTJXOCcKwQh0dE2pxhEcok5GCKAtVQTqd
21 Ebjj4vKGl/+e5E5KVan5X/KAKDJLEWxpJnpB9YlW1Fn07Lm/xAVpmfo8xw7xc82Urr
22 mXbeSoIf1E5/SOYr9Y/wvQa0X/fzpx3hXqgaEdw4Dq4JCUfldzI9xlwI+F7ckiCneCi
23 GWDcoMBZC1E6T8DvVPNbDK4KZap03JE62nfph6zUKm6NfYorfQTt3GVbr/iKxEq2G5WN
24 Vlcw==
25 ARC-Authentication-Results: i=1; mx.google.com;
26 spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
27 Return-Path: <billjobs@microapple.com>
28
29
30 Received: from localhost (emkei.cz. [93.99.104.210])
31 by mx.google.com with ESMTPS id s16sil70171wmj.176.2021.01.25.22.41.18
32 for <themajoronearth@gmail.com>
33 (version=TLS1_2 cipher=ECDHE-ECDSA-CHACHA20-POLY1305 bits=256/256);
34 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
35 Received-SPF: fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) client-ip=93.99.104.210;
36 Authentication-Results: mx.google.com;
37 spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
38 Received: by localhost (Postfix, from userid 33)
39 id 1993E221F8; Tue, 26 Jan 2021 01:41:18 -0500 (EST)
40
41
42 To: themajoronearth@gmail.com
43 Subject: A Hope to CoCanDa
44 From: "Bill" <billjobs@microapple.com>
45 X-Priority: 3 (Normal)
46 Importance: Normal
47 Errors-To: billjobs@microapple.com
48 Reply-To: negeja3921@pashter.com
49 MIME-Version: 1.0
50 Content-Type: multipart/mixed; boundary=BOUND_600FB98E0DCEE8.49207210
51 Message-ID: <20210126064118.1993E221F8@localhost>
52 Date: Tue, 26 Jan 2021 01:41:18 -0500 (EST)

```

2. Email Routing (Received Hops)

The email went through these steps:

Step	Server	Details
1	localhost (Postfix)	Email generated locally on server (fake localhost)
2	emkei.cz [93.99.104.210]	Free fake email generator server
3	Google server (mx.google.com)	Google's incoming mail server received it
4	Internal Google servers (IDs: c2csp3604485ile, d18mr4483603wrc)	Internal Google handling before final delivery

```

1 Delivered-To: themajoroneearth@gmail.com
2 Received: by 2002:a92:bd02:00:0:0:0 with SMTP id s3cep3604485ile 4
3 Mon, 25 Jan 2021 22:41:18 -0800 (EST)
4 X-Google-Smtp-Source: ABdhBLwMORaiW/tZAR0XAwohqg9F8fpuLwCtC0d8r9tFXaBGidruGLq5PtDzenNW5arGU5A99
5 X-Received: by 2002:adf:9b92: with SMTP id cmr4483603wrc.170.1611643278636
6 Mon, 25 Jan 2021 22:41:18 -0800 (EST)
7 ARC-Seal: i=1; a=rsa-sha256; t=1611643278; cv=none;
8 d=google.com; s=arc-20160816;
9 b=hedJH2oAUpL4fSk43I2n1a4IXMtoAw3SxCMqyeFMYowCr5P8cUwV6Z2PNCjsjQX1Xe
10 5NtMQ5klqjPo2Pt7XzbK2X9DZfKifqsZFW2IoGml/q9FiFvXlv/Ob7s7WL917Do+4y0
11 jRlFqF7RXwZaTKVUJk5FjyXR+PAsMTerOHZbGZBb5PuWscS+kRzwJ+8ktN/vm7E9C6/
12 4md9RAKtLW3wpnsHarorYjo0sz/xlhqLUSK7gvquKXo9QCvWdQ0s4h1lQ9G3LZMT5QMU
13 kvBZstcDfuwQBI99Lhs0RsiylE8r0QUON39gI0IMupEXV7oQxAVGofic2dRgAP1Ue
14 lgAA==
15 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
16 h=date:message-id:mime-version:reply-to:errors-to:importance:from
17 :subject:to;
18 bh=GfMK2s9MDbqBDZeyMDCQoZLpa7Z72oNdlX0SgpgQDs=;
19 b=VllJepR1Dze0L0dlnU4WwAn9c2tV54CNGDtha7AyT0mEXWjoPzpad25j1Z5eot60dJ
20 bvqSxiY0ovvAisfUIPkscGcPxnJyd8RfaG0WTJXocKwQh0dE2pxhEco5GCKatVQTqd
21 Ebjj4vKgl/+e5E5KVan5X/KAKDJIEWxpJnpB9YLWlFn07Lm/xAVpmfoFo8Xw7xc82Urr
22 mXbeSoIf1E5/SOYr9Y/vwQa0X/f2px3XqgalEdw4Dq4JCufldZi9x1wI+F7ckiCneci
23 GWDcoNBZCIE6T9DvFPNbDK4ap03JE62nph6zUKm8NfYorQT3GVbr/ikXEq2G5WN
24 Vlcw==
25 ARC-Authentication-Results: i=1; mx.google.com;
26 spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
27 Return-Path: <billjobs@microapple.com>
28
29
30 Received: from localhost (emkei.cz. [93.99.104.210])
31 by mx.google.com with ESMTPS id s16s117017lwmj.176.2021.01.25.22.41.18
32 for <themajoroneearth@gmail.com>
33 (version=TLS1_2 cipher=ECDHE-ECDSA-CHACHA20-POLY1305 bits=256/256);
34 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
35 Received-SPF: fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) client-ip=93.99.104.210;
36 Authentication-Results: mx.google.com;
37 spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
38 Received: by localhost (Postfix, from userid 33)
39 id 1993E221F8; Tue, 26 Jan 2021 01:41:18 -0500 (EST)
40
41
42 To: themajoroneearth@gmail.com
43 Subject: A Hope to CoCanada
44 From: "Bill" <billjobs@microapple.com>
45 X-Priority: 3 (Normal)
46 Importance: Normal
47 Errors-To: billjobs@microapple.com
48 Reply-To: negeja392l@pashter.com
49 MIME-version: 1.0
50 Content-Type: multipart/mixed; boundary=BOUND_600FB98E0DCEE8.49207210
51 Message-Id: <20210126064118.1993E221F8@localhost>
52 Date: Tue, 26 Jan 2021 01:41:18 -0500 (EST)

```

Key Points:

- The email originated from a fake email tool (localhost/emkei.cz).
- It traveled securely to Google using TLS1.2 encryption.
- Google assigned internal IDs as it moved through Google's servers.

3. Authentication Analysis

Check	Result	Comment
SPF	Fail	Sender IP 93.99.104.210 is NOT authorized to send emails for domain microapple.com.
ARC	Present	Google applied ARC (Authenticated Received Chain) to record the authentication results.
ARC-Authentication-R results	spf=fail	Repeats that SPF failed at Google's mail server.
ARC-Seal	Present	Google sealed the ARC chain with RSA-SHA256 encryption.

Important:

- **SPF** failure suggests the email is **very likely forged or suspicious**.
 - **ARC** records exist because Google wants to preserve what they observed, even if email is forwarded further.
-

4. Technical Details

Header	Value
MIME-Version	1.0
Content-Type	multipart/mixed (Email has attachment or multiple parts)
Message-ID	20210126064118.1993E221F8@localhost
X-Priority	3 (Normal)
Importance	Normal
Errors-To	billjobs@microapple.com

5. Security Observations

- **Sender Identity:**
 - Claimed to be from **billjobs@microapple.com**, but really sent from a suspicious server (not microapple.com official server).
- **Spoofing Attempt:**
 - Usage of **emkei.cz** (known fake email service) suggests the sender wanted to **impersonate** someone.
- **Reply-To Different:**
 - The **Reply-To** address is different (**negeja3921@pashter.com**) → classic sign of **phishing or fraud** attempt (sending you to a different email).
- **SPF Failure:**

- Strong signal the email was **not authorized** by the real owner of microapple.com.
- **ARC Present:**
 - Google took the extra step to **seal** the authentication results to help any future email forwarding stay verified.

6. Final Verdict

This email is highly suspicious and likely a spoofed (forged) email. It failed SPF authentication, originated from a fake email service, and tried to impersonate a trusted domain (microapple.com).

Caution is advised — do not trust links, attachments, or reply to this email.

7. Visual Summary

[localhost (Postfix)] ➡ [emkei.cz server 93.99.104.210] ➡ [Google (mx.google.com)] ➡ [Delivered to inbox]
SPF Fail ARC Chain Recorded

8. Sources

[Email Header Analysis.eml](#)
[Chatgpt_Support](#)

E N D

thanuka03@gmail.com