

# Phishing Email Detection & Awareness Report

**Intern:** Jayshri Sutar

**Domain:** Cyber Security

---

## 1. Introduction

Phishing is a social engineering attack where attackers attempt to steal sensitive information by impersonating legitimate organizations.

This report analyzes five email samples to identify phishing indicators and classify associated risks.

---

## 2. Objective

- Identify phishing indicators
  - Classify suspicious emails
  - Provide awareness and prevention guidelines
- 

## 3. Email Analysis

---

### Email 1 – Fake Bank Alert

**Classification:** Phishing

**Risk Level:** High

#### Indicators Identified:

- Suspicious sender domain
- Urgency (24 hours)
- Fake login link
- Generic greeting

#### Explanation:

The attacker attempts to create panic and redirect the user to a fake login page to steal credentials.

---

### Email 2 – Fake PayPal Login

**Classification:** Phishing

**Risk Level:** High

#### Indicators:

- Fake sender domain

- Account closure threat
- Suspicious link

**Explanation:**

The email impersonates PayPal to trick users into revealing login credentials.

---

 **Email 3 – Lottery Scam**

**Classification:** Phishing

**Risk Level:** High

**Indicators:**

- Unrealistic reward
- Request for bank details
- No official verification

**Explanation:**

This is a classic advance-fee scam designed to steal financial information.

---

 **Email 4 – Fake Password Reset**

**Classification:** Phishing

**Risk Level:** Medium

**Indicators:**

- Misspelled domain (amazOn)
- Suspicious URL
- Fear-based message

**Explanation:**

Attackers use lookalike domains to trick users.

---

 **Email 5 – Legitimate Security Notification**

**Classification:** Safe

**Risk Level:** Low

**Indicators:**

- Official domain
- HTTPS secure link
- No urgent threat

**Explanation:**

This appears to be a legitimate security notification.

---

**4. Common Phishing Indicators**

- Spoofed sender address
  - Urgent or threatening language
  - Suspicious links
  - Grammar mistakes
  - Unexpected attachments
- 

**5. Prevention Guidelines**

- Verify sender email carefully
  - Do not click suspicious links
  - Enable Multi-Factor Authentication
  - Use spam filters
  - Report phishing emails
- 

**6. Conclusion**

The analysis demonstrates how phishing attacks exploit fear, urgency, and deception.

User awareness and proper verification practices can significantly reduce phishing risks.