Test Report

(Task 2)

Name:Akhilesh.M

CIN ID:FIT/JAN26/5527

Github: https://github.com/ig-immortal

PHISHING EMAIL DETECTIONS AND AWARENESS SYSTEM

Phishing

Phishing is one of the most common cyberattacks today, where criminals impersonate trusted organizations to trick people into revealing sensitive information like passwords, credit card numbers, or personal details. These attacks often arrive as emails that look authentic, create urgency, and push victims to click links or download attachments, leading to identity theft, financial loss, or malware infection.

📧 What is Phishing?

- **Definition: A fraudulent attempt to steal sensitive information by pretending to be a legitimate entity such as a bank, government agency, or popular website.**
- **Mechanism: Attackers send fake emails or create websites that mimic real ones, luring victims into entering confidential data.**
- **Goal: Steal credentials, financial details, or install malware.**

🔑 Characteristics of Phishing Emails

- **Suspicious sender address: Domains slightly altered (e.g., micros0ft.com).**
- **Urgency or fear tactics: “Your account will be locked in 24 hours.”**
- **Generic greetings: “Dear Customer” instead of your name.**
- **Fake links: URLs that look legitimate but redirect to malicious sites.**
- **Unexpected attachments: Files that may contain malware.**
- **Too-good-to-be-true offers: Promises of rewards or refunds.**

🎭 Types of Phishing Attacks

Type	Description	Example
Email Phishing	Mass emails urging clicks or downloads	“Update your PayPal account now”
Spear Phishing	Targeted at specific individuals/orgs	CFO receives fake invoice request
Whaling	Targets executives	CEO asked to approve wire transfer
Smishing	Phishing via SMS	“Your bank account is blocked, click here”
Vishing	Voice phishing via phone calls	Caller posing as tax authority
Clone Phishing	Duplicate of a real email with malicious links	Resent “meeting invite” with malware

---

⚠️ Risks of Falling Victim

- **Identity theft: Stolen personal details used for fraud.**
- **Financial loss: Unauthorized transactions or wire transfers.**
- **Malware infection: Attachments install spyware or ransomware.**
- **Corporate breaches: Compromised accounts lead to data leaks.**
- **Reputation damage: If attackers impersonate your organization.**

🛡️ Prevention & Protection

- **Verify sender details before clicking.**
- **Hover over links to check URLs.**
- **Don’t download unexpected attachments.**
- **Enable multi-factor authentication (MFA) for accounts.**
- **Use email security filters and anti-phishing tools.**
- **Report suspicious emails to IT/security teams.**
- **Educate employees/users regularly on phishing awareness.**

✅ Key Takeaway

Phishing thrives on deception and urgency. The best defense is vigilance: always verify before clicking, question unexpected requests, and rely on trusted channels.

Phishing email samples

Received: from SA3PR19MB7370.namprd19.prod.outlook.com (::1) by

MN0PR19MB6312.namprd19.prod.outlook.com with HTTPS; Tue, 19 Sep 2023 18:36:46

+0000

Received: from BN0PR03CA0023.namprd03.prod.outlook.com (2603:10b6:408:e6::28)

by SA3PR19MB7370.namprd19.prod.outlook.com (2603:10b6:806:317::17) with

Microsoft SMTP Server (version=TLS1_2,

cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.27; Tue, 19 Sep

2023 18:36:45 +0000

Received: from BN8NAM11FT066.eop-nam11.prod.protection.outlook.com

(2603:10b6:408:e6:cafe::23) by BN0PR03CA0023.outlook.office365.com

(2603:10b6:408:e6::28) with Microsoft SMTP Server (version=TLS1_2,

cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id 15.20.6792.28 via Frontend

Transport; Tue, 19 Sep 2023 18:36:45 +0000

Authentication-Results: spf=temperror (sender IP is 137.184.34.4)

smtp.mailfrom=ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06; dkim=none (message not

signed) header.d=none;dmarc=temperror action=none

header.from=atendimento.com.br;compauth=fail reason=001

Received-SPF: TempError (protection.outlook.com: error in processing during

lookup of ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06: DNS Timeout)

Received: from ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (137.184.34.4) by

BN8NAM11FT066.mail.protection.outlook.com (10.13.177.138) with Microsoft SMTP

Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384) id

15.20.6813.19 via Frontend Transport; Tue, 19 Sep 2023 18:36:44 +0000

X-IncomingTopHeaderMarker:

OriginalChecksum:3B61F64750F88C5569DF38A496B2374685F23D8BC662A6A19B6823B2F6745D54;UpperCasedChecksum:62071BC7A7CF5B0844A7B406B0E9EFCDAA2CB94988E687CF8C56555AD4B52D30;SizeAsReceived:544;Count:9

Received: by ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06 (Postfix, from userid 0)

id 39DEA3F725; Tue, 19 Sep 2023 18:35:49 +0000 (UTC)

Content-type: text/html; charset=UTF-8

Content-Transfer-Encoding: base64

Subject: CLIENTE PRIME - BRADESCO LIVELO: Seu cartão tem 92.990 pontos LIVELO expirando hoje!

From: BANCO DO BRADESCO LIVELO<banco.bradesco@atendimento.com.br>

To: phishing@pot

Message-Id: <20230919183549.39DEA3F725@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06>

Date: Tue, 19 Sep 2023 18:35:49 +0000 (UTC)

X-IncomingHeaderCount: 9

Return-Path: root@ubuntu-s-1vcpu-1gb-35gb-intel-sfo3-06

X-MS-Exchange-Organization-ExpirationStartTime: 19 Sep 2023 18:36:44.2236

(UTC)

X-MS-Exchange-Organization-ExpirationStartTimeReason: OriginalSubmit

X-MS-Exchange-Organization-ExpirationInterval: 1:00:00:00.0000000

X-MS-Exchange-Organization-ExpirationIntervalReason: OriginalSubmit

X-MS-Exchange-Organization-Network-Message-Id:

b9106deb-bd54-4815-e5c9-08dbb93f5fab

X-EOPAttributedMessage: 0

X-EOPTenantAttributedMessage: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa:0

X-MS-Exchange-Organization-MessageDirectionality: Incoming

X-MS-PublicTrafficType: Email

X-MS-TrafficTypeDiagnostic:

BN8NAM11FT066:EE_|SA3PR19MB7370:EE_|MN0PR19MB6312:EE_

X-MS-Exchange-Organization-AuthSource:

BN8NAM11FT066.eop-nam11.prod.protection.outlook.com

X-MS-Exchange-Organization-AuthAs: Anonymous

X-MS-UserLastLogonTime: 9/19/2023 6:25:15 PM

X-MS-Office365-Filtering-Correlation-Id: b9106deb-bd54-4815-e5c9-08dbb93f5fab

X-MS-Exchange-EOPDirect: true

X-Sender-IP: 137.184.34.4

X-SID-PRA: BANCO.BRADESCO@ATENDIMENTO.COM.BR

X-SID-Result: NONE

X-MS-Exchange-Organization-PCL: 2

X-MS-Exchange-Organization-SCL: 5

X-Microsoft-Antispam: BCL:9;

X-MS-Exchange-CrossTenant-OriginalArrivalTime: 19 Sep 2023 18:36:44.1298

(UTC)

X-MS-Exchange-CrossTenant-Network-Message-Id: b9106deb-bd54-4815-e5c9-08dbb93f5fab

X-MS-Exchange-CrossTenant-Id: 84df9e7f-e9f6-40af-b435-aaaaaaaaaaaa

X-MS-Exchange-CrossTenant-AuthSource:

BN8NAM11FT066.eop-nam11.prod.protection.outlook.com

X-MS-Exchange-CrossTenant-AuthAs: Anonymous

X-MS-Exchange-CrossTenant-FromEntityHeader: Internet

X-MS-Exchange-CrossTenant-RMS-PersistedConsumerOrg:

00000000-0000-0000-0000-000000000000

X-MS-Exchange-Transport-CrossTenantHeadersStamped: SA3PR19MB7370

X-MS-Exchange-Transport-EndToEndLatency: 00:00:02.6179349

X-MS-Exchange-Processed-By-BccFoldering: 15.20.6792.025

X-Microsoft-Antispam-Mailbox-Delivery:

wl:1;pcwl:1;ucf:0;jmr:0;ex:0;psp:0;auth:0;dest:I;OFR:TrustedSenderList;ENG:(5062000305)(920221119095)(90000117)(920221120095)(91040095)(9050020)(9075021)(9100341)(944500132)(2008001134)(4810010)(4910033)(9610028)(9560006)(10180021)(9439006)(9310011)(9220031)(120001);

X-Message-Info:

qZelhIiYnPlgo3oeAkqKQrb/Je8fpvpPmRGjYwLej8PYXc5p/l16IG5I8gDUPoij+JWSvja0BAMLtkgrOcbx5zEN7V98T2UZUZs4k8BX/DcDfI7QJ0t2aouiqx4ENvkR1M3sDKP/XN09+50x9Rxi6onUtDV4eqq36VUi2qAa0zCzkJwjdI3Y9DzNE1OkaWjrHAizeUyMZ/UtK/Pz9zhA2A==

X-Message-Delivery:
Vj0xLjE7dXM9MDtsPTA7YT0wO0Q9MTtHRD0yO1NDTD0tMQ==

X-Microsoft-Antispam-Message-Info:

=?utf-8?B?QTlXRFVaTVRhbmFzVTRkbVBTSFRSUURrQTRyaDhzZVczY2RROWF3bVVDTWdk?=

=?utf-8?B?bVU0VHJ2UU9wWUFLbXlFRWVUcmx1Z244ajk4M0JMRVYzZW9WVkE3NVZpK0dp?=

=?utf-8?B?STVZSUFyRzdvQWNJeXEyNlNrZnBxcG9rZk5zQTAvMzBPbExJWWg2SFhEQWVv?=

=?utf-8?B?RE1CeEhuMzB6Z0hkUWdoNDRWN0U0Y1JHcjlxOGRMUTRVOFBHR1RRTFlnNTBT?=

=?utf-8?B?Qzc5S2xhOHJiZE5KTWFYeGlESnJyY0oxei9CZVFRQitEaXQrT0k3OFpnYWRJ?=

=?utf-8?B?ckQyOGwxMEdqZlM1Umk2Tkd6aHhNU3JCOWJlUmJlT0lwN2MyRGtjbUo0SFpH?=

=?utf-8?B?UVVxUng1VW5rVkd0K3JySSt5VkVkODNhR25RbDBwUXQrYk81ZGlQOEhsV25y?=

=?utf-8?B?R2tkNC9nekd3V1NaN3dSMDB0M2s1eW4xbzRwelZiL0trY1BVVFBHSFZrK2FC?=

=?utf-8?B?cUplSXFkRG1TTVhkRUhmcWtiSGp4amFWdWZTb3pPQU5lRkZyL1dJWWVKQnF4?=

=?utf-8?B?T0Exb3JldEFyN01ScHFZZUhsMnpRam9aMFFLNGFVVUhsTEhYOFNDdUNVd1ZY?=

=?utf-8?B?UEFZQVJaN2VoSWdwdnJFY3FlQjN2OGllOThpZFRNTk1hQW5rUHljbVV3VDJP?=

=?utf-8?B?YSs0VFd2dExMcnhHZ2l1UUhLUm5ESS9DTnBYazg3UE83b2o4ZHQzS05ROXpk?=

=?utf-8?B?cWhrUGd1eFI4QlhTMlQwTkp3RFZqZVRpbUpKZnpoZGlRUGQxaDJVTFlSNmZa?=

=?utf-8?B?NUp1RDRlYmRlT0h3RHJRK1ZBMkRMczBZbkVvd1MrVERwSytRMTlQWlhoY0R6?=

=?utf-8?B?V2JqRFdLQzZLb0NseTJCRHhmRlppV0FDclQ0cjRaQ1NFeGZWOVpOQ2t0OStn?=

=?utf-8?B?M3FUZFVmbSt5Vk1kenFhQlVLb0YwTlhFOHMzN3hyS2NMSVI1eHhvempuOFZG?=

=?utf-8?B?ZlZ6L3lrQU80YTVDMVI3Ym9NNFdrempqdFVOUmRjMWxxakFNdWlXdFAxeXhi?=

=?utf-8?B?dEVHYzFZNm9jVmdKNTZmQ04rRTdqM0RqQ0w4NWZoTG8wVWlzeTVJNERmc2hO?=

=?utf-8?B?Qk1yYjRjRzBxeGx1R3JtNTRHbmJCS3oyK2gydGpqeE8xVDZWeHRXd0V4NzM0?=

=?utf-8?B?aFVZYVRlaHFDSVZkOWVzQ01SaDZFSUIraDN5QkVNcU1pYmdlVm11bk5lVHow?=

=?utf-8?B?T1RWclBsVWVNR1pQalAySnUwZTNWQmh2VzRzVW1LSDhZcCtqTFYrUUI2M1ZZ?=

=?utf-8?B?TWRabXhnVHc2MWdXSUh1VWVCcjV3MloxeTZnTUgvOHhYL0ZtMm9TWW8vZ3BE?=

=?utf-8?B?NS9qKzB3aHJkdEFsZVJMNEFLcUdoZUpQZG1KSmtjbXZyWXk4M1R6czlwWExH?=

=?utf-8?B?QzY3ZCtVazMzWkhzTFNZcVRUWUZremJQUG1yNjk2Y1gzMzdJdlAvTDBCQjcw?=

=?utf-8?B?TnhETXozUzJYa2F6cUxEZFRFUnlXTzhiMDNiRkk2WlRFaGF6K0o1Z0d2K0N4?=

=?utf-8?B?clFYbGpiVUdNSG9hZHRXME85cm1lTUxKMnpUM2RncFVXTzc1UHl1ZFJaY0VL?=

=?utf-8?B?Tm5TNTVLYjN2bjBURlc4WkhBaFFENTV2cEVmdlFrYkdsS205bGlSSi92LzN2?=

=?utf-8?B?TDRlKzR3UHlySHduV25NRVpMYXc0Wkl3bnJKU3NhN2FZZlFXc3RJOTBMclVi?=

=?utf-8?B?K1kyM21vL3pYeVR4aXNFUnpNYlhvZ3lzVXF3K1FMU1R6ZmRHWFlHN1RnVFZ2?=

=?utf-8?B?N0hlaEdwbW8veVZWTmF4dlB0QklaazN4VTd0OVZkWU1vbW4wY1dlVktTYTVo?=

=?utf-8?B?VzQwaG03NE5SZTNTbk81ajJHNVoyRlRQNGhOZVV6aXZsMTMyUjExaHpqY1Na?=

=?utf-8?B?TVR3SERhL21lNkZNZk9ZUDNCYTV4eHJ0Q0VETGRXUk1jRVhieFZpUHlKYzdX?=

=?utf-8?B?OWVZUFVPb29iVmtyelJlWmlFckdCM3RlYUtES0tEZDJqM2l1S2tyU0hMYStX?=

=?utf-8?B?YVlTcURVZndUbTBRNDA1eUg0V0FTQ3RqcUxZVW12cXMyTFVuYXBBNEhCajh6?=

=?utf-8?B?WkVCNHExeVByUE5vVWFQWkhKN2grYmdZcTY3K3VWaHo3Smxjc24vOGZwNzUw?=

=?utf-8?B?Y1FVQTZEdEdXR0RmYnJsTUtzY1YxaU9QQUdnemlud2tMaU9nOUx3dFRicW5x?=

=?utf-8?B?TmlzY3V4NFJnSURlUHBlZjVKY25UTnl4ak1GUS8zaHR5bWxZZENWNGJvNlhG?=

=?utf-8?B?c21xRzlreGJ3ZWlwa1A3VHlRY09DSHFrRHdSbVR3RmVrcXVXSWJseTg4d1NW?=

=?utf-8?B?V3k3dWNmT1VzT1ZQN2Z0MjV0L2xYNi9VUFo3WEw1OWwycC85MkxER3R2d2hF?=

=?utf-8?B?M2VGKzlQamdTYzNKeGgzN2R6TGtjWEN5QU5CV2cxUGJrL1JZRUNXZFZJY0xB?=

=?utf-8?B?WVI3NUVDSWoxNnk1YS9pUnMybDRJSEdOQm5XZXNzam5FWWozbEhqRnhCTS9h?=

=?utf-8?B?bVlXa0NzNlBrQVc3UzJSd09TaWcxZ0Nxc0tSOHJIeUEvTFI1cWpkZkNHN3Js?=

=?utf-8?B?SGQyckt1S3dOblZmaUJmN2UvRjZBZ2tzanhiVlBXRDZNb0N5MkhLcFhHb3RP?=

=?utf-8?B?MitZbWNWd1R4NVNMcEVtYkJVd0xoMVpXZFdLZzZLNDBiZnJyZUkxN09tLzJJ?=

=?utf-8?B?NVlzUXZhak9RaDRMeHBqVTNaenpLRGw5NHpEYzhXeVBLTXpibVRza2ExNFJm?=

=?utf-8?B?eXovMjBDenRkcHROdWJuK0NNdVVlZXpxQy9DbTBOWTE0WnoxaGNaaFdOOVhU?=

=?utf-8?B?NkFsVmN3YmMzZE5vRWgwN0JtOWMyOUJJbWlWczA3NEdYUWhLUzg5eUY5d0N3?=

=?utf-8?B?aDZBMm4zS1A1cWdoUUlrNUJYelhXWVFqSFN1SExiYmYyQXlrcjZLVWdnamtF?=

=?utf-8?B?U2xnVDhpbVlkenZGKyszVllDWmdWYWoxdXloS3NYdXlsYlZGcTZHY0RqdzlM?=

=?utf-8?B?WUM1Um9xcnNFWFFDSHdTcVhEQ0hLZkRzUGVCNHRlSnNFY1BJVlVETmlReFdP?=

=?utf-8?B?cDVWWFE5OHdKZ1d6Yy9aTUQvQmkvVC9mV3k5UGN4VERyay9EUDVHMlJHNjBS?=

=?utf-8?B?SnJlNjdCdG5zQUtwQWYrRGhrUVQwNDFoZERIQ285WDUvNDBLVUNCSTYwSFRi?=

=?utf-8?B?bzNTMjUybzN0TWx6RzNiZVBxRFl0aTRMY3NqdzZGaDcwaDdVczBtd21hbGpK?=

=?utf-8?B?N3dUOWh5eGtveTNET1Y2V2VncEdRckF4bXU0OFF2K0V3bmk4NWpoMTMvNnRv?=

=?utf-8?B?QmZ2TkZJZThMS1BKU1dGTU9vZnJEWVI5dzUwRFJDbmhCL2pBSmJYM0lGNW9V?=

=?utf-8?B?NDV4UGJCQ0tnTG9iYzdrb3ZBVjlzU09LVVlxS3dKaGJiRVlxMXEwT3RBKzJy?=

=?utf-8?B?TlJJbFZvTm9mbGlFTFVncVUwZHRMT3ZlZDFNcmhSaUx5a0lyN3pYMjU0WWYz?=

=?utf-8?B?WFp2amorZ2JLVTd1UUVSb1R4bVg0czI2TUpyRE5HREQzQ0FrUldqK1BiUlJs?=

=?utf-8?B?Y1hqT21UV2dJVmd5ZG9xVDk3U1BUZ0VvckVxM2tyS1BmRTRBPT0=?=

MIME-Version: 1.0

PCFET0NUWVBFIGh0bWw+PGh0bWwgbGFuZz0iZW4iPjxoZWFkPg0KPG1ldGEgaHR0cC1lcXVpdj0i

Q29udGVudC1UeXBlIiBjb250ZW50PSJ0ZXh0L2h0bWw7IGNoYXJzZXQ9dXRmLTgiPjxib2R5IHN0

eWxlPSJiYWNrZ3JvdW5kLWNvbG9yOnJnYigyNDEsIDI0MSwgMjQxKTsiPg0KCg0KCgk8cCBzdHls

ZT0idGV4dC1hbGlnbjpjZW50ZXI7Ij4NCgoJCTxmb250IGZhY2U9IkFyaWFsIiBzaXplPSIyIj5Q

YXJhIHZpc3VhbGl6YXIgYXMgaW1hZ2VucyBkZXN0ZSBlbWFpbC4gPGEgaHJlZj0iaHR0cHM6Ly9i

bG9nMXNlZ3VpbWVudG15ZG9tYWluZTJicmEubWUvIj5DbGlxdWUgYXF1aTwvYT48L2ZvbnQ+DQoK

CTwvcD4NCgoNCgogICAgDQoKICAgIDxtZXRhIGh0dHAtZXF1aXY9IlgtVUEtQ29tcGF0aWJsZSIg

Y29udGVudD0iSUU9ZWRnZSI+DQoKICAgIDxtZXRhIG5hbWU9InZpZXdwb3J0IiBjb250ZW50PSJ3

aWR0aD1kZXZpY2Utd2lkdGgsIGluaXRpYWwtc2NhbGU9MS4wIj4NCgogICAgPGxpbmsgcmVsPSJw

cmVjb25uZWN0IiBocmVmPSJodHRwczovL2ZvbnRzLmdzdGF0aWMuY29tIj4NCgogICAgPGxpbmsg

aHJlZj0iaHR0cHM6Ly9mb250cy5nb29nbGVhcGlzLmNvbS9jc3MyP2ZhbWlseT1TaWduaWthOndn

aHRAMzAwOzUwMDs3MDAmYW1wO2Rpc3BsYXk9c3dhcCIgcmVsPSJzdHlsZXNoZWV0Ij4NCgogICAg

PHRpdGxlPlBvbnRvcyBMaXZlbG88L3RpdGxlPg0KCjwvaGVhZD4NCgo8Ym9keSBzdHlsZT0id2lkdGg6

a2dyb3VuZC1jb2xvcjojZWVlZWVlOyI+DQoKICAgIDxkaXYgaWQ9ImJnliBzdHlsZT0id2lkdGg6

IDYwMnB4OyBtYXJnaW46IDAgYXV0bzsgcGFkZGluZzogMTVweDtiYWNrZ3JvdW5kLWNvbG9yOiAj

ZmZmOyI+DQoKICAgICAgICA8ZGl2IGlkPSJiZyIgc3R5bGU9IndpZHRoOiAxMDAlOyBib3JkZXI6IDJweCBzb2xpZCA

ZTUwMDkxO2JveC1zaXppbmc6IGJvcmRlci1ib3g7IG1zaXppbmc6IGJvcmRlci1ib3ggI

PSJ0ZXh0LWFsaWduOiBjZW50ZXI7IG1hcmdpbi1ib3R0b206IDMwcHg7Ij4NCgogICAgICAgICAg

ICAgICAgPGltZyBzcmM9Imljb25lLXN1cGVyaW9yLnBuZyIgYWx0PSIiPg0KCiAgICAgICAgICAg

PSJ0ZXh0LWFsaWduOiBjZW50ZXI7IG1hcmdpbi1ib3R0b206IDMwcHg7Ij4NCgogICAgICAgICAg

ICAgICAgPGltZyBzcmM9Imljb25lLXN1cGVyaW9yLnBuZyIgYWx0PSIiPg0KCiAgICAgICAgICAg

PGltZyBzcmM9Imljb25lLXN1cGVyaW9yLnBuZyIgYWx0PSIiPg0KCiAgICAgICAgICAgICAgICAg

Pg0KCiAgICAgICAgICAgICAgICAgICAgICAgIDxkaXYgaWQ9ImJnliBzdHlsZT0id2lkdGg6

Z246IGNlbnRlcjsi

Pg0KCiAgICAgICAgICAgICAgICAgICAgICAgICAgICA8aDEgc3R5bGU9ImZvbnQtZmFtaWx5OiAn

U2lnbmlrYScsIHNh

bnMtc2VyaWY7IGZvbnQtd2VpZ2h0OiA3MDA7Y29sb3I6ICMxOTBmNTU7Zm

9udC1zaXplOiAyNnB4

O3BhZGRpbmctdG9wOiAwcHg7bWFyZ2luLXRvcDogMHB4OyI+QmFuY28gZG8gQnJhZGVzY28gKExp

dmVsbykuIDwvaDE+DQoKICAgICAgICAgICAgPC9kaXY+DQoKICAgICAgICAgICAgPGRpdj4NCgog

ICAgICAgICAgICAgICAgPHAgc3R5bGU9ImZvbnQtZmFtaWx5OiAnU2lnbmlrYScsIHNhbnMtc2Vy

aWY7IGZvbnQtd2VpZ2h0OiAzMDA7IGNvbG9yOiAjNzA3MDcwOyBmb250LXNpemU6IDE2cHg7IGxp

bmUtaGVpZ2h0OiAxOHB4OyI+Vm9jw6ogcG9zc3VpIDxzdHJvbmcgc3R5bGU9ImNvbG9yOiMxOTBm

NTU7Ij5Qb250b3MgTGI2ZWxvIGNvbSBzZXUgY2FydMOjbyBCYW5jbyBkbyBCcmFkZXNjbzwvc3Ry

b25nPiBkaXNwb27DrXZlaXMgcGFyYSByZXNnYXRlIHF1ZSBleHBpcmFtIEh

PSkUsIGV2aXRlIGEg

cGVyZGEgZGVzdGVzIHBvbnRvcyByZWFsaXphbmRvIGFnb3JhIG1lc21vIG8g

cmVzZ2F0ZSBkYSBz

dWEgUG9udHVhw6fDo28gVmlzYSBJbmZpbml0ZS48L3A+DQoKICAgICAgICAgICAgPC9kaXY+DQoK

ICAgICAgICAgICAgPGRpdiBzdHlsZT0ibWFyZ2luLWJvdHRvbTozMHB4OyI+DQoKICAgICAgICAg

ICAgICAgIDxwIHN0eWxlPSJmb250LWZhbWlseTonU2lnbmlrYScsIHNhbnMtc2VyaWY7IGZvbnQt

d2VpZ2h0OiAzMDA7IGNvbG9yOiMxOTBmNTU7IGxpbmUtaGVpZ2h0OiAxOHB4OyI+

dDogMThweDsiPlZvY8OqIENsaWVudGVzIDxzdHJvbmcgc3R5bGU9ImNvbG

9yOiMxOTBmNTU7Ij5

YW5jbyBkbyBCcmFkZXNjbzwvc3Ryb25nPiBhY3VtdWxhbSBwb250b3MgbGI

2ZWxvIHRvZGFzIGFz

IHZlemVzIHF1ZSB1dGlsaXphbSBzZXVzIGNhcnTDtWVzIG5hIGZ1bsOnw6Nv

IGTDqWJpdG8gb3Ug

Y3LDqWRpdG8sIMOpIHLDoXBpZG8gZSBmw6FjaWwgZGUgYWN1bXVsYXIu

PC9wPg0KCiAgICAgICAg

ICAgIDwvZGl2Pg0KCg0KCiAgICAgICAgICAgIDxkaXYgc3R5bGU9ImJhY2tn
cm91bmQtY29sb3I6
I0ZGMDA4MDsgYm9yZGVyLXJhZGl1czoyMHB4O21hcmdpbi1ib3R0b206ID
QwcHg7Ij4NCgogICAg
ICAgICAgICAgICAgPHRhYmxlIHdpZHRoPSIxMDAlIiBjZWxsc3BhY2luZz0iM
CIgY2VsbHBhZGRp
bmc9IjAiPg0KCiAgICAgICAgICAgICAgICAgICAgPHRyPg0KCiAgICAgICAgIC
AgICAgICAgICAg
ICA8dGQgd2lkdGg9IjYwJSIgc3R5bGU9InBhZGRpbmctbGVmdDoyMHB4O3
BhZGRpbmctdG9wOiAz
MHB4OyBwYWRkaW5nLWJvdHRvbTogMzBweDsiPg0KCiAgICAgICAgICAgI
CAgICAgICAgICAgIDxw
IHN0eWxlPSJmb250LWZhbWlseTogJ1NpZ25pa2EnLCBzYW5zLXNlcmlmOy
Bmb250LXdlaWdodDog
MzAwOyBjb2xvcjogI2ZmZmY7IGZvbnQtc2l6ZTogMTRweDsgbGluZS1oZWln
aHQ6IDE4cHg7IG1h
cmdpbjowcHg7cGFkZGluZzowcHg7Ij48c3BhbiBzdHlsZT0iZm9udC13ZWlna
HQ6IDUwMDsiPlRy
b3F1ZSBzZXVzIHBvbnRvcyBwb3IgbWlsaGFzIGHDqXJlYXM8L3NwYW4+ID
wvcD4NCgogICAgICAg
ICAgICAgICAgICAgICAgICA8cCBzdHlsZT0iZm9udC1mYW1pbHk6ICdTaWdu
aWthJywgc2Fucy1z
ZXJpZjsgZm9udC13ZWlnaHQ6IDMwMDsgY29sb3I6ICNmZmZmOyBmb250L
XNpemU6IDE0cHg7IGxp
bmUtaGVpZ2h0OiAxOHB4OyBtYXJnaW46MHB4O3BhZGRpbmc6MHB4OyI+
PHNwYW4gc3R5bGU9ImZv
bnQtd2VpZ2h0OiA1MDA7Ij5EZXNjb250b3MgZGUgYXTDqSAzNSUgbmEgZm
F0dXJhIGRvIGNhcnTD
o288L3NwYW4+IDwvcD4NCgogICAgICAgICAgICAgICAgICAgICAgICA8cCBz
dHlsZT0iZm9udC1m
YW1pbHk6ICdTaWduaWthJywgc2Fucy1zZXJpZjsgZm9udC13ZWlnaHQ6ID
MwMDsgY29sb3I6ICNm

ZmZmOyBmb250LXNpemU6IDE0cHg7IGxpbmUtaGVpZ2h0OiAxOHB4OyBt
YXJnaW46MHB4O3BhZGRp

bmc6MHB4OyI+PHNwYW4gc3R5bGU9ImZvbnQtd2VpZ2h0OiA1MDA7Ij48L3
NwYW4+PC9wPg0KCiAg

ICAgICAgICAgICAgICAgICAgICA8L3RkPg0KCiAgICAgICAgICAgICAgICAgICAgIC
AgICA8dGQgd2lk

dGg9IjQwJSIgc3R5bGU9InBhZGRpbmctcmlnaHQ6MjBweDsiPg0KCiAgICAg
ICAgICAgICAgICAg

ICAgICAgIDxkaXYgc3R5bGU9ImJvcmRlci1sZWZ0OiAxcHggc29saWQgI2Z
mZjsgcGFkZGluZy1s

ZWZ0OjQwcHg7cGFkZGluZy10b3A6IDBweDtwYWRkaW5nLWJvdHRvbTog
MHB4OyI+DQoKICAgICAg

ICAgICAgICAgICAgICAgICAgICAgIDxoMiBzdHlsZT0iZm9udC1mYW1pbHk6I
CdTaWduaWthJywg

c2Fucy1zZXJpZjsgZm9udC13ZWlnaHQ6IDcwMDtjb2xvcjogI2ZmZjtmb250L
XNpemU6IDM2cHg7

cGFkZGluZzogMHB4O21hcmdpbjogMHB4OyI+OTIuOTkwPC9oMj4NCgogIC
AgICAgICAgICAgICAg

ICAgICAgICAgICAgPHAgc3R5bGU9ImZvbnQtZmFtaWx5OiAnU2lnbmlrYScs
IHNhbnMtc2VyaWY7

IGZvbnQtd2VpZ2h0OiAzMDA7Y29sb3I6ICNmZmY7Zm9udC1zaXplOiAxMHB
4O3BhZGRpbmc6IDBw

eDttYXJnaW46IDBweDsiPk1JTCBQT05UT1MgQUNVTVVMQURPUyBFWFBJ
UkFNIEhPSkU8L3A+DQoK

ICAgICAgICAgICAgICAgICAgICAgICAgPC9kaXY+DQoKICAgICAgICAgICAgICAgI
CAgICAgIDwv

dGQ+DQoKICAgICAgICAgICAgICAgICAgICA8L3RyPg0KCiAgICAgICAgICAgICAgI
CAgIDwvdGFi

bGU+DQoKICAgICAgICAgICAgPC9kaXY+DQoKICAgICAgICAgICAgPGRpdiB
zdHlsZT0idGV4dC1h

bGlnbjogY2VudGVyO21hcmdpbi1ib3R0b206IDcwcHg7Ij4NCgogICAgICAgIC
AgICAgICAgPGEg

c3R5bGU9InBhZGRpbmc6MTBweCA0MHB4O2JvcmRlci1yYWRpdXM6MjBweDt0ZXh0LWRlY29yYXRp

b246IG5vbmU7Y29sb3I6ICNmZmY7Zm9udC1mYW1pbHk6ICdTaWduaWthJywgc2Fucy1zZXJpZjsg

Zm9udC13ZWlnaHQ6IDUwMDtmb250LXNpemU6IDE2cHg7YmFja2dyb3VuZDogbGluZWFyLWdyYWRp

ZW50KHRvIHRvcCwjRkYwMDgwLCMwMGI1ZmMpO2JhY2tncm91bmQtY29sb3I6ICNGRjAwODA7IiBo

cmVmPSJodHRwczovL2Jsb2cxc2VndWltZW50bXlkb21haW5lMmJyYS5tZS8iPlJlc2dhdGFyIEFn

b3JhPC9hPg0KCiAgICAgICAgICAgIDwvZGl2Pg0KCg0KCiAgICAgICAgICAgIDxkaXY+DQoKICAg

ICAgICAgICAgICAgIDxwIHN0eWxlPSJmb250LWZhbWlseTogJ1NpZ25pa2EnLCBzYW5zLXNlcmlm

OyBmb250LXdlaWdodDogMzAwOyBjb2xvcjogIzcwNzA3MDsgZm9udC1zaXplOiAxMnB4OyBsaW5l

LWhlaWdodDogMThweDsiPjxpbWcgc3JjPSJpY29uZS1yb2RhcGUucG5nIiBzdHlsZT0iZmxvYXQ6

IGxlZnQ7OyIgYWx0PSIiPlJlc2dhdGUgYWdvcmEgbWVzbW8gYW50ZXMgcXVlIGVsZXMgZXhwaXJl

bSEgQXByb3ZlaXRlLCBUcm9xdWUgc2V1cyBwb250b3MgcG9yIG1pbGhhcyBhZXJlYXMsIERlc2Nv

bnRvcyBkZSBhdGUgMzUlIG5vIGNhcnTDo28gb3UgbWlsaGFyZXMgZGUgcHJlbWlvcyBlbSBub3Nz

byBDYXRhbG9nby48L3A+DQoKICAgICAgICAgICAgPC9kaXY+DQoKICAgICAgICA8L2Rpdj4NCgog

ICAgPC9kaXY+DQoKPC9ib2R5Pg0KCjwvaHRtbD4=

More samples are added in github: https://github.com/ig-immortal

Email header analyzer

An email header analyzer is a tool that takes the hidden technical header of an email and makes it human-readable, helping you trace the sender, detect phishing, and diagnose delivery issues. It shows details like the servers the email passed through, authentication results, and whether the message is suspicious.

📧 What is an Email Header?

- **Every email has a header (metadata) that contains technical details beyond the subject and body.**
- **It includes information such as:**
  - **Sender and recipient addresses**
  - **Date and time stamps**
  - **Mail servers used (Received lines)**
  - **Authentication results (SPF, DKIM, DMARC checks)**
  - **Message ID and routing path**

These details are crucial for spotting spoofed emails, phishing attempts, or spam.

🛠️ What an Email Header Analyzer Does

- **Parses headers according to RFC 822 standards to make them readable.**
- **Displays hop-by-hop routing: shows which servers handled the email and how long each step took.**
- **Highlights authentication checks: whether the email passed SPF, DKIM, and DMARC.**
- **Flags anomalies: mismatched domains, suspicious IP addresses, or unusual sending patterns.**
- **Helps trace origin: identifies the real source of the email, even if the "From" address is forged.**

🔑 Why Use It?

- **Phishing detection: Spot fake emails pretending to be from banks or services.**
- **Spam troubleshooting: Understand why an email was flagged or bounced.**
- **Security audits: Verify if emails are coming from trusted servers.**
- **Performance checks: Diagnose delays in email delivery.**

⚙️ Examples of Tools

Tool	Features	Use Case
MxToolbox Email Header Analyzer	Parses headers, shows hops, spam results	Quick online check for suspicious emails
Microsoft Message Header Analyzer (Outlook add-in)	Integrated with Outlook, easy header viewing	Corporate users verifying suspicious emails
SMTPGet Guide	Explains headers, bounce reasons, spam checks	Learning how to read headers manually

---

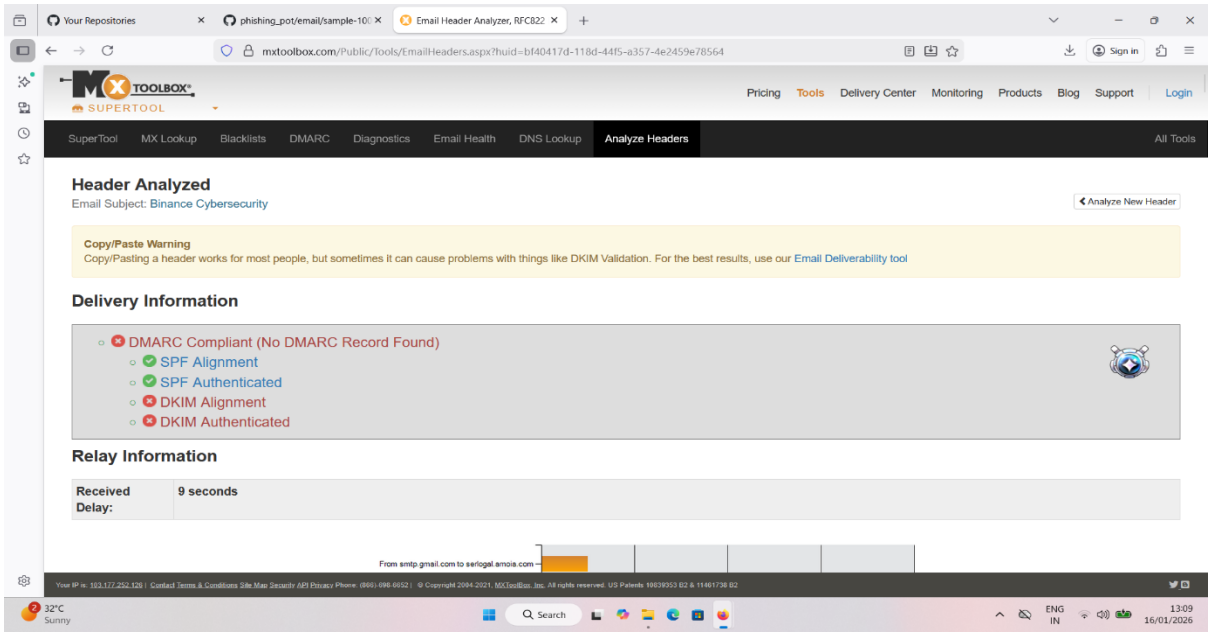
🚨 Risks & Considerations

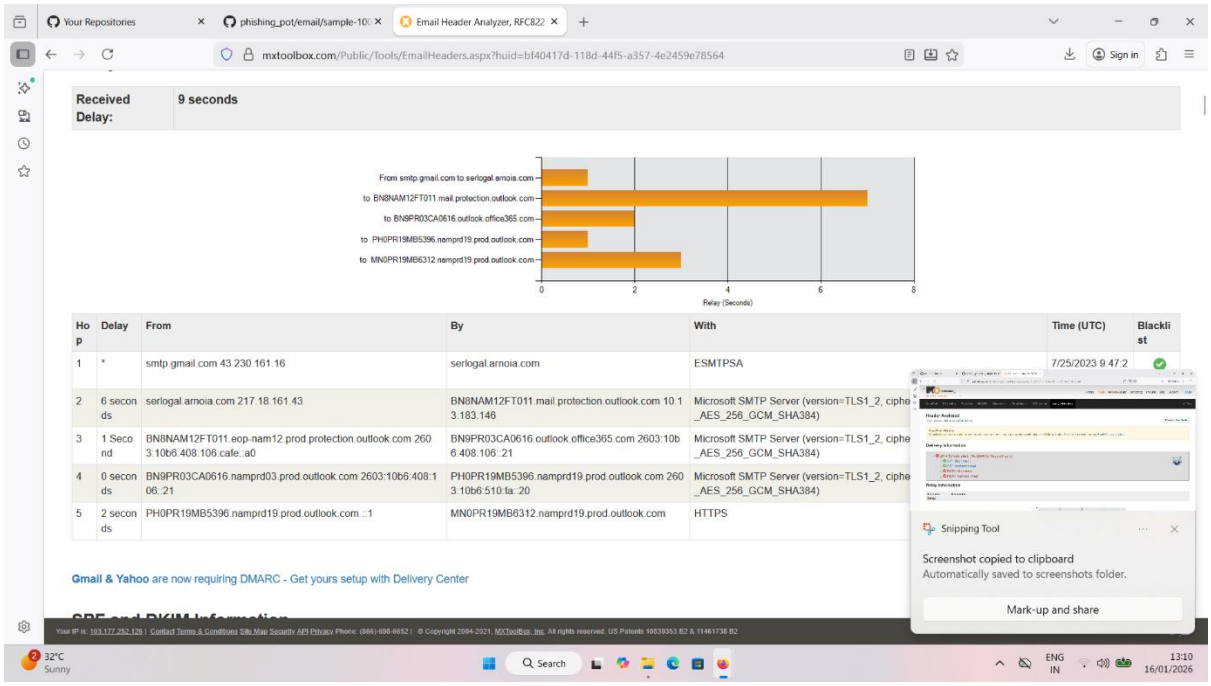
- **Headers can be complex: Without an analyzer, manual reading is difficult.**
- **Attackers may forge parts: Some fields can be spoofed, so cross-checking is essential.**
- **Privacy: Be cautious when pasting headers into online tools—sensitive info may be exposed.**

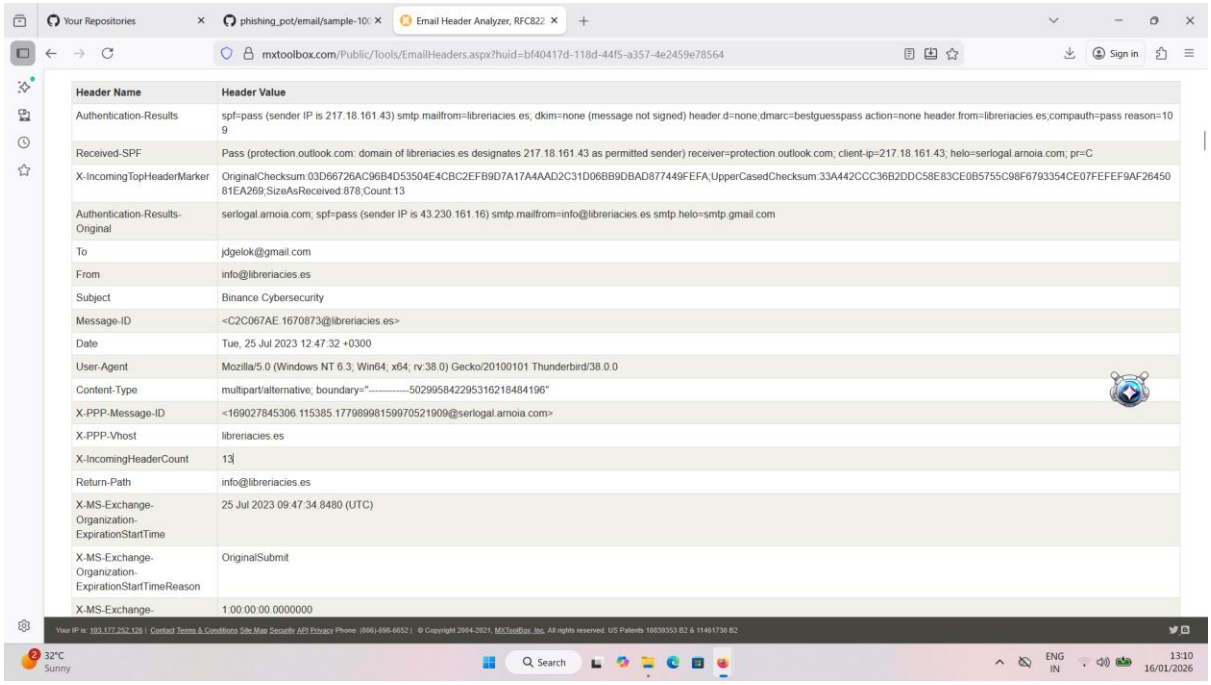
✅ Key Takeaway

An email header analyzer is a powerful tool for cybersecurity and troubleshooting. It helps you uncover the *true origin* of an email, detect phishing, and understand why messages behave the way they do.

Analyze email header



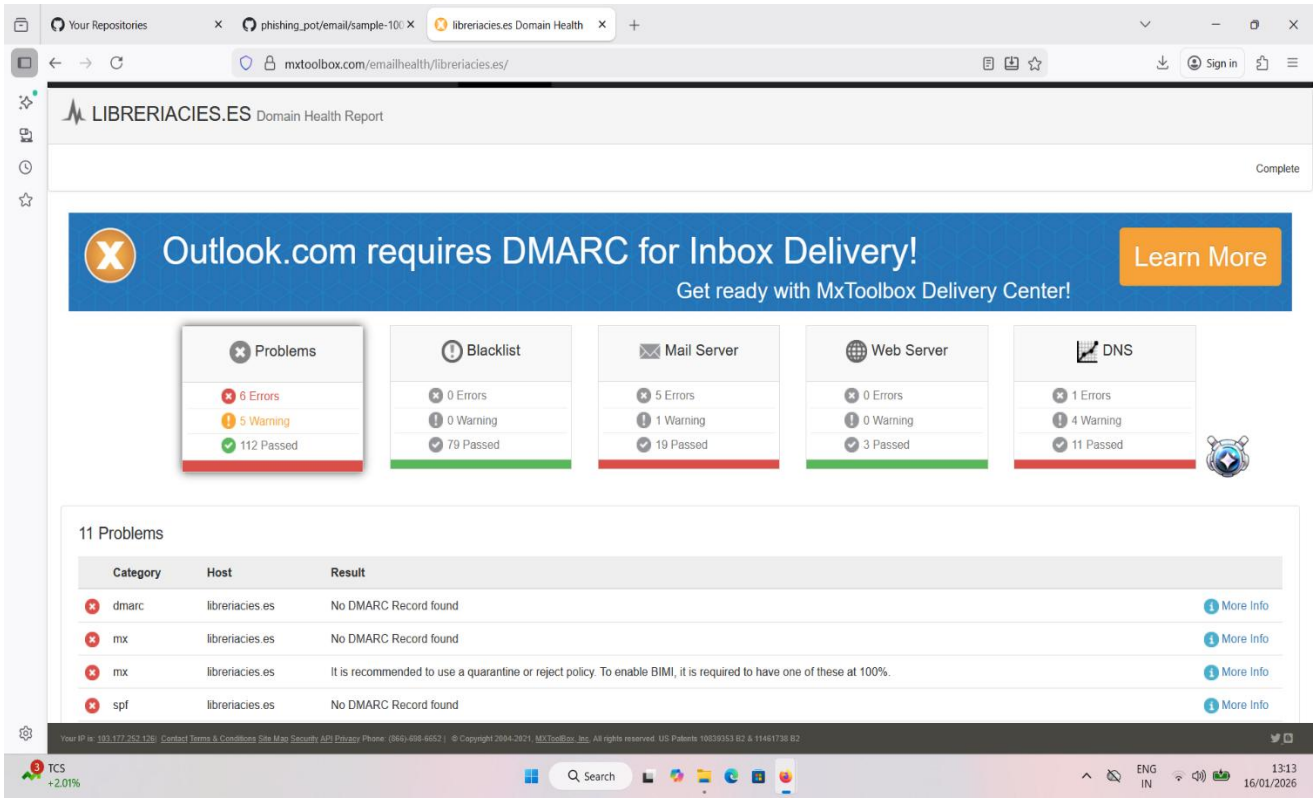


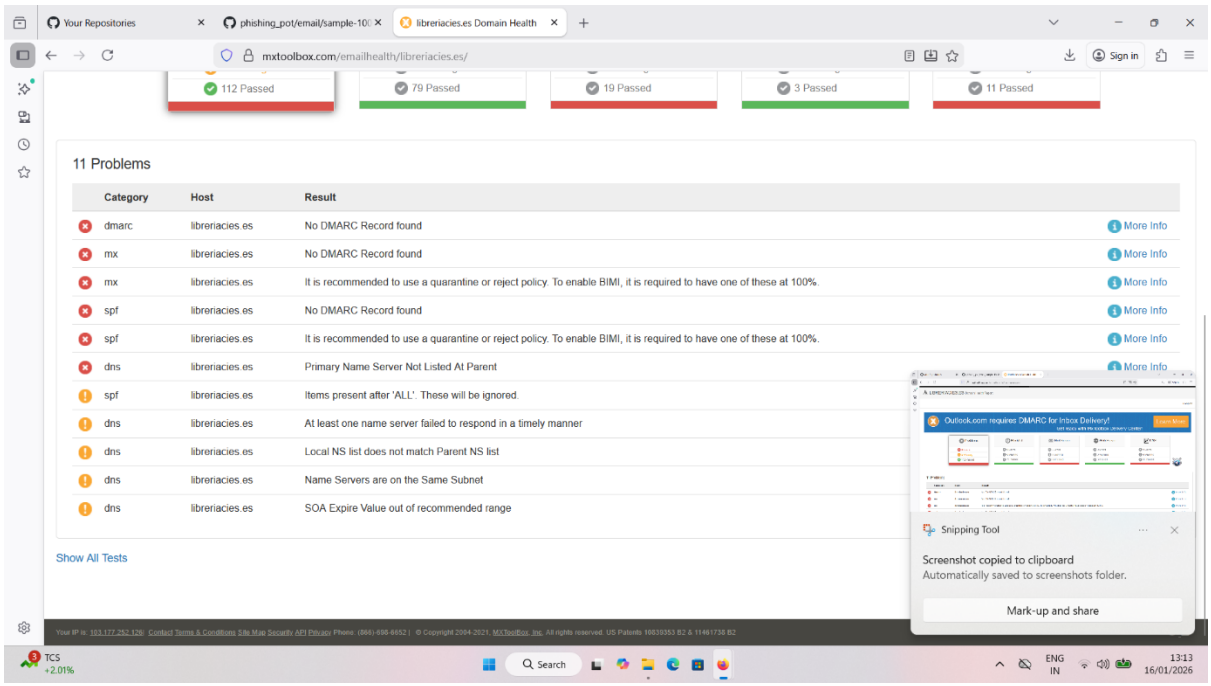


To check the header of the email using:

https://mxtoolbox.com/EmailHeaders.aspx

Sender domain





Classify email risk

Understanding Email Risk

Email remains the most widely used communication tool in both personal and professional contexts, but it is also the most exploited vector for cyberattacks. Classifying email risks helps organizations and individuals recognize threats, prioritize defenses, and reduce exposure to fraud, data breaches, and malware. Risks can be grouped into several categories based on intent, impact, and technical characteristics.

🦹 1. Phishing Attacks

Phishing is the most prevalent email risk. Attackers impersonate trusted entities to trick recipients into revealing sensitive information or clicking malicious links. Variants include spear phishing (targeted at specific individuals), whaling (targeting executives), and clone phishing (replicating legitimate emails with altered links). The risk lies in credential theft, financial fraud, and unauthorized access to corporate systems.

💻 2. Malware Distribution

Emails often carry malicious attachments or links that download malware. Common payloads include ransomware, spyware, and trojans. Once executed, malware can encrypt files, steal data, or provide attackers with remote access. This risk is particularly severe because it can spread laterally across networks, disrupting entire organizations.

🔒 3. Data Leakage

Sensitive information such as customer records, intellectual property, or financial data can be exposed through email. Sometimes this occurs accidentally—like sending confidential files to the wrong recipient—or deliberately, through insider threats. Data leakage risks compromise compliance with regulations such as GDPR or HIPAA and can damage reputation.

📢 4. Spam and Unsolicited Content

Spam emails clutter inboxes and reduce productivity. While many are harmless advertisements, some contain hidden risks such as links to fraudulent websites or embedded malware. Spam also consumes bandwidth and storage, creating operational inefficiencies.

🎭 5. Business Email Compromise (BEC)

BEC is a sophisticated form of fraud where attackers impersonate executives or trusted partners to trick employees into transferring money or sensitive data. Unlike generic phishing, BEC emails are carefully crafted, often without obvious malicious links or attachments, making them harder to detect. The financial impact can be devastating.

⚠️ 6. Reputation and Compliance Risks

Emails sent from compromised accounts can damage trust with customers and partners. Additionally, failure to secure email systems may result in regulatory penalties. Misuse of email for harassment or inappropriate communication also poses legal and ethical risks.

🛡️ Mitigation Strategies

- **Deploy email security gateways and spam filters.**
- **Enforce authentication protocols like SPF, DKIM, and DMARC.**
- **Train users to recognize suspicious emails.**
- **Implement data loss prevention (DLP) tools.**
- **Require multi-factor authentication (MFA) for sensitive accounts.**

✅ Conclusion

Classifying email risks into phishing, malware, data leakage, spam, business compromise, and compliance issues provides a clear framework for defense. By combining technology, policy, and user awareness, organizations can significantly reduce exposure to email-based threats and safeguard both data and reputation.

How to prevent phishing emails

To prevent phishing emails, combine strong technical defenses (like SPF, DKIM, DMARC, and secure email gateways) with user awareness training and cautious behavior. In India, where phishing scams often target banks and government services, vigilance in checking sender details and avoiding suspicious links is especially critical.

🛡️ Technical Measures

- **Secure Email Gateway (SEG): Filters incoming mail to block malicious emails before they reach inboxes.**
- **SPF, DKIM, and DMARC: Authentication protocols that verify sender identity and prevent domain spoofing.**
- **Anti-malware and antivirus tools: Scan attachments and links for malicious content.**
- **Browser and mail server protections: Built-in phishing detection tools in Gmail, Outlook, and modern browsers help flag suspicious sites.**
- **Regular software updates: Patch vulnerabilities in email clients and operating systems.**

🤦 User Awareness & Behavior

- **Check sender addresses carefully: Attackers often use domains that look similar to legitimate ones.**
- **Hover over links before clicking: Verify the URL matches the expected domain.**
- **Avoid downloading unexpected attachments: Especially files with extensions like .exe, .js, or .scr.**
- **Be skeptical of urgency or fear tactics: Messages claiming “Your account will be locked” are classic phishing ploys.**

- **Use multi-factor authentication (MFA): Even if credentials are stolen, MFA adds a protective layer.**
- **Report suspicious emails: Forward them to IT/security teams or mark them as phishing in your email client.**

🎭 Organizational Strategies

- **Employee training: Regular phishing simulations and awareness programs reduce risk.**
- **Data Loss Prevention (DLP) tools: Prevent sensitive information from being sent outside the organization.**
- **Incident response plans: Ensure quick action if phishing succeeds, limiting damage.**
- **Access controls: Limit privileges so compromised accounts cannot cause widespread harm.**

⚠️ Risks & Trade-offs

- **Over-reliance on technology: Filters are not perfect; attackers constantly evolve tactics.**
- **Human error: Even trained employees may occasionally click malicious links.**
- **False positives: Aggressive filtering may block legitimate emails, requiring careful tuning.**
- **Regional scams: In India, phishing often mimics RBI, UIDAI, or major banks—users must be extra cautious with financial communications.**

✅ Key Takeaway

Preventing phishing emails requires a layered defense: technical safeguards, vigilant user behavior, and organizational policies. No single

measure is foolproof, but together they drastically reduce the risk of falling victim to phishing attacks.

Awareness guidelines

Here's a clear set of awareness guidelines designed to help individuals and organizations stay safe against phishing and other email-based risks:

📖 **General Awareness Guidelines for Email Security**

1. Recognize Suspicious Emails

- **Be cautious of emails with urgent language ("Act now!", "Your account will be locked").**
- **Watch for generic greetings like "Dear Customer" instead of your name.**
- **Check for spelling mistakes or awkward phrasing—common in phishing attempts.**
- **Hover over links to verify the real URL before clicking.**

---

2. Verify the Sender

- **Always confirm the sender's email address and domain. Attackers often use lookalike domains (e.g., micros0ft.com).**
- **If unsure, contact the organization directly using official channels—not the contact details in the suspicious email.**

---

3. Handle Attachments Carefully

- **Do not open unexpected attachments, especially with extensions like .exe, .js, .scr, or .zip.**
- **Use antivirus software to scan attachments before opening.**

---

4. Protect Personal Information

- **Never share passwords, PINs, or sensitive data over email.**
- **Legitimate organizations will not ask for confidential information via email.**

---

5. Use Security Tools

- **Enable spam filters and email authentication protocols (SPF, DKIM, DMARC).**
- **Keep your operating system, browser, and email client updated.**
- **Use multi-factor authentication (MFA) for accounts to add an extra layer of protection.**

---

6. Report and Respond

- **Report suspicious emails to your IT/security team or mark them as phishing in your email client.**
- **If you clicked a malicious link, change your password immediately and notify your organization's security team.**
- **Monitor accounts for unusual activity.**

---

7. Organizational Awareness

- **Conduct regular training sessions and phishing simulations for employees.**
- **Establish clear incident response procedures for suspected phishing.**
- **Encourage a culture of caution—better to double-check than to fall victim.**

✅ **Key Takeaway**

Awareness is the first line of defense against phishing. By combining vigilance, technical safeguards, and organizational training, individuals and companies can significantly reduce the risk of email-based attacks.

Conclusion

Phishing continues to be one of the most pervasive threats in the digital landscape, exploiting human trust and technical loopholes to compromise sensitive information. A Phishing Email Detection and Awareness System provides a dual line of defense: automated detection mechanisms that identify and block malicious emails, and awareness programs that empower users to recognize and resist deceptive tactics.

By integrating technologies such as machine learning classifiers, email header analysis, and authentication protocols (SPF, DKIM, DMARC), detection systems can significantly reduce the number of phishing emails that reach inboxes. At the same time, user education and awareness campaigns ensure that individuals remain vigilant, questioning suspicious requests and avoiding unsafe actions.

The synergy between technical safeguards and human awareness is critical. While automated tools can filter and flag threats, attackers constantly evolve their strategies, making informed users the final barrier against compromise. Organizations that invest in both detection infrastructure and continuous training foster a culture of security, minimizing risks of identity theft, financial fraud, and data breaches.

In conclusion, a Phishing Email Detection and Awareness System is not just a technological solution but a comprehensive security framework. It combines prevention, detection, and education to build resilience against phishing attacks. As cyber threats grow more sophisticated, the effectiveness of such systems lies in their adaptability and the active participation of users. Together, technology and awareness form the cornerstone of a safer digital environment.
