TASK 2 (FUTURE INTERN)

Phishing Email Analysis – Sample 1

1. Email Details

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

From: BANCO DO BRADESCO LIVELObanco.bradesco@atendimento.com.br

Impersonated Organization:
Banco Bradesco

Date:
19 September 2023

2. Header Observation

The email claims to be sent on behalf of a well-known bank.
However, the sender email address does not belong to the official bank domain.

This indicates that the sender identity is suspicious.

3. Identified Phishing Indicators

Indicator	Observation
Sender domain mismatch	The email uses the domain **atendimento.com.br**, which is not the official domain of the bank.
Impersonation	The sender name pretends to be a trusted bank brand.
Urgency	The subject says that reward points are expiring today.
Social engineering	The message is designed to push the user to act quickly without verification.

4. Link and Content Observation

The email is designed to make the user believe that reward points will expire.
Such messages usually contain a link that leads to a fake website where users are asked to provide sensitive information.

5. Risk Classification

Phishing

6. How the Attack Works (Simple Explanation)

This email pretends to come from a bank and informs the user that their reward points are about to expire.
The attacker tries to create urgency so that the user clicks a link and enters personal or banking information on a fake website.
Once the user submits the details, the attacker can steal them.

7. Final Conclusion

This email is a phishing attempt that impersonates a legitimate bank in order to trick users into revealing sensitive information.

Phishing Email Analysis – Sample 2

1. Email Details

Subject:
Urgent: Suspicious Activity Detected on Your PayPal Account

Sender (From):
security-alert@paypal-support.com

Impersonated Organization:
PayPal

2. Sender Observation

The email claims to be sent from PayPal security.
However, the sender email address uses the domain **paypal-support.com**, which is not the official PayPal domain.

This indicates that the sender is pretending to be PayPal.

3. Identified Phishing Indicators

Indicator	Observation
Fake sender domain	The sender domain **paypal-support.com** is not the official PayPal domain.
Urgency	The email asks to verify within 24 hours.
Fear message	The email says the account has suspicious activity and is limited.
Suspicious link	The link points to a different domain and not to the real PayPal website.
Generic greeting	The email uses “Dear Customer” instead of the real name.

4. Link and URL Observation

The email contains the following link:

https://paypal-security-check.com/verify

The domain name is different from the official PayPal website.
This strongly suggests that the link may lead to a fake login page.

5. Risk Classification

Phishing

6. How the Attack Works

This email pretends to be sent by PayPal and tells the user that there is suspicious activity on the account.
The attacker creates fear and urgency so that the user clicks the verification link.
When the user opens the fake website and enters login details, the attacker steals the account information.

7. Final Conclusion

This email is a phishing attempt that impersonates PayPal in order to trick users into clicking a fake verification link and sharing their login details.

Introduction

This report analyzes phishing email samples in order to identify common phishing indicators and to create awareness among users to prevent email-based cyber attacks.

Tools used

- Google Admin Toolbox – Message Header Analyzer
- MXToolbox
- Browser inspection
- Public phishing samples from **GitHub**

Email Analysis

Sample 1 (Bradesco email)

Sample 2 (PayPal email)

Prevention & Awareness

Do’s

- Check the sender’s email address carefully
- Hover over links before clicking
- Verify urgent messages through official websites
- Report suspicious emails to the IT team

Don’ts

- Do not click unknown links
- Do not share passwords or OTP
- Do not download unknown attachments
- Do not reply to suspicious emails