

Task no: 2

❑ Phishing Email Analysis Report

- ❑ **Subject:** Urgent: Your Account Will Be Suspended!
 - ❑ **Sender:** support@paypal.com (*spoofed domain*)
 - ❑ **Reply-To:** help@fakeupdate.ru (*does not match sender*)
-

❑ Analysis Details

1. Sender Email Address:

- The domain `paypal.com` is trying to look like `paypal.com` using the number “1” instead of the letter “l”.
- This is a classic spoofing technique.

2. Email Header Analysis:

- Header shows email came from an unknown mail server not associated with PayPal.
- Return-path and Reply-To go to a suspicious `.ru` domain.

3. Suspicious Links:

- Displayed link: `https://paypal.com/login`
- Actual link (on hover): `http://scam-alert.ru/paypal/verify`
- This mismatch is a phishing trick.

4. Urgent or Threatening Language:

- "Your account will be suspended within 24 hours unless you verify now!"
- Tries to scare the user into clicking.

5. Grammar & Spelling Errors:

- “We detecting unusual activitys.”
- “Please click hear to secure it.”

6. Attachments:

- File named `Account_Security_Update.zip` — unexpected and potentially malicious.
-

□ **Conclusion:**

This email is a **phishing attack**. It shows multiple indicators:

- Spoofed sender address
- Mismatched links
- Urgent, threatening tone
- Grammar errors
- Malicious-looking attachment

□ **Never click links or download files from such emails.**