

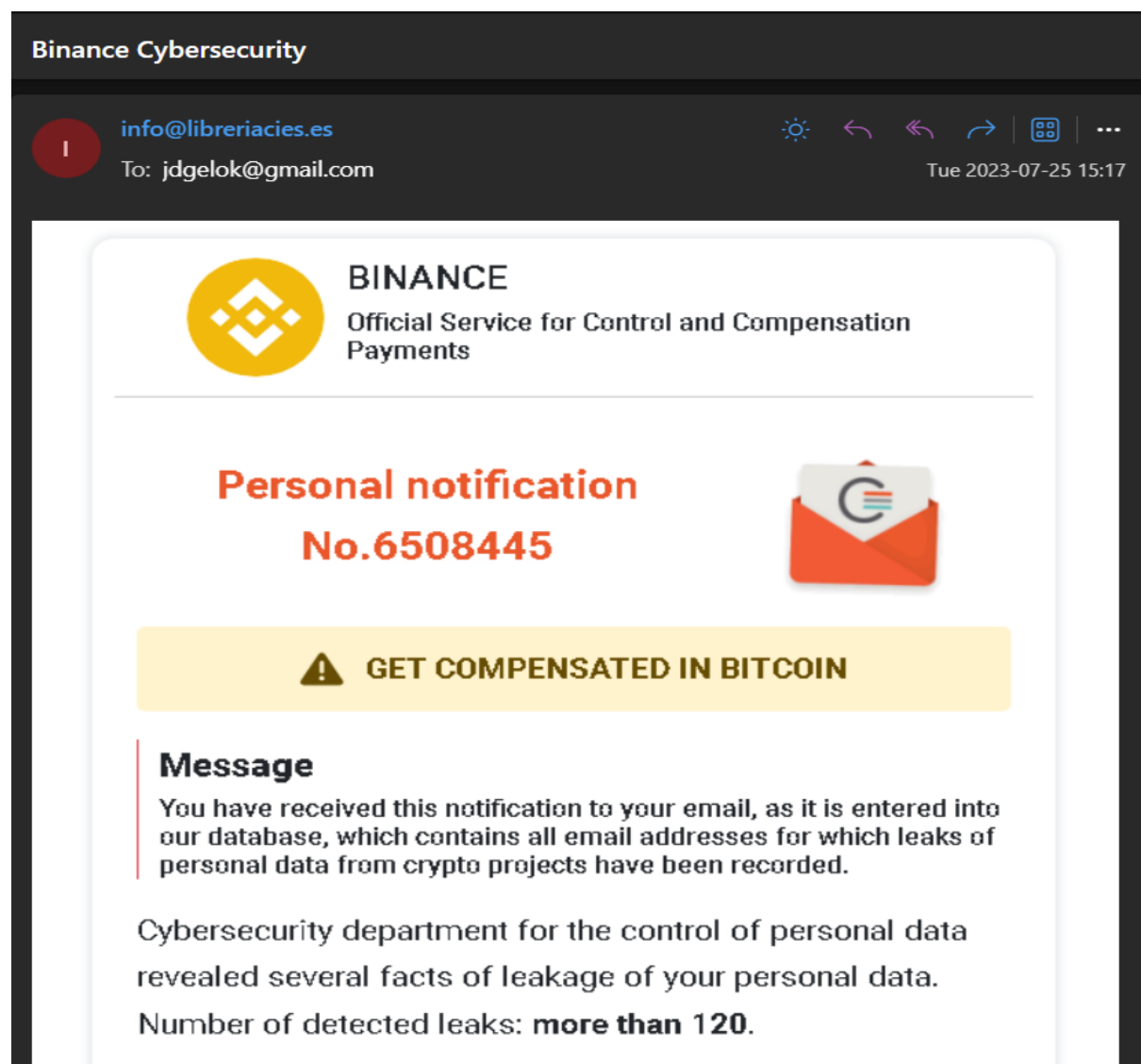
Task 2: Analyze a Phishing Email Sample.

Objective: Identify phishing characteristics in a suspicious email sample.

Tools: Email client or saved email file (text), free online header analyzer.

Deliverables: A report listing phishing indicators found

1. Sample Phishing Email:



2. Sender's email address doesn't match with the company name:

- i. Company name: Binance
- ii. Sender's email address: [info@libreriacies\[.\]es](mailto:info@libreriacies.es)

3. Email header results:

Host	Delay	From	By	With	Time (UTC)	Blacklist
1	*	smtp.gmail.com 43.230.161.16	serlogal.arnoia.com	ESMTPSA	7/25/2023 9:47:28 AM	✓
2	6 seconds	serlogal.arnoia.com 217.18.161.43	BN8NAM12FT011.mail.protection.outlook.com 10.13.183.146	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	7/25/2023 9:47:34 AM	✓
3	1 Second	BN8NAM12FT011.eop-nam12.prod.protection.outlook.com 2603:10b6:408:106:cafe:a0	BN9PR03CA0616.outlook.office365.com 2603:10b6:408:106:21	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	7/25/2023 9:47:35 AM	✓
4	0 seconds	BN9PR03CA0616.namprd03.prod.outlook.com 2603:10b6:408:106:21	PH0PR19MB5396.namprd19.prod.outlook.com 2603:10b6:510:fa:20	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	7/25/2023 9:47:35 AM	✓
5	2 seconds	PH0PR19MB5396.namprd19.prod.outlook.com ::1	MN0PR19MB6312.namprd19.prod.outlook.com	HTTPS	7/25/2023 9:47:37 AM	✗

4. Suspicious attachments:

- Image with the link.
- Redirected link.

Personal notification
No.6508445



5. Language used:

- Threatening (data loss)
- Reward (compensation in bitcoin)



GET COMPENSATED IN BITCOIN

Message

You have received this notification to your email, as it is entered into our database, which contains all email addresses for which leaks of personal data from crypto projects have been recorded.

Cybersecurity department for the control of personal data revealed several facts of leakage of your personal data.
Number of detected leaks: **more than 120.**

6. Links present are redirecting to different site:

7. Summarizing the traits used in this phishing email:

- i. Sender's email mismatch as of company name.
- ii. Image with link redirecting to different site.
- iii. Link which is also redirecting to different site (same to image link).
- iv. Threatening language used (data leak).
- v. Giving reward (bitcoin compensation)