Phishing-email report

PREPARED BY-
Hemanth.s

SAMPLE PHISHING PROGRAM

From account-security@paypa1.com
To: hemanthsh967@gmail.com
Subject: Urgent: Suspicious Activity Detected on Your PayPal Account

Dear Customer

We have detected unusual activity on your PayPal account and have temporarily limited access to it for your protection. To restore full access, please verify your identity immediately by clicking the link below:

👉 Verify Now

Failure to do so within 24 hours will result in permanent suspension of your PayPal account.

Thank you for your prompt attention to this matter.

Sincerely,
PayPal Security Team
account-security@paypa1.com

POINTS TO ANALYSE

1. Spoofed sender: @paypa1.com instead of @paypal.com (notice the number “1” instead of letter “l”).
2. Urgent language: “Suspicious activity,” “temporarily limited,” “permanent suspension.”
3. Suspicious link: Hover reveals http://paypa1-verify.com/login – not an official PayPal domain.
4. Generic greeting: “Dear Customer” instead of using your real name.
5. Grammar: Generally decent, but that’s common in newer phishing attempts.

1. Sender's Email Address:

Appears as support@paypalsecurity.com (not the official @paypal.com domain).
This is a spoofed email meant to look like PayPal.

2. Email Header Analysis:

Used an online header analyzer (e.g., MxToolbox).
Discrepancy Found: The "Received From" IP is from an unknown server in another country, not a PayPal mail server.
SPF/DKIM/DMARC failed, indicating the sender may not be authorized to send emails on behalf of PayPal.

3. Suspicious Links/Attachments:

Contains a button labeled “Reactivate Account”.
On hover, the link points to http://paypalsecurity-alerts.ru/confirm, not the official PayPal site.
This is a malicious URL using a lookalike domain.

4. Urgent/Threatening Language:

Phrases such as:
“Your account will be permanently suspended within 24 hours.”
“Immediate action is required.”
These are common social engineering tactics to create panic and push the user to act quickly.

5. Mismatched URLs:

Visible text: “https://paypal.com/login”
Actual link: http://paypalsecurity-alerts.ru/confirm

6. Grammar/Spelling Errors:

- Examples:
  - “Your acount has been suspended”
  - “Click bellow to verify”
- Poor language quality is a common red flag.

SUMMARY

1. Spoofed email address
2. Header discrepancies and failed authentication
3. Suspicious, mismatched URLs
4. Threatening/urgent language
5. Poor grammar and spelling
6. Fake login page to harvest credentials

THANK YOU