

## Mîndruleanu Matei Daniel - tema 2 SSI

### Exercitiul 1:

A 4

B 2

C 1

D 3

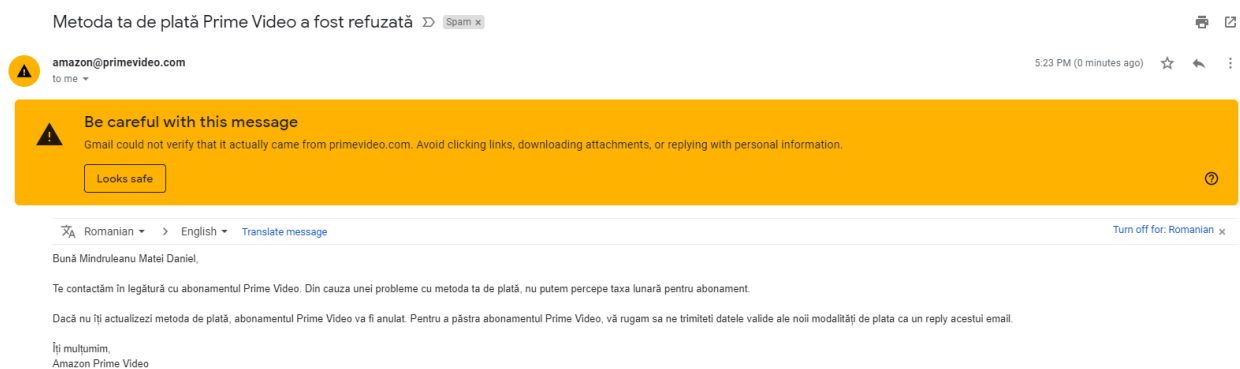
E 6

F 5

### Exercitiul 2:

- emailul de pe care este trimis acest mail.
- link-ul de zozweb de jos.
- faptul ca mail-ul a fost marcat automat ca junk.
- greselile de scriere din text.

### Exercitiul 3:



Mail-ul din screenshot-ul de mai sus este un mail de tip phishing pe care mi l-am trimis singur. Mail-ul are ca obiectiv obținerea datelor cardului/metodei de plată cu care victima își plătește contul de Amazon Prime. Observăm că gmail-ul ne anunță automat că este ceva în neregulă cu acest mail 😞.

Analizarea header-ului folosind <https://mha.azurewebsites.net/> :

6	ARC-Authentication-Results	is 1; mx.google.com: spf=fail (google.com: domain of amazon@primevideo.com does not designate 101.99.94.116 as permitted sender) smtp.mailfrom=amazon@primevideo.com; dmarc=fail (p=QUARANTINE sp=QUARANTINE dis=QUARANTINE) header.from=primevideo.com
---	----------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**From** Amazon Prime Video <amazon@primevideo.com>  
**Reply to** amazon@primevideo.com  
**To** mateimindruleanu@gmail.com

Received headers					
Hop↓	Submitting host	Receiving host	Time	Delay	Type ⇒
1		emkei.cz (Postfix, from userid 33)	11/12/2021 5:23:00 PM		
2	emkei.cz (emkei.cz, [101.99.94.116])	mx.google.com	11/12/2021 5:23:01 PM	1 second	ESMTPS
3		2002:a50:34c3:0:0:0:0:0	11/12/2021 5:23:01 PM	0 seconds	SMTP


Analizarea header-ului folosind <https://toolbox.googleapps.com/apps/messageheader/> :

MessageId	20211112152300.E15182834B@emkei.cz
Created at:	11/12/2021, 5:23:00 PM GMT+2 ( Delivered after 1 sec )
From:	Amazon Prime Video <amazon@primevideo.com>
To:	mateimindruleanu@gmail.com
Subject:	Metoda ta de plată Prime Video a fost refuzată
SPF:	fail with IP Unknown! <a href="#">Learn more</a>
DMARC:	fail <a href="#">Learn more</a>

#	Delay	From *	To *	Protocol	Time received
0	1 sec	emkei.cz	→ [Google] mx.google.com	ESMTPS	11/12/2021, 5:23:01 PM GMT+2
1			→ [Google] 2002:a17:907:1c85::	SMTP	11/12/2021, 5:23:01 PM GMT+2
2			→ [Google] 2002:a50:34c3:0:0:0:0:0	SMTP	11/12/2021, 5:23:01 PM GMT+2

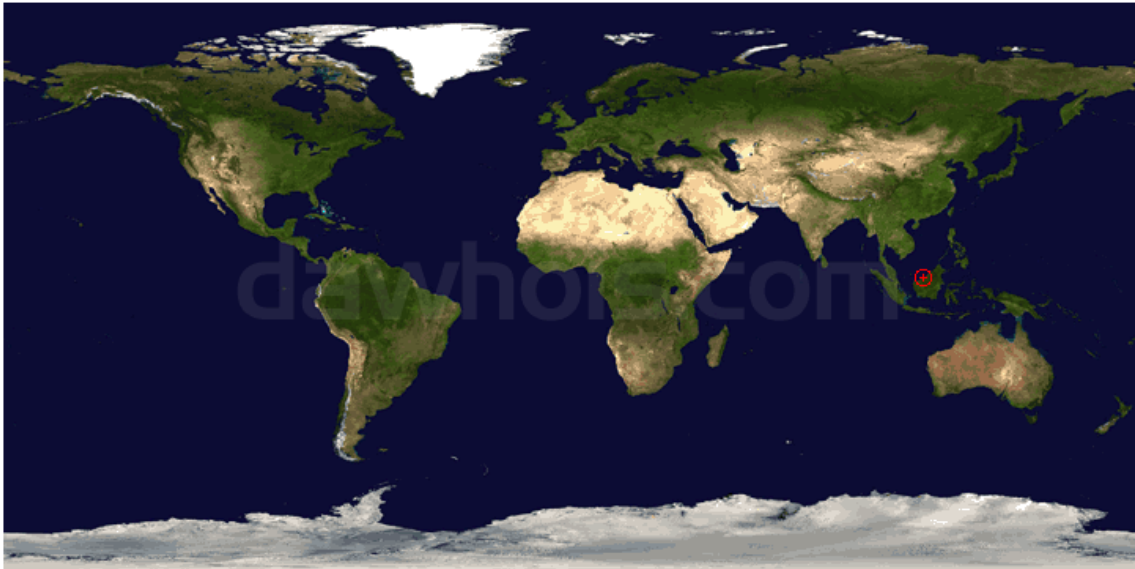
Analizarea Ip-ului folosind [101.99.94.116 whois lookup - Whois \(dawhois.com\)](https://101.99.94.116.whois.lookup-Whois.dawhois.com) :

101.99.94.116 - Geo Information

IP Address	<a href="https://101.99.94.116.whois.lookup-Whois.dawhois.com">101.99.94.116</a>
Host	emkei.cz
Location	 MY, Malaysia
City	- ,
Organization	Piradius Net
ISP	Piradius Net
Latitude	2 ° 50'00" North
Longitude	112 ° 50'00" East
Distance	9751.91 km (6059.56 miles)

Map Location

☒ [World Map](#)
☐ [Google Maps](#)
☐ [Yahoo Maps](#)
☐ [Microsoft Live Maps](#)



Compararea cu analizarea unui header si ip de la un mail legitim de la amazon:

9	Authentication-Results	mx.google.com; dkim=pass header.i=@primevideo.com headers.s=ffepm36afmbr4x4kcgthnln7d5c header.b="Y/C050"; dkim=pass header.i=@amazon.com headers.s=ukultai25t5tblgky6ym32ef7uqv header.b="QnK/050"; spf=pass (google.com: domain of 20210629091716e6031562310649f7bcedbcb7c5a0p@eu.bounces.primevideo.com designates 54.240.1.103 as permitted sender) smtp.mailfrom=20210629091716e6031562310649f7bcedbcb7c5a0p@eu.bounces.primevideo.com; dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE) header.from=primevideo.com
10	DKIM-Signature	v=1; s=xnse-sha256; q=dns/txt; c=relaxed/simple; s=ffepm36afmbr4x4kcgthnln7d5c; d=primevideo.com; ts=1624958236; hu=From/Reply-To/Message-ID/Subject/MIME-Version/Content-Type/Date; bh=xKPLggrj5/hak10X5c2u6L13ymvZQ8+UKXVTlgacx; b=FV/CDS0HzbaggS1mqz9QbmMBUjho4E+Q7bC8Q9N9b43Um54ocfveKbTD/1bt2uvQ2ND1gECg1wciPSPMcIOyISiqcYvan3qg/L2NquW/30qjIgr57e ATChADh3kXKw052b4pSSWBhde8X3z5MoLM8=
11	DKIM-Signature	v=1; s=xnse-sha256; q=dns/txt; c=relaxed/simple; s=ukultai25t5tblgky6ym32ef7uqv; d=amazon.com; ts=1624958236; hu=From/Reply-To/Message-ID/Subject/MIME-Version/Content-Type/Date/Feedback-ID; bh=xKPLggrj5/hak10X5c2u6L13ymvZQ8+UKXVTlgacx; b=QnK/050W8Mh4KcTs7ua1Ccsnef8BAo8Xn-cR+mo58cDIFDRWqYqNMIC0gCz 12C65V/RqoFD93ud8p8wntg11j/C31xLE5q2Hhng1R8hSUPQK6G/ZjgU6Tf GQGasiUm/u7Kao3qdort5NpBZC8w60vcjCSac=


Received headers

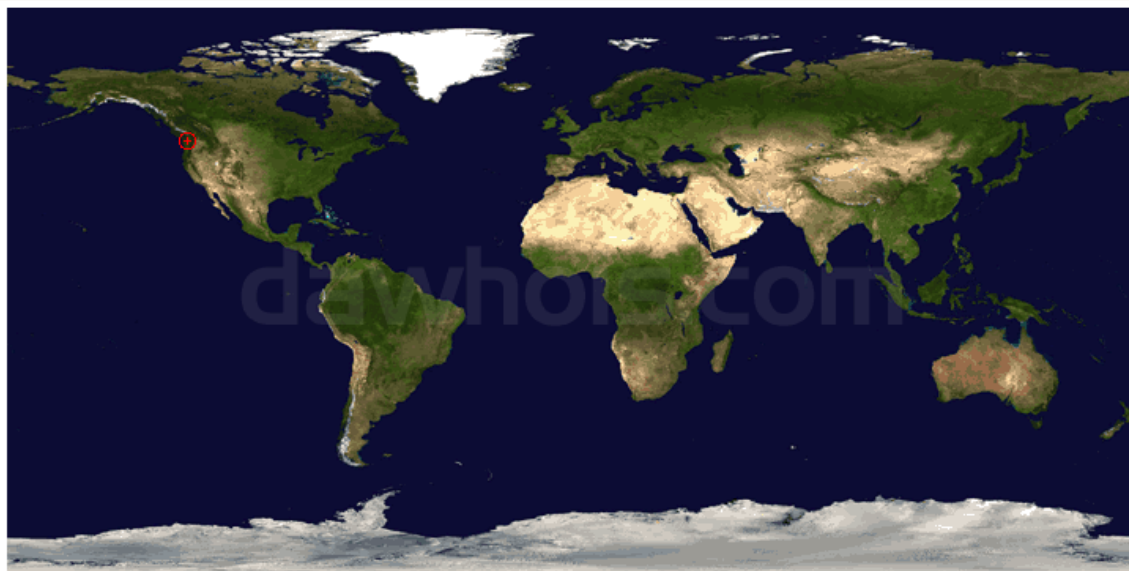
HopI	Submitting host	Receiving host	Time	Delay	Type =>
1	a1-103.smtp-out.eu-west-1.amazonaws.com (a1-103.smtp-out.eu-west-1.amazonaws.com. [54.240.1.103])	mx.google.com	6/29/2021 12:17:17 PM		ESMTPS
2		2002:a54:2b01:0:0:0:0	6/29/2021 12:17:17 PM	0 seconds	SMTP

MessageId	0102017a570ef8d4-e20177cd-bc9c-43a1-bf10-6d24298aeb96-000000@eu-west-1.amazonaws.com
Created at:	6/29/2021, 12:17:16 PM GMT+3 ( Delivered after 1 sec )
From:	Amazon Prime Video <no-reply@primevideo.com>
To:	mateimindruleanu@gmail.com
Subject:	Metoda ta de plată Prime Video a fost refuzată
SPF:	pass with IP 54.240.1.103 <a href="#">Learn more</a>
DKIM:	pass with domain primevideo.com pass with domain amazonSES.com <a href="#">Learn more</a>
DMARC:	pass <a href="#">Learn more</a>

#	Delay	From *		To *	Protocol	Time received
0	1 sec	a1-103.smtp-out.eu-west-1.amazonaws.com.	→	[Google] mx.google.com	<a href="#">ESMTPS</a>	6/29/2021, 12:17:17 PM GMT+3
1			→	[Google] 2002:a1c:f30e::	<a href="#">SMTP</a>	6/29/2021, 12:17:17 PM GMT+3
2			→	[Google] 2002:a54:2b01:0:0:0:0:0	<a href="#">SMTP</a>	6/29/2021, 12:17:17 PM GMT+3

### 54.240.1.103 - Geo Information

IP Address	<a href="#">54.240.1.103</a>
Host	a1-103.smtp-out.eu-west-1.amazonses.com
Location	 US, United States
City	Seattle, WA 98144
Organization	Amazon.com
ISP	Amazon Technologies
AS Number	AS16509 Amazon.com, Inc.
Latitude	47° 58'39" North
Longitude	122° 29'95" West
Distance	9424.61 km (5856.18 miles)
Map Location <sup>new</sup>	<input checked="" type="radio"/> <a href="#">World Map</a> <input type="radio"/> <a href="#">Google Maps</a> <input type="radio"/> <a href="#">Yahoo Maps</a> <input type="radio"/> <a href="#">Microsoft Live Maps</a>



La compararea analizelor mail-urilor observam ca din mail-ul fake lipseste DKIM-ul, iar SPF-ul si DMARC-ul sunt semnalate ca fail, iar locatia este in Malaezia, la organizatia Piradius Net, chiar daca mail-ul este de la amazon. In mail-ul real, DKIM-ul, SPF-UL si DMARC-ul sunt toate semnalate cu verde ca si cum au trecut verificarile, in timp ce locatia este in America la organizatia Amazon.