Phishing Detection & Awareness Report

Future Interns Task 2

P Charan Teja

24-01-2026

Introduction & Methodology

Executive Summary :

This report presents a technical audit of three sophisticated phishing campaigns. By analyzing raw email headers and social engineering triggers, this document identifies key indicators to improve organizational security posture.

Investigation Methodology :

- **Data Source**: Public phishing repositories (GitHub phishing_pot).
- **Analysis Tools**: Google Admin Toolbox for Header Analysis and manual URL inspection.
- **Verification**: Checking SPF/DKIM records to confirm sender identity fraud.

Case Study #1: Norton Brand Impersonation

From: Norton ALERT newslettertdn@bluemooncaterers.com **Sent:** Tuesday, December 30, 2025

Subject: ⚠️ Last Notice: Your Norton Subscription Has Expired

Dear User,

Your Norton Subscription has expired on Tuesday, December 30, 2025. To protect your device and maintain your security, you must renew your subscription immediately.

Failure to renew will result in the loss of real-time protection and potential data vulnerability.

[Renew Now] Regards, Norton Security Team

Analysis Report

- **Risk Classification**: High
- **Indicator 1: Sender Mismatch**: The display name says "Norton ALERT," but the actual email address is newslettertdn@bluemooncaterers.com, which has no affiliation with the brand.
- **Indicator 2: Urgency**: High-pressure language such as "Last Notice" and "Expired" is used to trigger fear and force the user to act without thinking.

Case Study #2: Cloud Storage Service Threat

From: Cloud Storage hello@CloudStorageSecurityxyt.uk **Sent:** Saturday, November 29, 2025 **Subject:** 🔔 Billing Issue Detected — Reactivate or Lose Every File Forever

Dear Customer,

We were unable to process your most recent monthly payment. As a result, your cloud storage account has been scheduled for permanent deletion.

Impact of Deletion:

- All photos, documents, and backups will be wiped from our servers.
- Access to shared files will be revoked immediately.
- This action is **irreversible**.

To prevent the permanent loss of your data, please update your billing information now.

[Reactivate My Account]

Regards, Cloud Billing Department

Analysis Report

- **Risk Classification**: Critical
- **Indicator 1: Loss Aversion**: The attacker uses the threat of "permanent deletion" of personal photos and documents to create panic and bypass critical thinking.
- **Indicator 2: Malicious Link**: The "Reactivate My Account" button is designed to lead the user to a fake login page to steal account credentials.

Case Study #3: PayPal Financial Fraud

From: PayPal Service support-update@verification-dept-99.com **Sent:** Wednesday, January 28, 2026
Subject: ⚠️ Action Required: Your account has been limited

Dear Customer,

We have noticed some unusual activity on your PayPal account. As a security precaution, we have temporarily limited your access to send or withdraw funds.

Reference Number: PP-009-882-121

To restore your account access, we require you to confirm your identity by clicking the link below and following the on-screen instructions.

[Resolve Account Issue Now]

If this is not completed within 48 hours, your account may be permanently restricted.

Thank you, PayPal Security Team

Analysis Report

- **Risk Classification**: High
- **Indicator 1: Impersonation**: The email uses an official-looking "Reference Number" (PP-009-882-121) to build false trust with the victim.
- **Indicator 2: Deadline**: A strict 48-hour time limit is set to discourage the user from taking the time to contact official support for verification.

Prevention & Awareness Guidelines

Security Best Practices

User Action: DO

- Always check the sender's full email address for domain inconsistencies.
- Hover your mouse over all buttons and links to see the true destination URL before clicking.
- Enable Multi-Factor Authentication (MFA) on all sensitive accounts to provide an extra layer of security.

User Action: DON’T

- Do not download attachments or click links from unrecognized or suspicious senders.
- Do not enter passwords, credit card details, or OTPs on websites reached via an email link.
- Never reply to a suspicious email, as this confirms your email address is active to the attacker.