**Phishing Analysis Report 🕵️**

**Email Subject:** "Urgent Action Required: Your Account Has Been Compromised"

**1. Sender's Email Address 📧**

I noticed the sender's address was **"support@paypal-security.info"**, which immediately looked suspicious to me. I know that a real PayPal email would come from an official domain, so the use of "paypal-security" in a different domain (.info) was my first red flag. This is a classic example of **domain spoofing**.

**2. Email Headers 📋**

When I examined the full email headers, I saw some major discrepancies. The Return-Path and Received headers showed me that the email originated from a server in a different country, like **Russia** or **China**. This didn't match PayPal's corporate network, which told me the email was from a malicious source.

**3. Suspicious Links and URLs 🔗**

Inside the email, I found a button that said, "Verify Your Account Now." I made sure to **hover my cursor over the link** to see the real URL. The link pointed to **"**[**http://192.168.1.10/verify\_account.html**](https://www.google.com/search?q=http://192.168.1.10/verify_account.html&authuser=3)**,"** not a legitimate PayPal address. The use of an internal IP address or an unrelated domain made it clear to me that this was a phishing attempt.

**4. Urgent and Threatening Language ⚠️**

I felt the pressure right away from the subject line and the email body. The phrases **"Urgent Action Required"** and **"Your account will be suspended within 24 hours"** were designed to make me panic and act without thinking. This is a common social engineering tactic I've seen before.

**5. Spelling and Grammar Errors ✍️**

I spotted several grammatical errors, such as **"We have detected a unathorized login"** and **"your account is in risk."** I know that official communications from large companies don't usually have these kinds of mistakes, so these errors were a key giveaway for me.

**Summary of Phishing Indicators**

Based on my analysis, I found multiple signs of a phishing attack:

* **Spoofed Domain**: The sender's email address didn't match the official company domain.
* **Suspicious Headers**: The email's origin was inconsistent with the claimed sender.
* **Mismatched URLs**: The link text hid a malicious or incorrect destination.
* **Social Engineering**: The email used a sense of **urgency and fear** to manipulate me.
* **Poor Language**: The presence of **spelling and grammar errors** made it feel fake.

