PHISHING EMAIL DETECTION & AWARENESS REPORT

ADARSH SINGH RAWAT
CYBER SECURITY - TASK 2
INTERNSHIP – FUTURE INTERNS
CIN ID: FIT/FEB26/CS6144
FEBRUARY 2026

INTRODUCTION

In order to find possible security risks and evaluate the risk impact, this paper examines a suspected phishing email. In order to stop financial fraud and identity theft, the goal is to assess phishing indications and offer awareness instructions.

EMAIL SAMPLE OVERVIEW

Subject: Urgent: Your Bank Account Will Be Suspended
Sender: support@secure-banking-alerts.com

Dear Customer,

We have detected unusual activity in your bank account.
To avoid permanent suspension, please verify your account immediately.
Click here to secure your account:
http://secure-bank-login-verification.com
Failure to verify within 24 hours will result in account closure.

Thank you,
Bank Security Team

IDENTIFIED PHISHING INDICATORS

Bullet points:

- **Generic greeting (“Dear Customer”)**
- **No official bank name mentioned**
- **Suspicious sender domain**
- **Urgency-based messaging**
- **Suspicious HTTP link**
- **Possible domain spoofing**

RISK CLASSIFICATION

- **RISK LEVEL : HIGH**

Through a fake link, this email aims to fool recipients into disclosing their banking information, potentially resulting in financial fraud.

POTENTIAL IMPACT

- Credential theft
- OTP capture
- Unauthorized transactions
- Financial loss
- Identity theft

PREVENTION & AWARENESS GUIDELINES

- Verify sender domain carefully
- Do not click suspicious links
- Contact official bank directly
- Enable multi-factor authentication
- Report phishing emails

CONCLUSION

Common social engineering techniques including haste and domain spoofing are displayed in this phishing email. Users need to be on the lookout for unusual communications and confirm them before acting. Users must remain vigilant and verify suspicious communications through official channels before taking any action.