Subject: **Your PayPal Account Will Be Suspended!**  
From: **PayPal Support support@paypalsecurity-update.com**  
Body:

Dear Customer,

We have detected suspicious activity in your PayPal account. For your security, we have placed a temporary hold on your account. If you do not verify your identity within 24 hours, your account will be permanently suspended.

Click the link below to confirm your details and restore access:  
https://paypal.secure-login-update.com

header

Return-Path: <support@paypalsecurity-update.com>

Received: from mail.fakehost.ru (mail.fakehost.ru. [203.0.113.45])

by mx.google.com with ESMTP id a1csp987654qka;

Thu, 28 Aug 2025 09:22:34 -0700 (PDT)

Authentication-Results: mx.google.com;

spf=fail (google.com: domain of support@paypalsecurity-update.com does not designate 203.0.113.45 as permitted sender) smtp.mailfrom=support@paypalsecurity-update.com;

dkim=fail header.i=@paypalsecurity-update.com;

dmarc=fail (p=REJECT sp=REJECT dis=NONE) header.from=paypalsecurity-update.com

Received-SPF: fail (google.com: domain of support@paypalsecurity-update.com does not designate 203.0.113.45 as permitted sender) client-ip=203.0.113.45;

From: "PayPal Support" <support@paypalsecurity-update.com>

Reply-To: scammerhelpdesk@gmail.com

To: victim@example.com

Subject: Your PayPal Account Will Be Suspended!

Date: Thu, 28 Aug 2025 09:21:55 -0700

MIME-Version: 1.0

Content-Type: text/html; charset=UTF-8

Message-ID: <1234567890@mail.fakehost.ru>

<html>

<body style="font-family:Arial, sans-serif;">

<p>Dear Customer,</p>

<p>We have detected suspicious activity in your PayPal account. For your security, we have placed a temporary hold on your account.

If you do not verify your identity within <b>24 hours</b>, your account will be permanently suspended.</p>

<p>Please confirm your details by clicking the secure link below:</p>

<p><a href="http://paypal.secure-login-update.com/verify">https://www.paypal.com/verify</a></p>

<p>Thank you for your prompt attention,<br>

PayPal Security Team</p>

</body>

</html>

**Final Report Phishing Indicators Found**

1. **Spoofed Sender Address** – not from official domain (@paypal.com).
2. **Suspicious Links** – domain mismatch, leads to fake login page.
3. **Urgent/Threatening Language** – pushes immediate action (24-hour deadline).
4. **Email Header Discrepancies** – failed SPF/DKIM authentication.
5. **Grammar Errors** – poor wording, unprofessional tone.
6. **Generic Greeting** – “Dear Customer” instead of user’s real name.
7. **Possible Credential Theft Attempt** – fake login page link.