FUTURE INTERNS

CYBERSECURITY TASK-2
PHISHING EMAIL DETECTION & AWARENESS SYSTEM

PREPARED BY

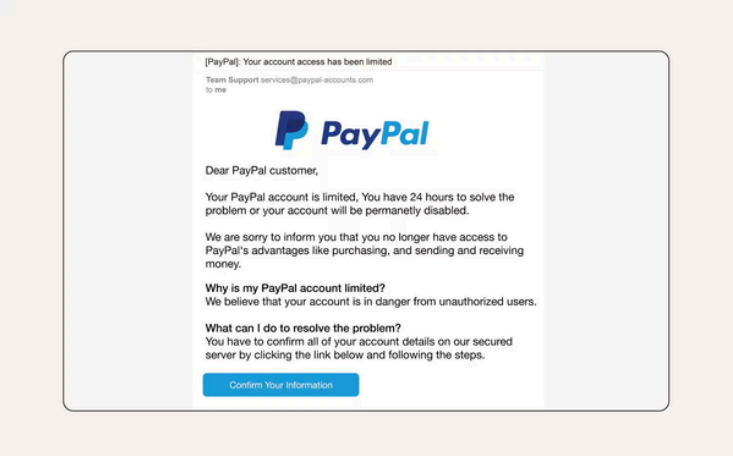
ANUSHA PEDDAPALLI

INTRODUCTION

Phishing is one of the most common cyber threats today. In phishing attacks, criminals send fake emails that appear to come from trusted sources to trick users into clicking malicious links, downloading harmful files, or sharing sensitive information like passwords and OTPs.

Many attacks succeed not because systems are weak, but because users are misled. This report analyzes real phishing email examples and explains how to identify suspicious messages in a simple way. The aim is to improve user awareness and help prevent phishing attacks in organizations.

PHISHING EMAIL EXAMPLES

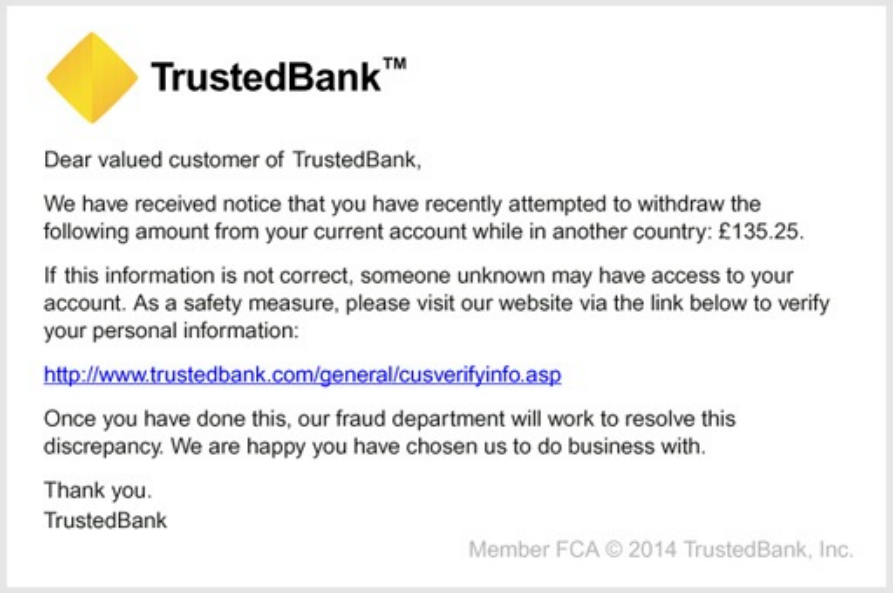


Case 1:Credential Harvesting Phishing
Risk Level: High (Phishing)

Description:
This email claims that your PayPal account has a problem and asks you to act quickly. It tries to scare you into clicking a button, which usually leads to a fake website.

Impact:
If you enter your details on that website, your account information can be stolen and misused.

Prevention Tips:
Do not click links in such emails.
Visit PayPal by typing the website address yourself.
Check the sender's email address.
Never share your password.



TrustedBank™

Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your current account while in another country: £135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/cusverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you.
TrustedBank

Member FCA © 2014 TrustedBank, Inc.

Case 2:Financial Phishing (Bank Impersonation)
Risk Level: High

Description:

This email pretends to be from a bank and says there was a suspicious money withdrawal. It uses fear and urgency to make the user click the link and check their account.

Impact:

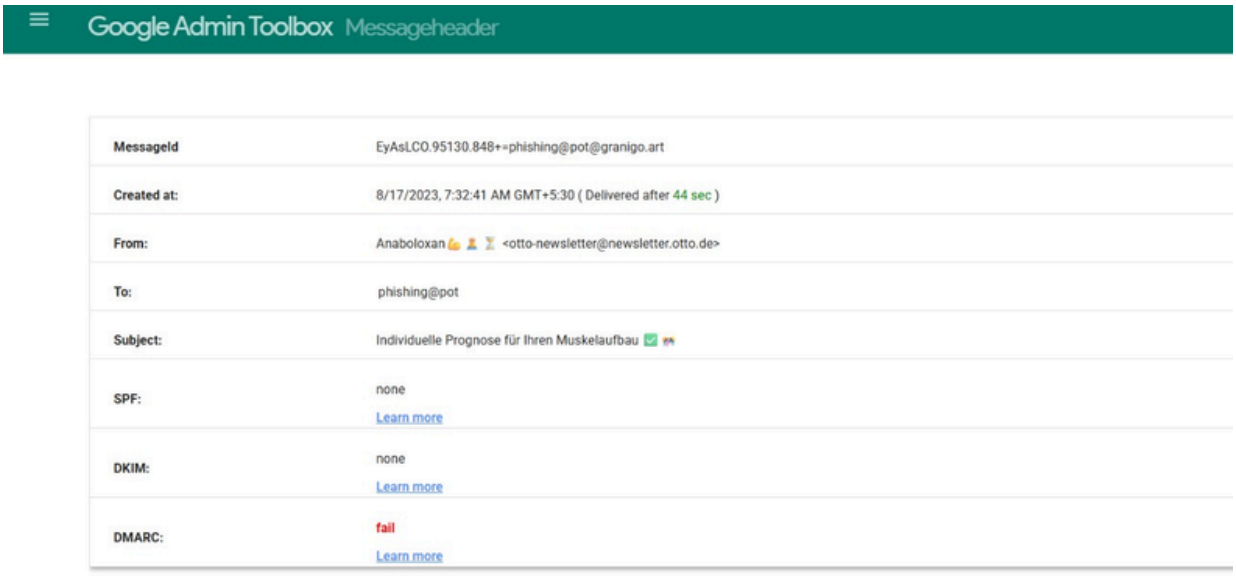
The link can open a fake bank website that looks real. When the user enters their personal or login details, the attacker steals this information and can misuse the bank account or the user's identity.

Prevention Tips:

Open the bank's website or app directly.
Never share passwords, PINs, or OTPs.
Report suspicious emails to the bank or IT/security team.

Google Message Header Analyzer

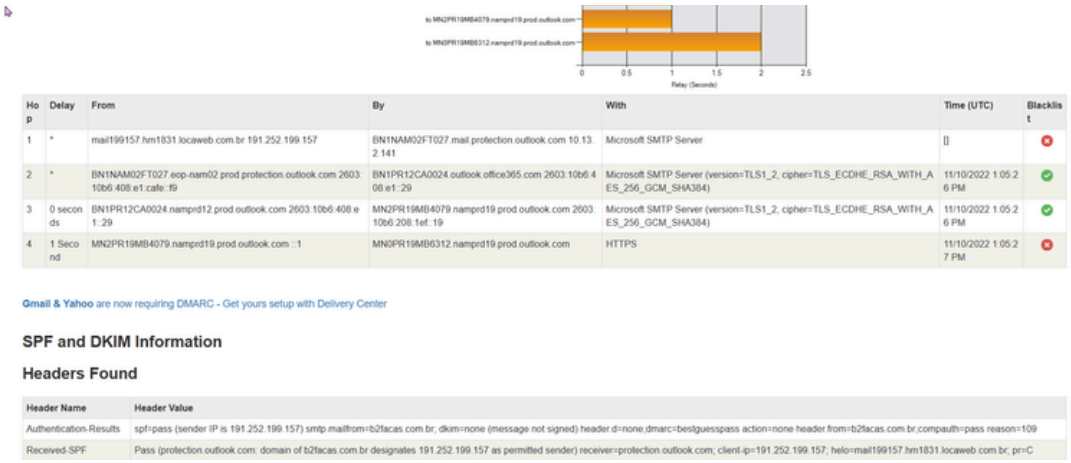
The email header was analyzed using Google Message Header Analyzer. This tool shows where the email came from and helps check if the sender is genuine.



The result indicates that the email is suspicious / phishing because the sender details do not match a trusted source. The tool works by checking the hidden technical details of the email.

MXT TOOL BOX

The email header was analyzed using MXToolbox. This tool helps check the sender's domain and basic email security settings.



Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	mail199157.hm1831.locaweb.com.br 191.252.199.157	BN1NAM02FT027.mail.protection.outlook.com 10.13.2.141	Microsoft SMTP Server	[]	
2	*	BN1NAM02FT027.eop-nam02.prod.protection.outlook.com 2603:10b6:408:e1::cafe:f9	BN1PR12CA0024.outlook.office365.com 2603:10b6:408:e1::29	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	11/10/2022 1:05:26 PM	
3	0 seconds	BN1PR12CA0024.namprd12.prod.outlook.com 2603:10b6:408:e1::29	MN2PR19MB4079.namprd19.prod.outlook.com 2603:10b6:208:1ef::19	Microsoft SMTP Server (version=TLS1_2, cipher=TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384)	11/10/2022 1:05:26 PM	
4	1 Second	MN2PR19MB4079.namprd19.prod.outlook.com ::1	MN0PR19MB6312.namprd19.prod.outlook.com	HTTPS	11/10/2022 1:05:27 PM	

Gmail & Yahoo are now requiring DMARC - Get yours setup with Delivery Center

SPF and DKIM Information

Headers Found

Header Name	Header Value
Authentication-Results	spf=pass (sender IP is 191.252.199.157) smtp.mailfrom=b2facas.com.br; dkim=none (message not signed) header.d=none;dmarc=bestguesspass action=none header.from=b2facas.com.br;compauth=pass reason=109
Received-SPF	Pass (protection.outlook.com: domain of b2facas.com.br designates 191.252.199.157 as permitted sender) receiver=protection.outlook.com; client-ip=191.252.199.157; helo=mail199157.hm1831.locaweb.com.br; pr=C

The result indicates that the email is suspicious / phishing because the domain or security checks do not match a trusted source. The tool works by checking the hidden details of the email and the sender's domain protection.

Phishing Attacks and User Awareness

Types of Phishing:

Phishing attacks come in different forms, but the goal is always the same: to trick users into giving away their information.

- **Email Phishing:** Fake emails that look like they are from banks, PayPal, or companies and ask you to click a link or log in.
- **Link Phishing:** Messages that contain dangerous links which open fake websites.
- **Attachment Phishing:** Emails that ask you to download a file which can be harmful.
- **Impersonation Phishing:** Emails that pretend to be from a trusted company or your workplace.

User Awareness and Safety Tips:

When you receive such messages, users should follow these simple steps:

- Do not click on links in suspicious emails
- Check the sender’s email address carefully
- Do not download unknown attachments
- Never share passwords, PINs, or OTPs
- Open websites by typing the address yourself
- Report suspicious emails to the IT or security team