18TH JANUARY 2026

PHISHING EMAIL DETECTION & AWARENESS REPORT

PRESENTED TO

Future Interns

PRESENTED BY

Chiluka Varshith Reddy

Confidentiality Statement

This document is prepared solely for educational and learning purposes as part of the Future Interns Cyber Security Internship Program. The contents of this report are intended to support security awareness and training initiatives and must not be used for malicious or unauthorized activities.

Disclaimer

This report is based on the analysis of publicly available phishing email samples and simulated examples used for security awareness training. No real individuals, organizations, or live email systems were targeted during this assessment. All analysis was conducted ethically and for educational purposes only.

Assessment Overview

Phishing attacks are one of the most common methods used by attackers to compromise user accounts and organizational security. This assessment focuses on identifying and analyzing phishing email characteristics and educating users on how to recognize and avoid such attacks.

The purpose of this report is to analyze phishing email samples, identify common indicators of phishing, classify email risk levels, and provide clear awareness guidelines that businesses can use to improve employee security awareness.

Scope

In Scope :

- Analysis of publicly available phishing email samples
- Identification of phishing indicators
- Email risk classification
- User awareness and prevention guidance

Out of Scope :

- Sending phishing emails
- Attacking real email systems
- Social engineering against real users
- Any form of illegal or unethical activity

Methodology

The following methodology was used during this assessment:

1. Collection of publicly available phishing email samples.
2. Review of email subject lines, sender details, and message content.
3. Inspection of URLs and domains in a safe manner.
4. Identification of phishing indicators and social engineering techniques.
5. Risk classification of emails.
6. Documentation of findings and awareness recommendations.

This approach aligns with standard security awareness and phishing analysis practices used in organizations.

What is Phishing?

Phishing is a form of social engineering attack in which attackers impersonate trusted entities to trick users into revealing sensitive information, clicking malicious links, or downloading harmful attachments. Phishing attacks often rely on urgency, fear, or curiosity to manipulate users into taking unsafe actions.

Common Phishing Indicators

The following indicators are commonly found in phishing emails:

- Suspicious or spoofed sender email addresses
- Urgent or threatening language
- Generic greetings instead of personalized names
- Suspicious links or shortened URLs
- Requests for sensitive information such as passwords or OTPs
- Spelling or grammatical errors

Recognizing these indicators is critical to preventing phishing attacks.

Phishing Email Analysis

Sample 1 - Fake Account Security Alert

Email Subject:

⚠️ Important: Unusual Login Activity Detected

Claimed Sender:

Security Team <security@account-alerts-support.com>

Email Summary:

The email claims that unusual login activity was detected on the user’s account and urges immediate action to secure the account. It attempts to create fear and urgency by warning that failure to respond may result in account suspension.

Phishing Indicators Identified:

- Sender email domain does not match any known or official organization.
- Urgent and fear-based language encouraging immediate action.
- Generic greeting instead of addressing the user by name.
- Embedded link directing the user to an unknown external website.
- Threat of account suspension to pressure the user.

Risk Classification:

Phishing

Why This Email Is Dangerous:

If a user clicks the link and enters their credentials, attackers can capture login information and gain unauthorized access to the user's account. This may lead to account takeover, identity theft, or misuse of personal information.

What the User Should Do:

- Do not click on links in unsolicited security alert emails.
- Verify the alert by logging in directly through the official website.
- Check the sender's email address carefully.
- Report the email to the organization's IT or security team.

Sample 2 - Fake Password Reset Email

Email Subject:

Password Reset Request – Action Required

Claimed Sender:

Support Team <no-reply@password-reset-help.com>

Email Summary:

The email claims that a password reset request was initiated for the user's account. It encourages the user to click a link to reset the password, even though the user may not have requested any such action.

Phishing Indicators Identified:

- Sender domain is generic and not associated with a legitimate service.
- Message creates urgency by implying account access issues.
- No clear reference to which service the password reset is for.
- Embedded link leads to an unverified external website.
- Generic message without personalization.

Risk Classification:

Phishing

Why This Email Is Dangerous:

Users who click the reset link may be redirected to a fake login page designed to steal credentials. This can result in account compromise and unauthorized access.

What the User Should Do:

- Avoid clicking password reset links from unexpected emails.
- Check official notifications by logging in directly to the service.
- Verify sender details carefully.
- Report the email as phishing.

Sample 3 - Job / Internship Related Email

Email Subject:

Internship Opportunity – Application Follow-Up

Claimed Sender:

Recruitment Team <recruitment@company-careers.net>

Email Summary:

The email claims to be a follow-up regarding an internship opportunity and asks the recipient to review additional details. While the email does not contain obvious malicious content, it lacks clear verification and appears generic in nature.

Phishing Indicators Identified:

- Sender domain is unfamiliar and not clearly linked to a known organization.
- Generic greeting without addressing the recipient by name.
- Limited information about the company or role.
- Encourages clicking a link for more details.

Risk Classification:

Suspicious

Why This Email Is Dangerous:

Although the email does not show strong phishing indicators, the lack of clear sender identity and specific details makes it risky. Users could be redirected to untrusted websites or be asked to provide personal information later.

What the User Should Do:

- Verify the company through official websites or LinkedIn.
- Avoid clicking links until the sender is confirmed.
- Contact the organization through official channels.
- Treat the email with caution.

Sample 4 - Delivery / Courier Notification

Email Subject:

Your Package Has Been Delivered

Claimed Sender:

Courier Service <notifications@officialcourier.com>

Email Summary:

The email informs the recipient that a package has been successfully delivered. It does not request sensitive information or urge immediate action.

Phishing Indicators Identified:

- Sender email domain appears legitimate.
- No urgent or threatening language used.
- No request for passwords, OTPs, or personal information.
- Links (if present) direct to the official courier website.

Risk Classification:

Safe

Why This Email Is Considered Safe:

The email contains clear and relevant information, does not pressure the user into taking immediate action, and does not request sensitive data. It aligns with expected communication from a delivery service.

What the User Should Do:

- Review the email normally.
- Verify delivery details if needed by visiting the official website directly.
- Continue to follow standard email safety practices.

Risk Classification Summary

Emails analyzed in this report will be classified into the following categories:

Risk Level	Description
Safe	Legitimate email with no phishing indicators
Suspicious	Requires verification before action
Phishing	Malicious intent identified

Prevention & Awareness Guidelines

To reduce the risk of phishing attacks, organizations should:

- Educate employees on identifying phishing indicators
- Encourage verification of suspicious emails
- Avoid clicking links from unknown sources
- Use email filtering and anti-phishing tools
- Report suspicious emails to security teams

Conclusion

Phishing attacks continue to be a major threat to organizations, primarily targeting users rather than systems. This report highlights common phishing techniques and provides practical awareness guidance to help users identify and avoid phishing emails. Strengthening employee awareness is a critical step toward improving overall organizational security.