Phishing Email Analysis Report

Internship Task 2nd Submission

Intern Name: Meenakshi Mehra
Role: Cybersecurity Intern
Organization: Elevate Labs
Date: 5 August 2025

Overview

Two suspicious emails were analyzed to assess the nature and indicators of phishing attacks. This report summarizes the findings, highlights the red flags identified, and provides clear recommendations to prevent falling victim to such attacks.

Email 1: Contoso Corp HR Shared an Item

Email Details

- **Subject:** Contoso Corp HR shared an item
- **From:** support@cont0so-c0rp.org
- **Attachment:** Updated Company Org Chart - Contoso Corp.pdf

Message Body

“Contoso Corp Human Resources (HR) has shared the following item:
Due to unforeseen circumstances, changes have been made to the current management structure.
Download the new org chart below to understand how these changes impact you.”

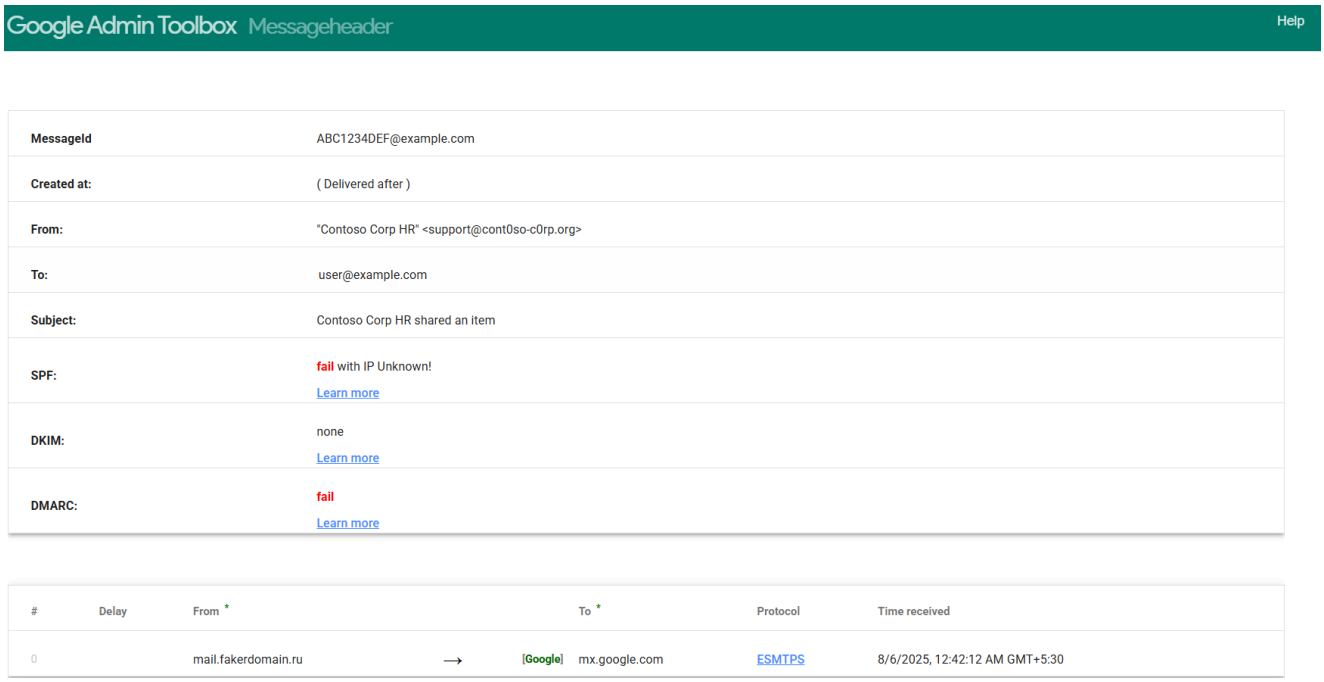
Phishing Indicators Identified

- **Suspicious Sender Domain:** The domain cont0so-c0rp.org mimics the legitimate contoso.com.
- **Urgency & Fear Tactic:** Language like "unforeseen circumstances" is used to provoke quick action.
- **Suspicious Attachment:** The attached PDF is unsolicited and potentially malicious.
- **Lack of Personalization:** The email does not address the recipient by name.
- **Email Header Authentication Failures:**

- **SPF:** Failed
- **DKIM:** None
- **DMARC:** Failed
- **IP:** 185.129.62.77 (Unrelated foreign IP)

Recommendations

- Do not open or download the attachment.
- Report the email to IT/Security teams.
- Mark the sender as spam and block the domain.



Email 2: Google Notifications – Sign-in Attempt Blocked

Email Details

- **Subject:** Google Notifications – Sign-in attempt was blocked
- **From:** google-support@webnotifications[.]net
- **To:** john.doe@mybusiness.com
- **Call to Action:** “Check activity” (link)

Message Body

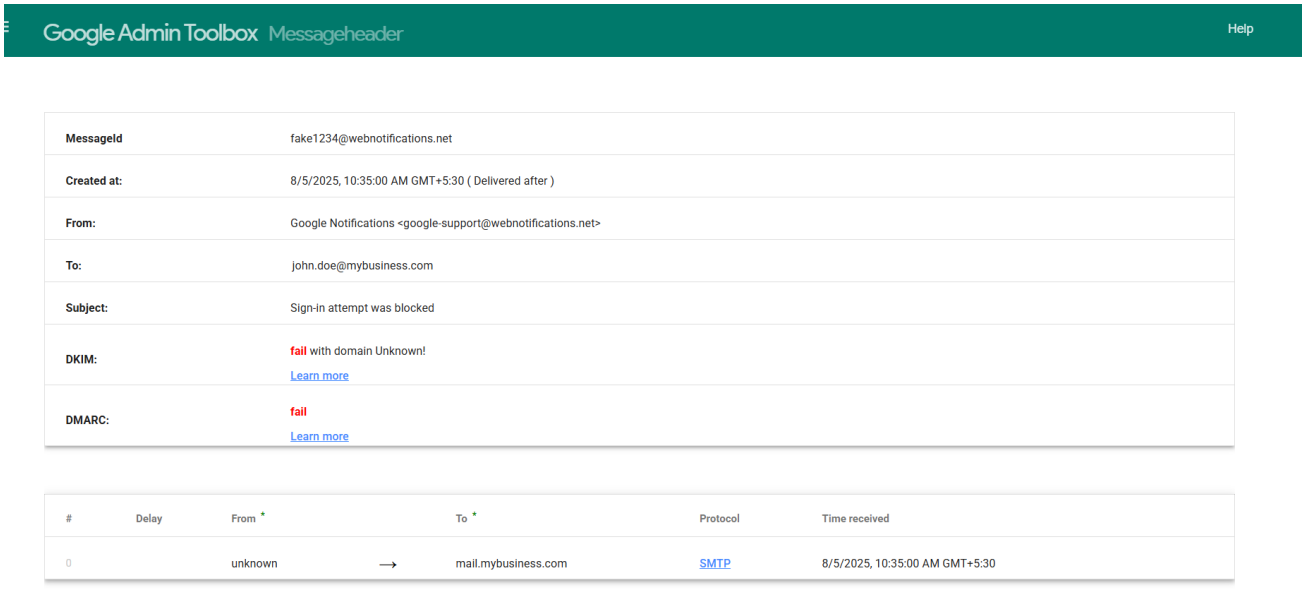
“Someone just used your password to try to sign in to your account from a non-Google app. Google blocked them, but you should check what happened. Review your account activity to make sure no one else has access.”

Phishing Indicators Identified

- **Deceptive Domain:** webnotifications.net is not a legitimate Google domain.
- **Fear & Urgency Tactic:** Suggests the account has been compromised to provoke response.
- **Malicious Call to Action:** Link may redirect to a fake login page.
- **Lack of Personalization:** Uses generic language instead of addressing the recipient.
- **Email Header Authentication Failures:**
    - **SPF:** Failed
    - **DKIM:** None
    - **DMARC:** Failed
    - **Reply-To:** Possibly mismatched

Recommendations

- Do not click the link.
- Mark the email as phishing using your email client.
- Verify such alerts through official Google security pages.



Conclusion

Both emails analyzed demonstrate classic signs of phishing, including deceptive domains, use of fear tactics, lack of personalization, and email authentication failures. Awareness and verification through official channels are critical to protecting sensitive information.

NOTE:

Both the emails are sample used here and by creating their Email Header I have analyze them in Google Admin Toolbox.