Phishing Email Analysis Report

Summary of Task

The objective of this task is to analyze a set of suspicious emails and identify common phishing traits. Each email was reviewed for indicators such as spoofed sender addresses, urgent or threatening language, malicious attachments or links, and impersonation of well-known companies.

Sample 1: Fake Debt Notice

Indicators of phishing:

- Suspicious sender email: feedbhanopor1998@answer.onlinestatusupdate.com – not a legitimate domain.
- Urgent language: 'Debt Payment Required Immediately' creates panic.
- Unusual method of communication: Debt notice shared via Google Drive is not standard practice.
- Brand misuse: 'MorganLewis®' is impersonated, unrelated domain used.

Sample 2: FedEx Delivery Scam

Indicators of phishing:

- Spoofed email address: TrackingUpdates@email-truck.com – not from official FedEx domain.
- Urgent warning: Threatens return of package if user doesn't respond.
- Generic greeting: 'Hi, Demo.' indicates bulk phishing.
- Suspicious link: Likely redirects to fake FedEx site.

Sample 3: Google Drive File Scam

Indicators of phishing:

- Suspicious sender email: goog...@protected-download.com – not a Google domain.
- Misleading and vague message: Doesn't name sender, uses generic template.
- Fake Google branding: Impersonates official UI.
- Malicious link: 'Click Here' may lead to a phishing site.

Sample 4: Netflix Password Reset Scam

Indicators of phishing:

- Fake email address: netflix@webnotifications[.]net – not associated with Netflix.
- Urgent password expiry notice: Designed to cause panic.
- Grammar issues: 'Netflix are requesting...' sounds unprofessional.
- Fake button: 'Reset Password' may redirect to a phishing website.

Common Phishing Traits Observed

- Use of spoofed or unrelated email domains.
- Urgency or scare tactics .
- Generic greetings .
- Impersonation of known brands.
- Malicious links disguised as legitimate actions.
- Poor grammar or vague messages.
- Unusual file delivery methods (e.g., Google Drive for debt notices).

Conclusion & Recommendations

The emails analyzed show clear signs of phishing attempts, including the use of fake email addresses, urgency, impersonation of trusted brands, and malicious links. Users should be cautious and trained to identify such traits. To stay safe, users should:

- Never click on links or download files from unknown senders.
- Always verify the sender's domain.
- Report suspicious emails to IT or security teams.
- Keep email software and antivirus programs updated