Task 2 - Phishing Email Analysis

Sample Email Content

From: support@paypa1.com

Subject: Immediate Action Required: Your Account is Locked

Dear User,

Your PayPal account has been temporarily locked due to suspicious activity.

To unlock your account, please click the link below and verify your details:

http://paypal.account-verify.ru

Failure to act within 24 hours will result in permanent suspension.

Regards,

PayPal Security Team

Phishing Indicators Identified

1. Spoofed Sender Address:

   - 'support@paypa1.com' uses number '1' instead of letter 'l'.

2. Fake URL:

   - Link points to '.ru' domain unrelated to PayPal.

3. Urgent Language:

   - Phrases like 'Immediate Action Required' cause panic.

4. Grammar Issues:

- Minor grammar errors present.

5. Email Header Issues:

- Return-path or SPF/DKIM header mismatch (if analyzed).

6. Branding:

- No official PayPal logo or footer; appears unprofessional.

Summary

This email uses urgency, spoofed sender, and fake URLs to trick users.

It demonstrates how phishing relies on social engineering and fear.

Tools Used

- MXToolbox Email Header Analyzer
- Link Hovering in Browser
- Visual Inspection

Conclusion

This task highlights how attackers exploit email systems for phishing.

Learning to recognize these signs is critical in cybersecurity.