PHISHING EMAIL
ANALYSIS REPORT

Prepared by: Sanjeel Shrestha

IT Graduate | Cybersecurity Enthusiast

Sydney, NSW, Australia

May 2026

Cisco Introduction to Cybersecurity — Portfolio Project

Introduction

Phishing is one of the most common cyber threats, leading to the loss of personal credentials and information. This report lists down three real-world phishing emails and my analysis on them. It shows my analytical thinking on spotting fake emails and identifying the red flags that reveal their malicious intent.

Email 1 — Fake Mail Delivery Failure

Email Type: Fake mail delivery failure / Credential harvesting

Sender Address: example.com – not a legitimate mail server, unrelated to any real organization

Subject Line: “Undelivered Mail Returned to Sender” – designed to create concern

What It’s Claiming: That 7 of outgoing emails have failed to get delivered and action needs to be taken immediately.

Red Flags

- **Red Flag 1:** The sender domain is example.com — a generic placeholder domain, not a real mail server. Legitimate mail delivery failure notices come from our own mail system.
- **Red Flag 2:** Specific details with exact number of failed messages and a precise timestamp are tactics used to generate urgency and make the email look authentic.
- **Red Flag 3:** The email has two links “Review” and “Delete” – a real email would never give a delete option via mail. Both links likely lead to a malicious destination.

Attack Technique: Social Engineering – impersonating a system administrator to manipulate the recipient into clicking a malicious link without questioning it.

Potential Impact: Redirection to a credential harvesting page to steal login details, or a malware/adware download onto the device.

⚠️ **VERDICT: Phishing — Do not click any links. Report to IT security immediately.**

Email 2 — Fake Password Expiry

Email Type: Fake password expiry / Credential harvesting

Sender Address: email@example.com – not a legitimate mail server, unrelated to any real organization

Subject Line: “Password Expiration…” – generation of urgency and concern

What It's Claiming: That the user's password is about to expire in 1 day and action needs to be taken immediately.

Red Flags

- **Red Flag 1:** The recipient is addressed as "help" — this means the mail was sent in bulk without addressing individuals. Legitimate organisations always address recipients by name.
- **Red Flag 2:** "Password is set to expire in 1 day(s)" — the extremely short timeframe generates a sense of urgency, preventing the recipient from thinking critically before acting.
- **Red Flag 3:** "We won't be responsible for any information lost" highlighted in red generates fear. The statement makes the user feel responsible for any data lost, pressuring them to act immediately.
- **Red Flag 4:** "Scanned and considered safe" — tries to manufacture trust and convince the user the email is genuine. Legitimate email security scanning happens automatically and invisibly — a sender claiming their own email is safe is itself a red flag.

Attack Technique: Social Engineering – using fear, urgency, and false assurance to manipulate the recipient into clicking a malicious link without questioning it.

Potential Impact: Redirection to a credential harvesting page to steal login and password details.

⚠️ **VERDICT: Phishing — Do not click any links, especially "Keep My Password". Report to IT security immediately.**

Email 3 — Fake PayPal Transaction

Email Type: Fake PayPal transaction / Vishing attempt

Sender Address: Service Center – not a real sender. Legitimate PayPal emails come from @paypal.com, not a generic "Service Center".

Subject Line: "Order Shipped" – misleading subject unrelated to the email content

What It's Claiming: That a transaction of $769.99 has been made with the recipient's PayPal account and they must call a number to dispute it.

Red Flags

- **Red Flag 1:** The grammar in the email is incorrect with missing and inconsistent punctuation. The variation in font sizes also generates an unprofessional appearance inconsistent with legitimate PayPal communications.

- **Red Flag 2:** The email forces a phone number instead of a link. Since a phone number is linked to an individual's personal data, calling it allows the attacker to access personal information at a deeper level than clicking a link.
- **Red Flag 3:** The transaction involves Bitcoin (BTC). Bitcoin transactions are irreversible — once sent, the money cannot be recovered. The attacker chose Bitcoin specifically to reduce traceability and make themselves untraceable.

Attack Technique: Vishing (Voice Phishing) – impersonating a legitimate brand to manipulate the victim into calling a fraudulent number and surrendering personal or financial information verbally.

Potential Impact: Leaking of personal data, credentials, and potential financial loss through irreversible Bitcoin transactions.

⚠️ **VERDICT: Phishing — Do not call the number provided. Verify directly through PayPal's official website. Report to IT security immediately.**

Conclusion

All three emails analysed in this report are confirmed phishing attempts using different techniques — fake delivery failures, password expiry scares, and voice phishing. In each case, the attacker relies on social engineering to bypass rational thinking through urgency, fear, and false trust. Awareness of these techniques is the first and most important line of defence against phishing attacks.