Phishing Detection and Awareness Report Cyber Security Task 2 (2026) Future Interns

SAMPLE NO : 1

Introduction

Phishing attacks are a common type of online fraud where attackers send fake emails to confuse or scare users into taking harmful actions. These emails often pretend to come from trusted companies such as banks, social media platforms, or online services so that users believe they are real. The main goal is to make people click on fake links, download unsafe files, or share personal information like passwords, OTPs, or financial details. The purpose of this report is to explain a phishing email example in simple and easy language, show how the attack works, and provide clear prevention tips so that even non-technical users can understand and stay safe.

Email Sample Details (Analyzed Mail)

Subject: Liberação de IRPF - 6NwlyfzWcsNerv0

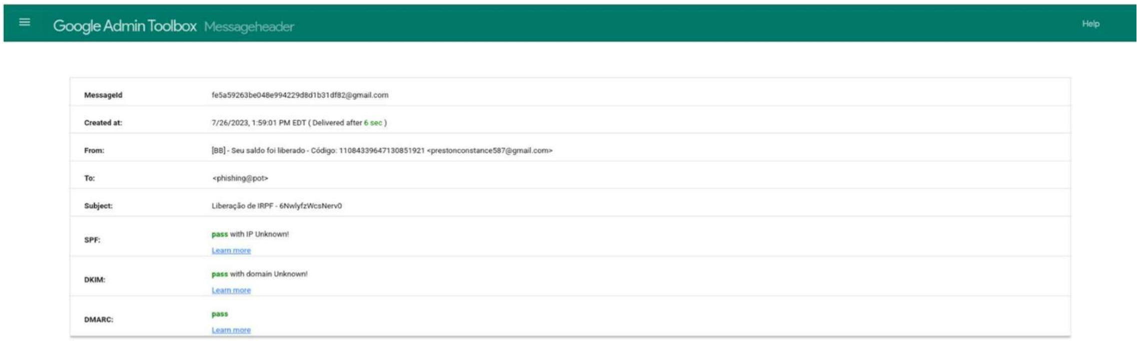
From: [BB] - Seu saldo foi liberado - Código: 11084339647130851921 prestonconstance587@gmail.com

Return Path: prestonconstance587@gmail.com

Sender IP: 209.85.160.178

Mail Server: smtp.gmail.com
SPF: Pass
DKIM: Pass
DMARC: Pass (policy = none)

Figure 1: Email Header Analysis using Google Admin Toolbox Messageheader.



MessageId	fe5a59263be048e994229d8d1b31df82@gmail.com
Created at:	7/26/2023, 1:59:01 PM EDT (Delivered after 6 sec)
From:	[BB] - Seu saldo foi liberado - Código: 11084339647130851921 <prestonconstance587@gmail.com>
To:	<phishing@pot>
Subject:	Liberação de IRPF - 6NwlyfzWcsNerv0
SPF:	**pass** with IP Unknown! Learn more
DKIM:	**pass** with domain Unknown! Learn more
DMARC:	**pass** Learn more

Phishing Indicators Identified

Suspicious Sender Domain:

The email was sent from a Gmail account even though the message appears to be related to financial or official communication. Legitimate organizations usually use official domain email addresses.

Suspicious Subject Line:

The subject contains a random alphanumeric code (6NwlyfzWcsNerv0), which is commonly used in phishing emails.

Possible Impersonation:

The sender name suggests a financial institution notification, which may indicate impersonation.

Weak DMARC Policy:

DMARC policy is set to “none,” meaning strict protection is not enforced.

Generic Structure:

Use of a free email provider instead of a verified corporate domain.

Email Header Analysis

Authentication Results:

SPF PASS — Email was sent from an authorized Gmail server.
DKIM PASS — Digital signature verified successfully.
DMARC PASS — However, policy enforcement is weak.

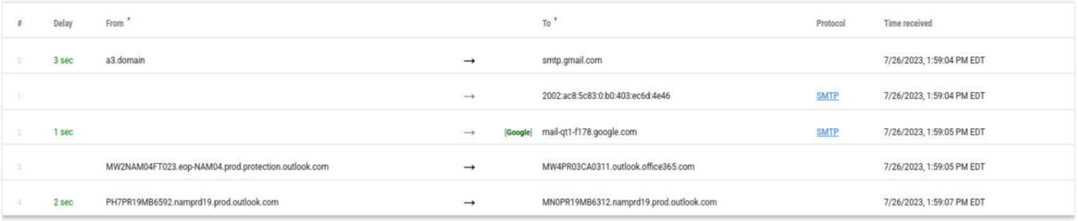
Important Note:

SPF and DKIM passing does not mean the email is safe. Attackers can use legitimate email services to send phishing emails.

Routing Analysis:

Email passed through Gmail servers and Outlook protection infrastructure. The IP address is not blacklisted, but phishing emails often use trusted infrastructure to bypass detection.

Figure 2: Email routing path showing mail server transitions.



#	Delay	From *			To *	Protocol	Time received
0	3 sec	a3.domain	→		smtp.gmail.com		7/26/2023, 1:59:04 PM EDT
1			→		2002:ac8:5c83:0:b0:403:ec6d:4e46	SMTP	7/26/2023, 1:59:04 PM EDT
2	1 sec		→	[Google]	mail-qt1-f178.google.com	SMTP	7/26/2023, 1:59:05 PM EDT
3		MW2NAM04FT023.eop-NAM04.prod.protection.outlook.com	→		MW4PR03CA0311.outlook.office365.com		7/26/2023, 1:59:05 PM EDT
4	2 sec	PH7PR19MB6592.namprd19.prod.outlook.com	→		MN0PR19MB6312.namprd19.prod.outlook.com		7/26/2023, 1:59:07 PM EDT

Link and Attachment Analysis

No direct malicious URL is visible in the header data.
Any malicious link or attachment would likely be present in the email body, not the headers.

Risk Classification

Risk Level: PHISHING (HIGH RISK)

Reasons:
Financial-themed message
Use of free email provider
Suspicious subject format
Potential impersonation attempt

How the Attack Works (Simple Explanation)

The attacker sends a fake email that looks like an important financial notification to make it appear real and trustworthy. The main aim is to create a sense of urgency so the user reacts quickly without thinking carefully. The email usually encourages the user to click on a link or download a file. When the user clicks the link, it may open a fake website that looks genuine but is actually created to steal login details or personal information.

Prevention Guidelines

Always double-check any financial email that you were not expecting before trusting it. Instead of clicking links directly from emails, open your browser and go to the official website yourself. Look carefully at the sender's email address to make sure it is genuine and not fake or misspelled. Avoid opening attachments if the email looks suspicious or comes from an unknown source. Use spam filters and basic email security settings to reduce risky emails. It is also helpful for employees to receive regular security awareness training so they can recognize phishing attempts and stay safe.

Do's and Don'ts for Users

Do check and confirm the sender's identity before replying to any email. Do report any suspicious or unusual emails to the IT or security team so they can investigate. Do move your mouse over links to see the real destination before clicking on them. Do not share passwords or any sensitive information through email messages. Do not immediately trust emails that create urgency or pressure you to act quickly. Do not download attachments from unknown or suspicious sources.

SAMPLE NO :2

Email Sample Details (Analyzed Mail)

Subject: Desvende os Segredos do Momentum Trading em Português

From: Raunaq Sahni
Email Address: raunaq.s@quantinsti.com

Return Path: em.quantinsti.com

Sender IP: 149.72.51.63

Mail Service: SendGrid Email Marketing Platform

Authentication Results:

SPF: Pass
DKIM: Pass
DMARC: Pass (policy = quarantine)

Email Header Analysis

Authentication Results:

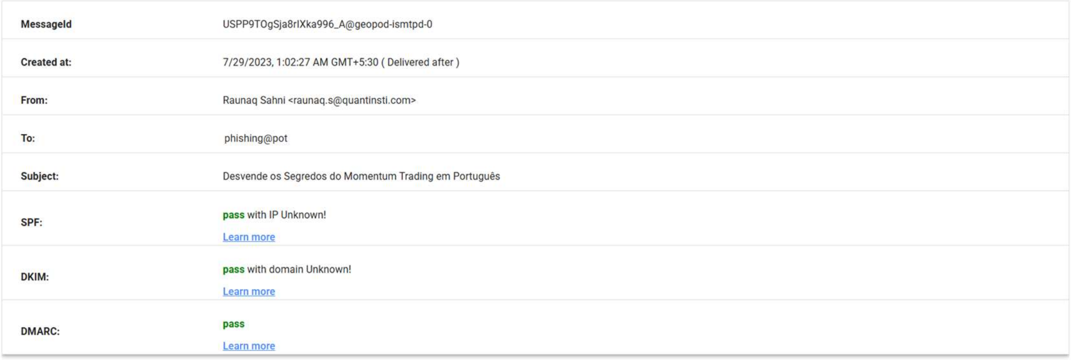
SPF PASS — The email was sent from an authorized server approved by the sender's domain.

DKIM PASS — The email content was verified and not modified during delivery.

DMARC PASS — The sender identity matches the domain and passes domain alignment checks.

Important Note:

Even if SPF, DKIM, and DMARC pass, it does not automatically mean the email is completely safe. Attackers sometimes use legitimate email services to send promotional or misleading emails.



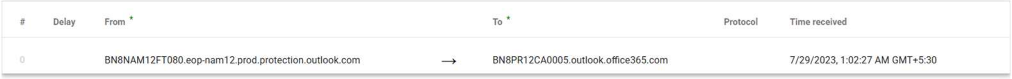
MessageId	USPP9TOgSja8rlXka996_A@geopod-ismtpd-0
Created at:	7/29/2023, 1:02:27 AM GMT+5:30 (Delivered after)
From:	Raunaq Sahni <raunaq.s@quantinsti.com>
To:	phishing@pot
Subject:	Desvende os Segredos do Momentum Trading em Português
SPF:	pass with IP Unknown! Learn more
DKIM:	pass with domain Unknown! Learn more
DMARC:	pass Learn more

Routing Analysis

The email passed through the following systems:

- SendGrid mail servers (email marketing infrastructure)
- Microsoft Outlook protection servers
- Secure encrypted TLS connections

The delivery path appears normal with no suspicious relay servers or abnormal delays.



#	Delay	From *		To *	Protocol	Time received
0		BN8NAM12FT080.eop-nam12.prod.protection.outlook.com	→	BN8PR12CA0005.outlook.office365.com		7/29/2023, 1:02:27 AM GMT+5:30

Content Review

The email contains:

- Promotional trading course information
- Marketing style language
- Discount offer (75%)
- Tracking links used for measuring user engagement

Tracking links are commonly used in marketing emails and do not necessarily indicate phishing.

Security Indicators Observed

Legitimate sender domain used
Authentication checks passed
Server IP not blacklisted
No impersonation detected in headers
Professional marketing structure

Potential concerns:

Unexpected promotional email
Use of tracking links
Marketing urgency language

Risk Classification

Risk Level: LOW RISK (Legitimate Promotional Email)

Based on technical analysis, the email appears to be a genuine marketing message rather than a phishing attack. No strong malicious indicators were found.

How the Email Works (Simple Explanation)

The organization sends a promotional email to advertise a course and encourage users to click links for more information or enrollment. Marketing emails often include tracking links to monitor user clicks and engagement. Although technically legitimate, users should always verify before interacting with unknown promotional messages.

Prevention Guidelines

Always verify promotional emails if you were not expecting them.
Avoid clicking links directly from emails; instead visit the official website manually.
Do not enter login credentials through email links unless you confirm the website is genuine.
Check the sender’s domain carefully.
Report suspicious emails to the security team.

Final Conclusion

Based on header authentication, routing path, and content analysis, this email is most likely a legitimate marketing email sent through authorized infrastructure. No strong evidence of phishing or malicious activity was detected.

SAMPLE NO : 3

Email Details

Subject: Urgent: Verify Your Account Now

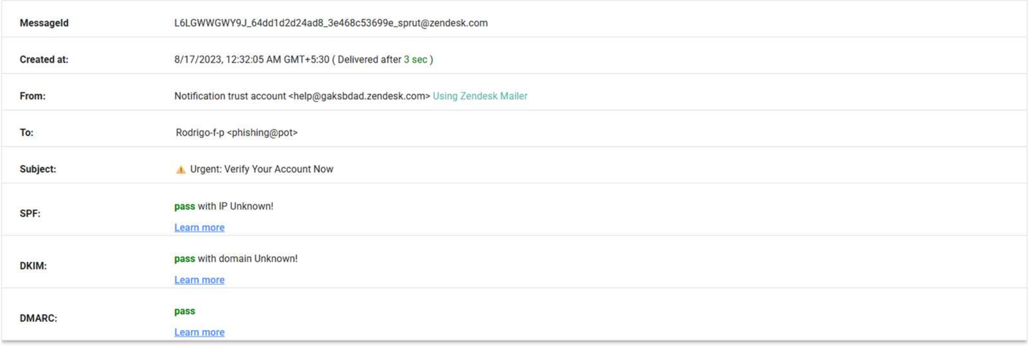
Sender: help@gaksbdad.zendesk.com

Email Service Used: Zendesk Mailer

Message Type: Account verification request pretending to be related to Trust Wallet.

Google Admin Toolbox Result (What it shows)

SPF: Pass
DKIM: Pass
DMARC: Pass



MessageId	L6LGWWGWY9J_64dd1d2d24ad8_3e468c53699e_sprut@zendesk.com
Created at:	8/17/2023, 12:32:05 AM GMT+5:30 (Delivered after 3 sec)
From:	Notification trust account <help@gaksbdad.zendesk.com> Using Zendesk Mailer
To:	Rodrigo-f-p <phishing@pot>
Subject:	⚠ Urgent: Verify Your Account Now
SPF:	pass with IP Unknown! Learn more
DKIM:	pass with domain Unknown! Learn more
DMARC:	pass Learn more

Simple meaning:

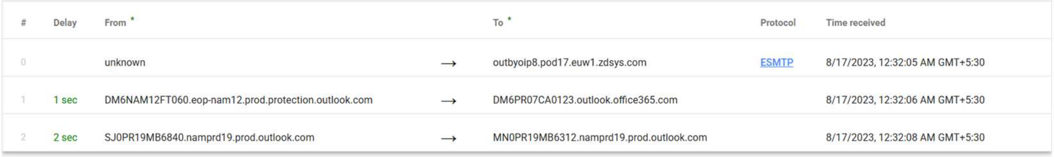
The email passed basic technical checks. This only means the email was sent from a valid server. It does NOT mean the email is safe or trustworthy.

Many phishing emails also pass these checks because attackers use real email services.

Email Routing Path Analysis

Email Routing Details (from Google Admin Toolbox):

The email passed through multiple mail servers before reaching the recipient. While this is normal for many emails, the initial sending source shows unclear or unknown origin details. Legitimate organizations usually have clearly identifiable sending paths. An unclear origin can sometimes indicate suspicious or phishing activity.



#	Delay	From *		To *	Protocol	Time received
0		unknown	→	outbyoip8.pod17.euw1.zdsys.com	ESMTP	8/17/2023, 12:32:05 AM GMT+5:30
1	1 sec	DM6NAM12FT060.eop-nam12.prod.protection.outlook.com	→	DM6PR07CA0123.outlook.office365.com		8/17/2023, 12:32:06 AM GMT+5:30
2	2 sec	SJ0PR19MB6840.namprd19.prod.outlook.com	→	MN0PR19MB6312.namprd19.prod.outlook.com		8/17/2023, 12:32:08 AM GMT+5:30

Suspicious Signs Found

The email asks the user to verify their account urgently.
It creates pressure by saying action is needed immediately.
It uses a general greeting like “Dear Customer.”
The sender address looks unusual and not like an official Trust Wallet email.
These are common signs of phishing emails.

Suspicious Link Found

Verification link inside email:

https://scnv.io/i5iT

Problems:

- The link is shortened, so the real website is hidden.
- It does not match the official company website.
- Phishing attackers often use shortened links to hide dangerous pages.

VirusTotal Safety Check

VirusTotal scan shows:

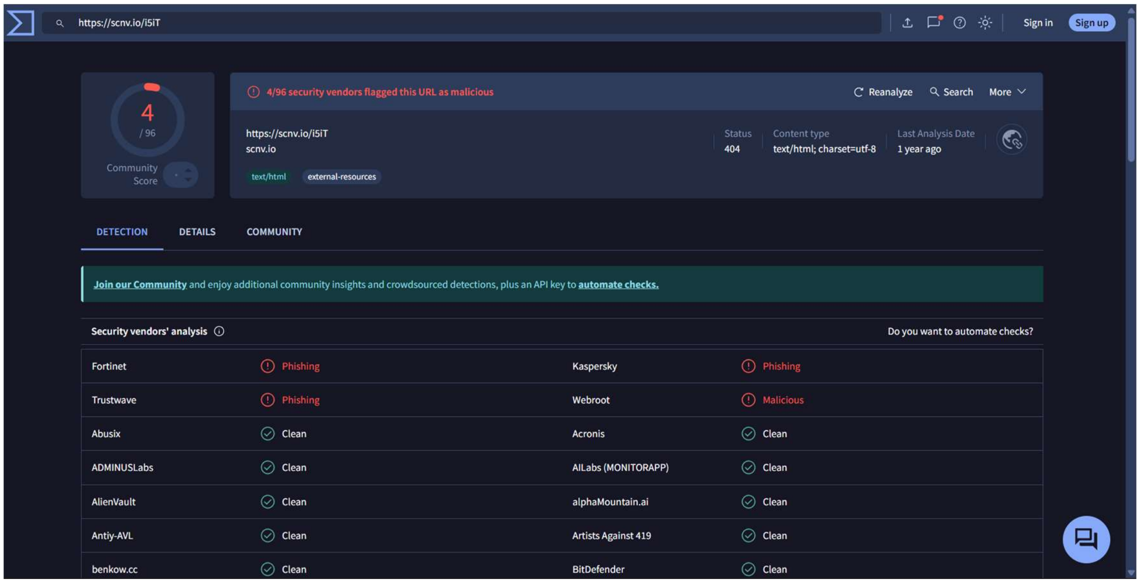
4 security vendors marked this link as phishing or malicious.

Examples:

Fortinet – Phishing
Trustwave – Phishing
Kaspersky – Phishing
Webroot – Malicious

Simple meaning:

Some security tools already identified this link as unsafe.



4/96 security vendors flagged this URL as malicious

https://scnv.io/i5iT
scnv.io
text/html external-resources

Status	Content type	Last Analysis Date
404	text/html; charset=utf-8	1 year ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Fortinet	Phishing	Kaspersky	Phishing
Trustwave	Phishing	Webroot	Malicious
Abusix	Clean	Acronis	Clean
ADMINUSLabs	Clean	AILabs (MONITORAPP)	Clean
AlienVault	Clean	alphaMountain.ai	Clean
Antiy-AVL	Clean	Artists Against 419	Clean
benkow.cc	Clean	BitDefender	Clean

Final Conclusion

Even though Google Admin Toolbox shows the email passed technical checks, the email is NOT safe.

Because:

- It contains a suspicious shortened link.
- Security tools flagged the link as phishing.
- The message uses urgency and impersonation tactics.

Final Verdict: This is likely a phishing email and should not be trusted.

Safety Advice

Do not click the link.
Do not enter any login details.
Delete or report the email as phishing.
Always open official websites manually instead of clicking email links.