

Phishing Email Analysis Report

Subject of Email: Your Account is Suspended!

Sender Address: PayPal <support@secure-paypal.com>

Link in Email: <https://paypal-secure-login.com/verify>

Phishing Indicators Found:

- **Spoofed Email Address:** The sender email (secure-paypal.com) is not the official domain (paypal.com).
- **Suspicious Link:** The embedded link looks like PayPal but redirects to a phishing site (paypal-secure-login.com).
- **Mismatched URLs:** Hovering over the link reveals a different domain than expected.
- **Urgent/Threatening Language:** The message pressures the user to act within 24 hours or face suspension.
- **No Personalization:** Email uses 'Dear Customer' instead of your real name—common phishing trait.
- **Email Header Discrepancies:** SPF/DKIM authentication failed or was missing. IP address does not match official PayPal servers.

Conclusion:

This email is a phishing attempt designed to trick the user into clicking a malicious link and revealing sensitive information. It uses urgency, spoofed domains, and fake branding to appear legitimate. Users must verify sender domains and never click suspicious links.

■ Example Phishing Email (Gmail Sample)

Subject: Your Account is Suspended!

From: PayPal

Dear Customer,

We noticed suspicious activity in your PayPal account. Your account has been temporarily suspended to protect your information.

To reactivate your account, please click the link below:

<https://paypal-secure-login.com/verify>

Failure to do so within 24 hours will result in permanent suspension.

Sincerely,

PayPal Security Team

Anshul pal | Cybersecurity Intern | August 2025