Elevate Labs

From: PayPal Security <support@paypalsecure.com>

To: [Your Email]

Subject: Urgent: Unusual Login Activity Detected – Action Required Immediately

Dear Customer,

We have detected **suspicious activity** on your PayPal account and temporarily limited your access for your security.

Location: Moscow, Russia

IP Address: 189.224.34.101

Time: 02:46 AM GMT

To restore full access to your account, please verify your information by clicking the secure link below:

[Verify Now] (http://paypal-verification-center.com/login)

If you do not complete the verification within **24 hours**, your account will be **permanently suspended**.

We apologize for the inconvenience and appreciate your prompt attention to this matter.

Sincerely,

PayPal Security Team

support@paypalsecure.com

This email was sent from an unmonitored mailbox. Do not reply to this message.

Identified Phishing Indicators:

Indicator	Description
Spoofed Sender Address	The sender email is support@paypalsecure.com, which looks similar to PayPal but is a fake domain (real PayPal domain is paypal.com).
Suspicious URL	The verification link appears legitimate but redirects to http://paypal-verification-center.com, which is a fraudulent site designed to steal credentials.
Urgency and Threat	The email uses scare tactics like "permanently suspended" and gives a tight deadline of "24 hours" to pressure the user into quick action.
Grammatical/Stylistic Issues	Some formatting inconsistencies and awkward phrasing (e.g., "Action Required Immediately") are typical of phishing messages.
Generic Greeting	Uses "Dear Customer" instead of addressing the recipient by name, which is common in mass phishing campaigns.
Unusual Location Mentioned	The IP and location (Moscow, Russia) are used to alarm the user and increase trust in the fake alert.
No Personal Information	Real companies usually reference some part of your account info (e.g., your name, last four digits, etc.)—this email doesn't.
No Reply Disclaimer	"Do not reply to this message" adds to the impersonation and discourages users from questioning its legitimacy.

SPF and DKIM Information (Using MXToolBox for Header Analysis)

Headers Found

Header Name	Header Value
From	PayPal Security <support@paypalsecure.com>
To	[Your Email]
Subject	Urgent: Unusual Login Activity Detected – Action Required Immediately

Step-by-Step Header Analysis

Field	What It Tells Us	Phishing Indicator?
Return-Path	support@paypalsecure.com is trying to spoof PayPal. Real domain should be paypal.com.	Yes – **Spoofed domain**
Received	Email was sent via fake-smtp.com with IP 185.199.108.153. Not a trusted PayPal mail server.	Yes – **Untrusted origin**
Received-SPF	Shows **SPF failed** – domain didn't authorize this IP to send mail.	Yes – **Authentication failure**
Authentication-Results	Both **DKIM** and **DMARC** failed. Message is **not from a verified source**.	Yes – **Spoofing confirmed**

Message-ID	Looks autogenerated. Format is okay, but not proof of legitimacy.	Possibly suspicious if inconsistent with other fields.
Reply-To	Goes to paypal-fraud-help.com (another fake domain), **not** PayPal.	Yes – **Redirects replies to attacker**
From:	Again shows support@paypalsecure.com — matches the spoof.	Yes – **Impersonation**
Date:	Can be checked against real-time for inconsistencies, but here looks normal.	No
To:	Standard — your email address.	No