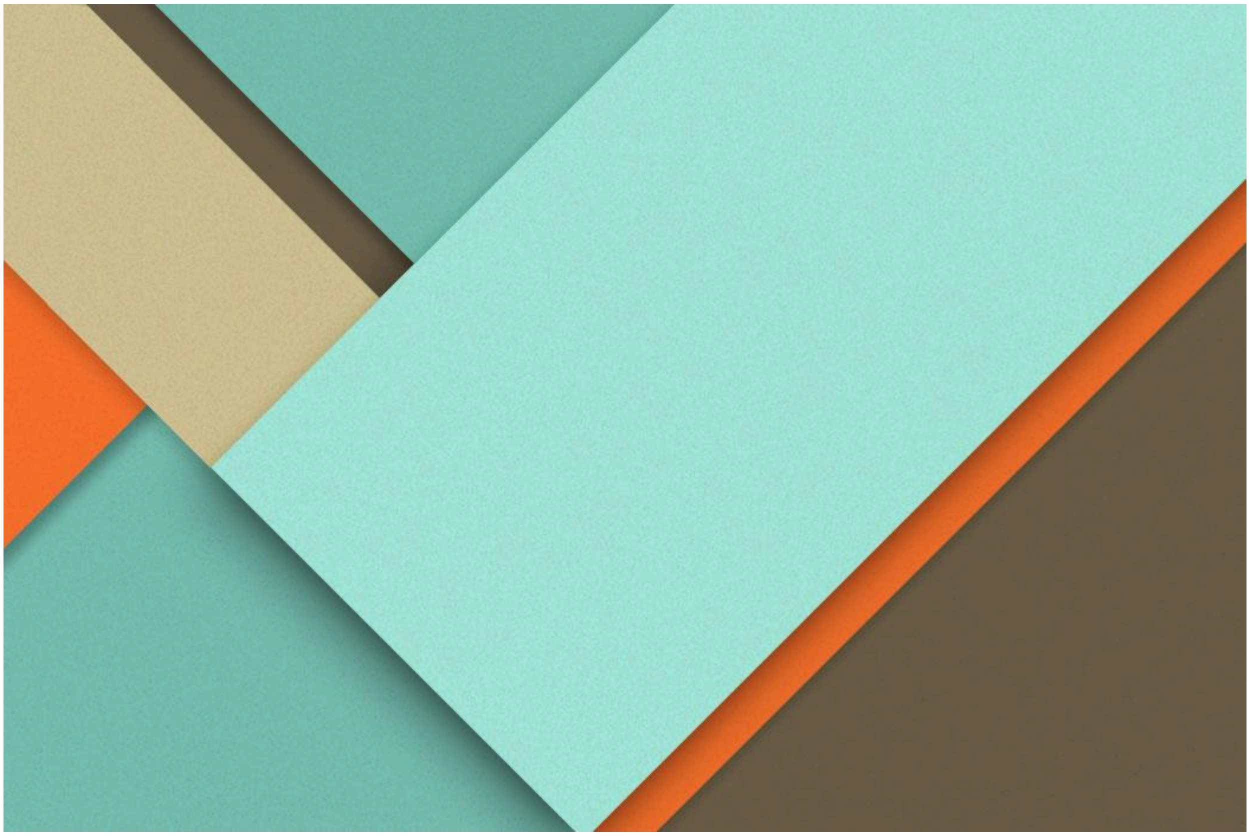


Phishing Email Detection And Awareness Report

02.02.2026

—

Done by:
SAGHANA K S

Phishing Email Detection & Awareness Report

Name: Saghana K S

Internship: Future Interns – Cybersecurity

Date: 02.02.2026

1. Introduction

Phishing is a cyber attack where attackers impersonate trusted organizations to trick users into revealing sensitive information, clicking malicious links, or performing unintended actions. This report analyzes three sample emails to identify phishing indicators, classify risks, and provide guidance on prevention.

2. Objective

- Identify phishing indicators in sample emails
- Classify emails as Safe / Suspicious / Phishing
- Explain phishing attack methods
- Provide clear prevention tips and user awareness guidance.

3. Tools Used

Message Header Analysis:

Tool: Google Admin Toolbox – Message Header Analyzer

Purpose: Analyze sender domain, mail routing, SPF/DKIM/DMARC authentication

Documentation & Reporting:

Google Docs / MS Word / PDF for professional reporting

4. Key Features of the Report

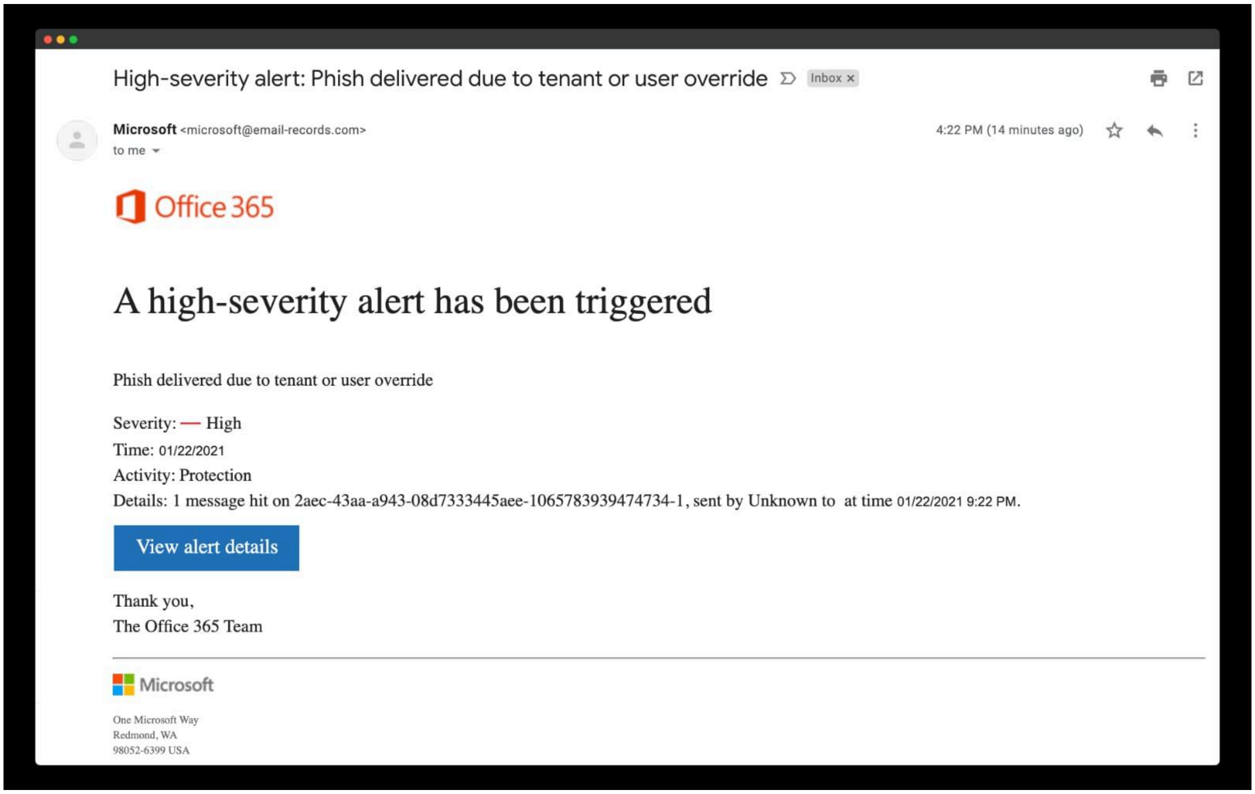
- Identification of phishing indicators
- Email risk classification
- Explanation of phishing attack methods
- Clear prevention tips
- Do’s and Don’ts for employees

5. Sample Email Analyses

Sample 1 – Microsoft Alert

Email Info:

From: Microsoft <microsoft@email-records.com>
Subject: High-severity alert: Phish delivered
Time: Recent



High-severity alert: Phish delivered due to tenant or user override

Microsoft <microsoft@email-records.com>
to me

4:22 PM (14 minutes ago)

A high-severity alert has been triggered

Phish delivered due to tenant or user override

Severity: — High
Time: 01/22/2021
Activity: Protection
Details: 1 message hit on 2aec-43aa-a943-08d7333445aee-1065783939474734-1, sent by Unknown to at time 01/22/2021 9:22 PM.

Thank you,
The Office 365 Team

One Microsoft Way
Redmond, WA
98052-6399 USA

Phishing Indicators:

- Domain mismatch
- Urgent / fear-based language
- Confusing message content
- Sent by unknown
- Suspicious call-to-action

Representative Header Analysis:

spf=fail

dkim=fail

dmarc=fail

Classification: 🔴 Phishing

User Tips:

- Hover over links before clicking
- Verify sender domain
- Access Microsoft alerts via official site
- Report suspicious emails.

Sample 2 – LinkedIn Demo Email

Email Info:

From: Support <support@careerbuildcompany.com>

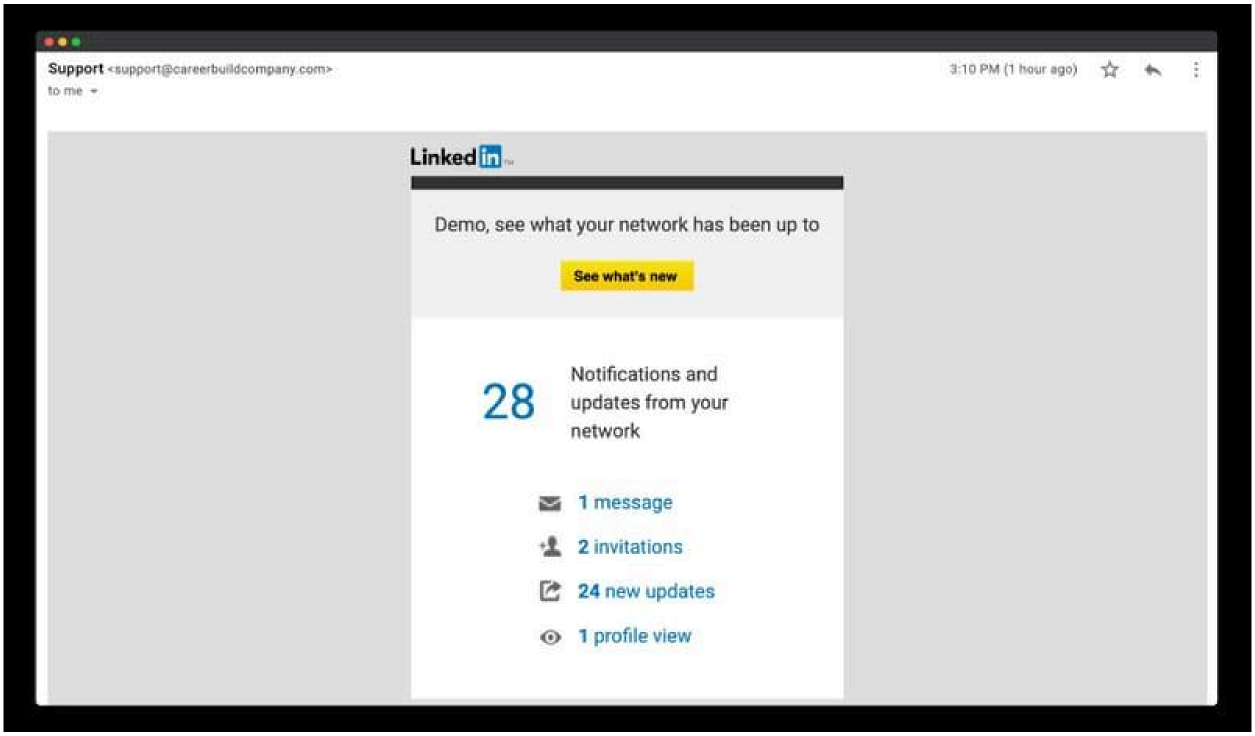
Subject: LinkedIn – Demo, see what your network has been up to

Time: Recent

Phishing Indicators:

- Domain mismatch

- Generic / curiosity-driven content
- Suspicious links



Support <support@careerbuildcompany.com>
to me

3:10 PM (1 hour ago)

Linkedin

Demo, see what your network has been up to

28 Notifications and updates from your network

1 message

2 invitations

24 new updates

1 profile view

Representative Header Analysis:

spf=fail

dkim=fail

dmarc=fail

Classification: 🔴 Phishing

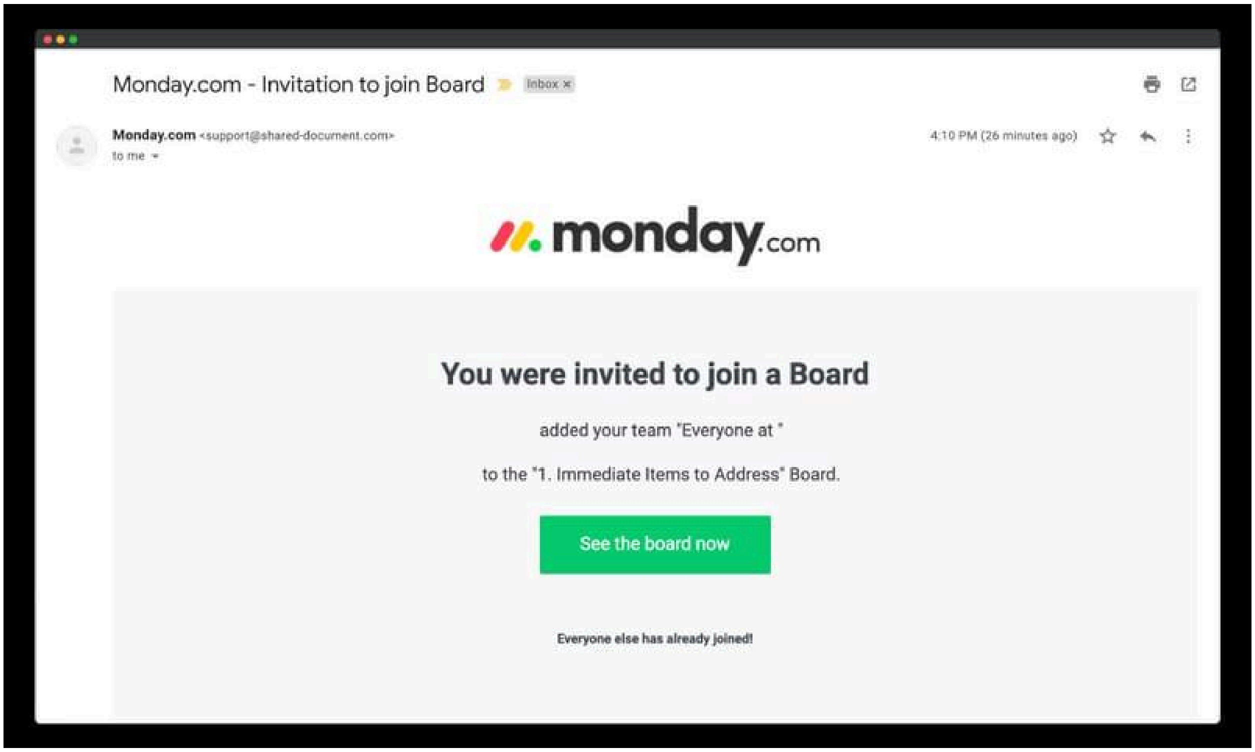
User Tips:

- Hover links before clicking
- Access LinkedIn via official website
- Report suspicious emails
- Do not reply or provide credentials

Sample 3 – Monday.com Board Invitation

Email Info:

From: Monday.com <support@shared-document.com>
Subject: Invitation to join Board
Time: Recent



Monday.com - Invitation to join Board

Monday.com <support@shared-document.com>
to me

4:10 PM (26 minutes ago)

monday.com

You were invited to join a Board

added your team "Everyone at "

to the "1. Immediate Items to Address" Board.

Everyone else has already joined!

Phishing Indicators:

- Domain mismatch
- Urgency / social proof
- Generic call-to-action

Representative Header Analysis:

spf=fail
dkim=fail
dmarc=fail

Classification: 🔴 Phishing

User Tips:

- Hover links before clicking
- Access Monday.com via official website
- Report suspicious emails
- Do not click links or provide credentials

6. Phishing Techniques Explained

- Domain Spoofing
- Urgency / Fear Tactics
- Social Engineering
- Malicious Links

7. Prevention & Awareness Tips

Do’s:

- Verify sender domain and email
- Hover over links to check URL
- Enable MFA
- Report suspicious emails

Don’ts:

- Do not click unknown links
- Do not provide credentials via email

- Do not download attachments from unverified sources

8. Conclusion

All three emails were classified as Phishing due to domain mismatches, unauthenticated headers, urgency-driven content, and suspicious links. Users should remain vigilant and follow cybersecurity best practices.

9. References / Tools

- Google Admin Toolbox – Message Header Analyzer
- Public phishing email samples