Email Analysis Report

1. Overview

This report analyses a sample phishing email to identify red flags and recommend best practices for avoiding email-based attacks. Phishing remains one of the most common and effective cyberattacks, where attackers impersonate trusted entities to steal credentials, deliver malware, or commit fraud. 2. Sample Email Summary

2. Sample Email Summary

From: support@paypa1.com

Subject: Urgent: Account Suspension Notice Received Date: 2025-05-15 09:32 UTC

Email Body (excerpt):

Dear Customer,

We detected unusual activity on your PayPal account. Please verify your account within 24 hours to avoid suspension.

Click here to verify: http://paypa1.verify-security.com/login

Failure to do so will result in permanent account suspension.

Regards,

PayPal Support Team

3. Red Flags and Indicators of Phishing Indicator Explanation Sender's Email Address support@paypa1.com uses a number "1" instead of letter "l" in "paypal" — a common spoofing trick. Urgency and Threat The email creates a false sense of urgency with threats of account suspension. Suspicious URL The link points to paypa1.verify-security.com, which is unrelated to the official PayPal domain. Generic Greeting Uses "Dear Customer" instead of your real name, indicating bulk phishing attempt. Grammar and Formatting Slightly off grammar and unusual phrasing typical in phishing emails. Unsolicited Request Requests immediate verification via link, which reputable companies avoid via email.

4. Technical Analysis

- **Domain analysis:** The domain verify-security.com is newly registered and not affiliated with PayPal.
- **URL redirection:** The link masks the true destination using subdomains and deceptive naming.
- **Email header inspection:** The email originates from an IP address outside PayPal's known mail servers.

- **No SPF/DKIM/DMARC validation**: The sender fails authentication protocols, increasing phishing risk.

5. Potential Risks

- **Credential Theft:** If the user clicks the link and enters login info, attackers capture credentials.
- **Malware Installation:** The link may deliver malware or ransomware payloads.
- **Financial Loss:** Attackers can gain access to linked accounts for fraud or theft.
- **Identity Theft:** Personal info could be harvested for identity fraud.

6. Recommendations to Avoid Such Attacks

User Awareness

- Always verify the sender's email address carefully, especially for small spelling differences.
- Never click on links from unsolicited or suspicious emails.
- Hover over links to see actual URLs before clicking.
- Beware of emails creating a sense of urgency or threats.
- Look for personalized greetings instead of generic ones.

Technical Controls

- Implement and enforce email authentication protocols: SPF, DKIM, and DMARC.
- Use email filtering solutions with phishing detection and quarantine.
- Enable multi-factor authentication (MFA) on all sensitive accounts.
- Educate employees regularly on phishing recognition and reporting.

7. Conclusion

Phishing emails like the analyzed example remain a significant threat due to their deceptive nature and psychological manipulation. A combined approach of user vigilance and technical defenses is essential to prevent successful phishing attacks and protect sensitive information.