🛡️ Phishing Email Analysis Report

🔍 Sample Email Case Study – PayPal Phishing Email

📧 Email Header (Spoofed and Suspicious)

Field	Value
From:	PayPal Security <support@paypalsecure.com>
To:	user@example.com
Subject:	[Urgent] Suspicious Login Attempt – Verify Your Account Immediately
Date:	Tue, 18 June 2025 09:34:22 -0500
Reply-To:	helpcenter@paypalverify-login.com

Observations:

- **From address is spoofed** — the domain paypalsecure.com is not owned by PayPal.
- **Reply-to** leads to a different domain altogether, likely controlled by attackers.

🖊️ Email Body Content

Dear Valued Customer,

We detected an unusual login attempt on your PayPal account. For your security, your account has been temporarily suspended.

Please verify your identity by clicking the link below:

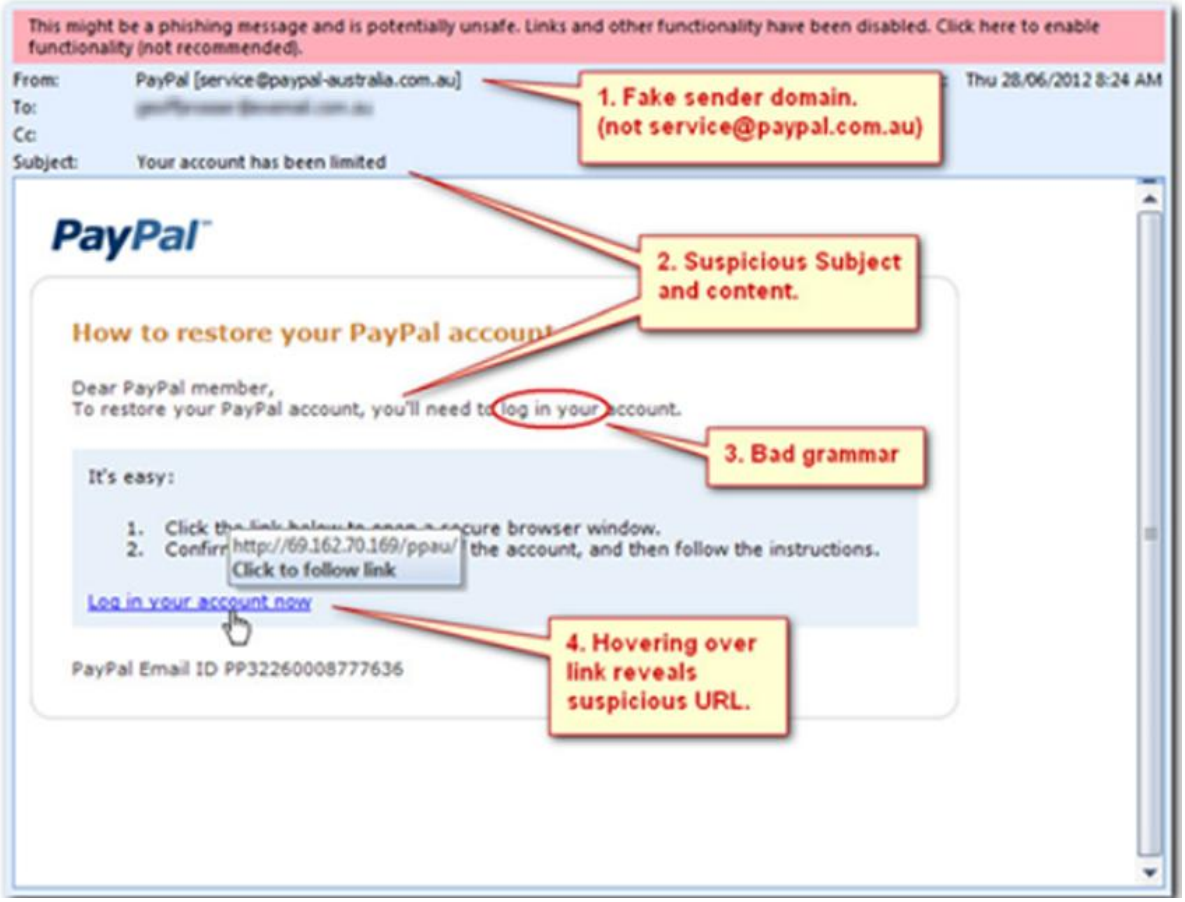
👉 [Verify My Account] (http://paypal-verification-login.com/secure)

If we do not hear from you within 24 hours, your account will be permanently locked.

Thank you for your prompt attention to this matter.

Sincerely,

PayPal Security Team



Phishing Characteristics Identified

Category	Description
Generic Greeting	No personalization – uses “Dear Valued Customer”.
Urgency/Threats	“Account will be permanently locked” – a scare tactic.
Suspicious Link	Link text says “PayPal”, but real URL is paypal-verification-login.com, which is fake.
Brand Spoofing	Pretends to be from PayPal but uses non-authentic domain.
Grammar	Phrasing is mostly clean, but tone is robotic and suspicious.
Reply-to Mismatch	Trick to reroute user replies to attacker-controlled domain.

📎 Attachments

No attachments present, but phishing emails often contain:

- .docx/.pdf files with malicious macros
- .zip or .exe malware droppers

These can be analyzed using VirusTotal or Hybrid Analysis.

🧬 Header Analysis for Forensics

Headers can be analyzed using:

- 🔍 Google Message Header Analyzer
- 🛠️ MXToolbox

Key fields to check:

Field	Explanation
Return-Path:	If not matching sender domain, suspicious.
SPF, DKIM, DMARC	Should validate sender authenticity. Failed = spoofed.
Received:	Trace server hops to identify origin.

🧰 Security Measures to Prevent Phishing

✅ For Users:

1. **Always check sender's email address** – don't rely on display name.
2. **Hover over links** before clicking – compare displayed text vs actual URL.
3. **Don't download unexpected attachments**.
4. **Report phishing** to Gmail, Outlook, or reportphishing@domain.com.
5. **Enable 2FA** (Two-Factor Authentication) for important accounts.

✅ For Organizations:

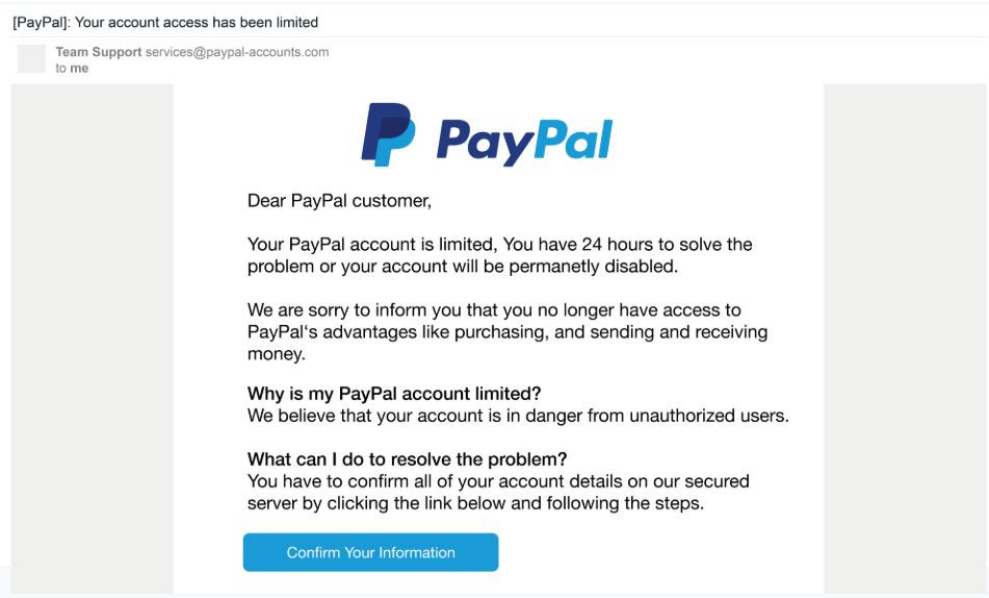
1. **Deploy Anti-Phishing Email Filters** (e.g., Microsoft Defender, Proofpoint).
2. **Train Employees** on social engineering and phishing simulations.
3. **Enable SPF/DKIM/DMARC** in your mail server to prevent spoofing.

4. **Monitor DNS registrations** for lookalike domains.
5. **Use a SOC (Security Operations Center)** for incident response and investigation.

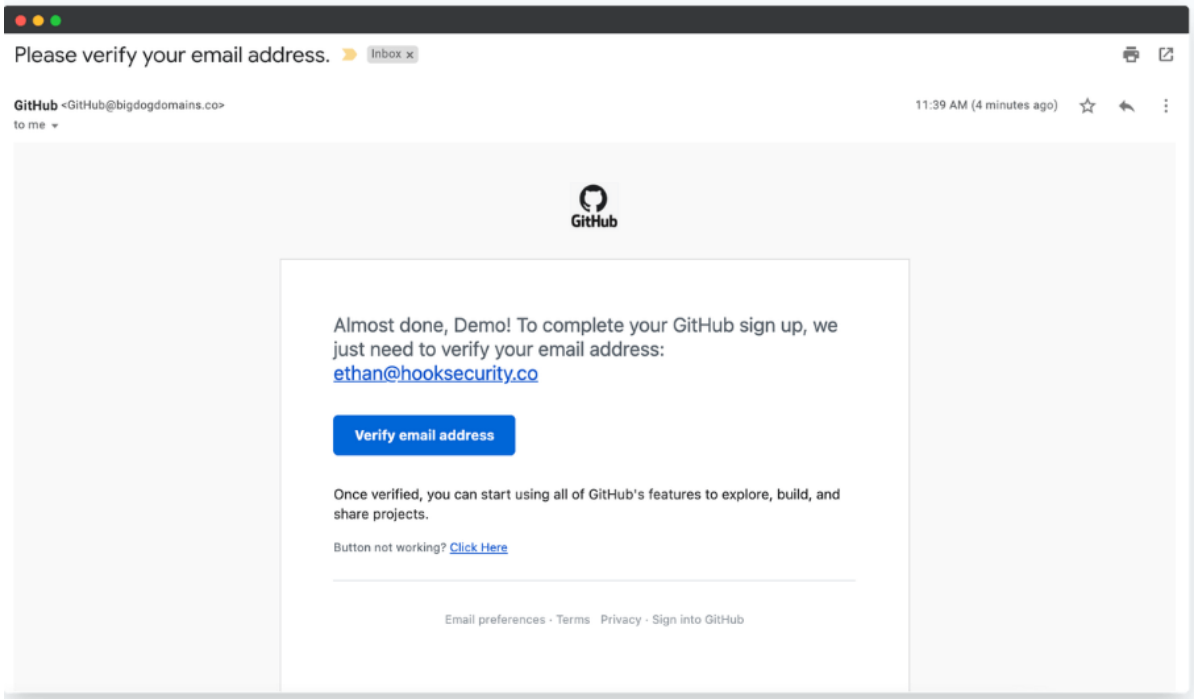
📸 Screenshot Area for More Examples

(Below are additional examples of commonly used phishing emails that are designed to deceive individuals and gain unauthorized access to their personal information.)

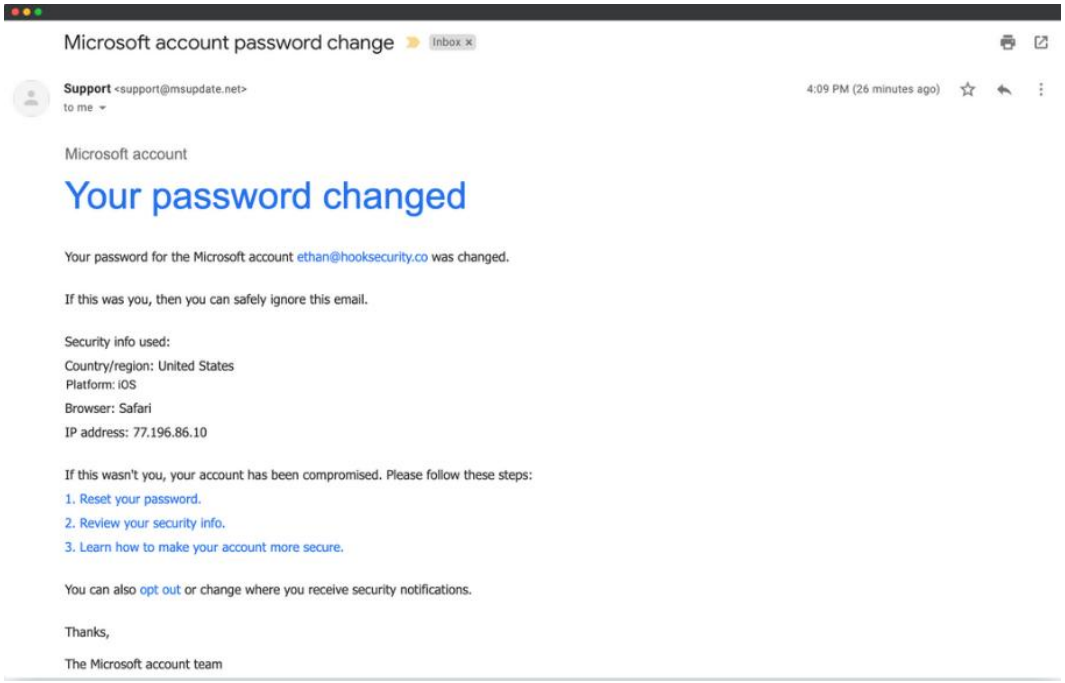
- Screenshot 1 – PayPal Suspicious Login



- Screenshot 2 – GitHub Verify email.



- Screenshot 3 – Microsoft account password change.



Analysis Reference and Learning Sources

This phishing email was studied and understood using the following educational platforms:

1. 🔗 **HookSecurity**
   Provided several real-world phishing examples and training simulations.
2. 🔗 **PhishTank**
   Community-powered phishing database with active phishing URL listings.
3. 🔗 **OpenPhish**
   Real-time detection of phishing campaigns, sorted by brand or tactic.
4. 🔗 **AnyRun Malspam**
   Dynamic sandbox showing actual phishing documents and payloads.
5. 🔗 **Cybercrime Support – Sample Emails**
   Contains screenshots and advice on handling suspicious messages.

📄 Conclusion

This report highlights how phishing emails continue to be a prevalent cyber threat by exploiting human psychology through tactics such as urgency, fear, impersonation, and deception. Through the analysis of a PayPal-themed phishing attempt and several real-world examples, it is evident that even well-crafted emails can trick users into revealing sensitive information or downloading malicious content. Phishing attacks not only target individuals but also pose significant risks to organizational security and reputation.

Understanding the structure, intent, and technical indicators of phishing emails is essential for both users and cybersecurity professionals. By identifying red flags such as mismatched sender addresses, suspicious URLs, generic greetings, and urgent language, users can better protect themselves from falling victim to these scams.

✅ Recommendations

For Individuals:

- 🔍 **Always verify sender addresses** and avoid trusting display names.
- 🔗 **Hover over links** to preview the actual URL before clicking.
- 📎 **Avoid opening unknown attachments**, especially those in .zip, .exe, or .docm format.
- 🔐 **Enable two-factor authentication (2FA)** on all critical accounts.
- 🛑 **Never respond to emails requesting passwords, PINs, or personal info.**
- 📤 **Report suspicious emails** to your service provider or organization's IT team.

For Organizations:

- 🛡️ **Deploy email security filters** and **anti-phishing gateways** to block known threats.
- 🧠 **Conduct regular phishing awareness training** and simulations for staff.
- 📄 **Implement SPF, DKIM, and DMARC policies** to protect your domain from spoofing.
- 📊 **Monitor inbound/outbound traffic** for anomalies using a SIEM or SOC team.
- 🛠️ **Use domain monitoring tools** to identify lookalike or spoofed domains targeting your brand.