PHISHING EMAIL DETECTION & AWARENESS REPORT

Future Interns – Cyber Security Task 2
Prepared By: S.R. Yashas

---

1. Executive Summary

Phishing continues to be one of the most prevalent and damaging cyber threats faced by organizations globally. Unlike attacks that exploit software flaws, phishing primarily targets human behavior by leveraging deception, urgency, and impersonation techniques.

This report evaluates selected phishing email scenarios to identify attack patterns, detect warning signs, and categorize the level of risk involved. Additionally, it provides practical awareness recommendations to help employees identify fraudulent communications and prevent credential compromise, financial fraud, and unauthorized data access.

---

2. Scope & Objective

Objective

The purpose of this assessment is to examine phishing email examples, detect common red flags, classify their severity, and develop an awareness reference guide for organizational training.

Scope Includes

- Examination of suspicious email content
- Verification of sender domain authenticity
- Analysis of embedded URLs
- Risk categorization
- Development of employee awareness recommendations

Scope Excludes

- Penetration testing of mail servers
- Interaction with malicious links or attachments
- Malware reverse engineering
- Any unauthorized or intrusive activity

This task strictly focuses on phishing identification and preventive awareness.

---

3. Phishing Email Sample 1 – Security Alert Impersonation

Email Subject:

Security Notice: Immediate Action Required to Secure Your Profile

Email Summary:

The message claims unusual login attempts were detected from an unknown device and asks the recipient to confirm their identity through a provided link to avoid account deactivation.

Suspicious URL:

http://account-security-check[.]net

Identified Warning Signs:

- Non-personalized greeting (“Hello Customer”)
- Artificial urgency and warning tone
- Threat of account suspension within 24 hours
- Unfamiliar domain unrelated to official services
- Absence of official branding elements

Attack Mechanism:

The attacker attempts to create anxiety by reporting suspicious login activity. The provided link typically redirects to a counterfeit login portal designed to capture usernames and passwords.

Risk Level:

High Risk – Confirmed Phishing Attempt

---

4. Phishing Email Sample 2 – Payment Failure Fraud

Email Subject:

Action Required: Transaction Declined – Update Payment Details

Sender Address:

accounts@secure-payments-support.com

Email Summary:

The email informs the recipient that a recent subscription payment could not be processed and urges immediate payment confirmation to prevent service interruption.

Suspicious URL:

http://billing-update-center[.]org

Identified Warning Signs:

- Domain attempting to resemble legitimate financial services
- Pressure to act quickly to avoid penalties
- Unexpected billing notification
- Hyperlink not matching official company domain
- Minor grammatical inconsistencies

Attack Mechanism:

The attacker impersonates a financial institution or subscription platform. Victims may click the malicious link and unknowingly submit banking details or download harmful files.

Risk Level:

High Risk – Phishing & Financial Fraud

---

5. Email Header & Domain Observations

Although complete raw email headers were not available for technical forensic review, phishing campaigns typically display irregularities such as:

- Inconsistency between display name and actual sending address
- Unknown or blacklisted IP addresses
- SPF authentication failures
- DKIM signature validation errors
- Reply-To address differing from the original sender

Attackers frequently use domain imitation techniques such as:

- Character substitution (e.g., replacing “o” with “0”)
- Slight misspellings of trusted brands
- Additional words such as “support” or “secure” to appear legitimate

Such manipulation is commonly referred to as **typosquatting** and is a strong indicator of phishing intent.

---

6. Common Phishing Characteristics Identified

From the analysis of both cases, recurring phishing traits include:

- Generic or vague greetings
- Fear-driven messaging
- Urgent deadlines
- Suspicious hyperlinks
- Financial or account-related threats
- Poor formatting or inconsistent branding
- Requests for sensitive information

These indicators align with patterns observed in real-world phishing campaigns targeting employees and individuals.

---

7. Risk Classification Framework

The following classification model was applied:

Category	**Description**
Safe	Verified sender, legitimate domain, no suspicious indicators
Suspicious	Minor inconsistencies requiring verification
Phishing (High Risk)	Multiple confirmed red flags and malicious intent

Both analyzed email samples fall under the **Phishing – High Risk** category due to multiple deception indicators.

---

8. Prevention & Awareness Recommendations

Organizations can significantly minimize phishing risks through structured awareness programs and internal security controls.

Recommended Best Practices:

- Carefully inspect sender email domains

- Hover over hyperlinks before clicking
- Avoid sharing passwords, OTPs, or financial details via email
- Independently verify urgent payment requests
- Immediately report suspicious emails to IT/security teams
- Enable Multi-Factor Authentication (MFA)
- Conduct regular phishing simulation training

Human vigilance is the strongest line of defense against phishing attacks.

---

9. Employee Guidelines – Do's & Don'ts

Do:

- Confirm unexpected requests through official channels
- Verify domain spellings carefully
- Use strong, unique passwords
- Report suspicious emails immediately

Don't:

- Click unknown links
- Download unsolicited attachments
- Share confidential information via email
- Respond impulsively to urgent or threatening messages

---

10. Conclusion

Phishing attacks primarily exploit human trust rather than technical vulnerabilities. By mimicking trusted entities and creating artificial urgency, attackers manipulate victims into revealing sensitive information.

This analysis demonstrates that phishing indicators can be easily identified through careful inspection and awareness training.

Continuous employee education, secure authentication practices, and effective reporting mechanisms are essential to protecting organizational assets.

Proactive awareness remains the most reliable defense against phishing threats in today’s digital environment.