Phishing Email Analysis Report

Name : Teljeeru Akhil

Date: September 23, 2025

Subject: Phishing Characteristics Assessment — Example Suspicious Email

1. Executive Summary

An example suspicious email claiming to be from “PayPal” was analyzed. The sample contains multiple high-confidence phishing indicators: a spoofed sender address, failed/absent email authentication (SPF/DKIM/DMARC), mismatched visible vs. actual URLs, an executable/archived attachment, urgent/pressure language, and spelling/grammar errors. The email is malicious and should be treated as phishing. Immediate reporting and blocking are recommended; recipients must not click links or open attachments.

2. Tools / Methodology Used

- Email client (viewed rendered message and raw source)
- Online header inspection (manual analysis of header fields)
- Manual link inspection (hover, compare displayed URL vs. href)
- Attachment type check (filename + extension)
- Content and language review

3. Sample Email (Rendered for Analysis)

From: PayPal Support <support@paypal-secure.com>
To: employee@company.com
Subject: URGENT: Your PayPal account will be suspended — Verify Now
Date: Mon, 22 Sep 2025 08:14:02 +0000

Body (abridged):
Dear Customer,

We detected suspicious activity on your account and must verify your information to avoid immediate suspension. Please verify your account within 24 hours or your account will be permanently limited.

Verify your account now: https://www.paypal.com/verify

Or download and open the attached invoice to confirm.

Regards,
PayPal Security Team

Attachment: Invoice_0922.zip

4. Technical Header Summary (Sample Excerpts)

Received: from unknown (HELO webmail) (198.51.100.23) by mx.company.com with SMTP; 22 Sep 2025 08:14:02 +0000
From: "PayPal Support" <support@paypal-secure.com>
Return-Path: return@198.51.100.23
Received-SPF: fail (client-ip=198.51.100.23; envelope-from=support@paypal-secure.com)
Authentication-Results: mx.company.com; dkim=none; spf=fail; dmarc=none

5. Indicators of Phishing (Detailed Findings)

5.1 Sender / Identity: Spoofed domain (paypal-secure.com vs legitimate paypal.com).

5.2 Authentication / Headers: SPF failed, no DKIM, no DMARC.

5.3 Links: Displayed PayPal link vs. actual IP-based redirect (198.51.100.23).

5.4 Attachments: Invoice_0922.zip likely contains malware.

5.5 Content: Urgent tone, spelling/grammar issues, generic greeting.

6. Indicators of Compromise (IOCs)

- Attacker domain: paypal-secure.com
- Originating IP: 198.51.100.23
- Malicious link: http://198.51.100.23/verify?uid=abc123
- Attachment: Invoice_0922.zip
- Subject: URGENT: Your PayPal account will be suspended — Verify Now

7. Risk Assessment

Likelihood of compromise: High
Impact: High — Credential theft or malware deployment likely.

8. Recommendations / Remediation Steps

Immediate actions:
1. Do not click links or open attachments.
2. Quarantine and report email.

3. Block domain and IP.
4. Add IOCs to detection systems.
5. Remove email from all inboxes.

Follow-up:
6. Scan affected machines.
7. Reset passwords if exposed.
8. Notify employees of phishing attempt.
9. Update spam filters.
10. Document in incident log.

9. Suggested User Education Blurb

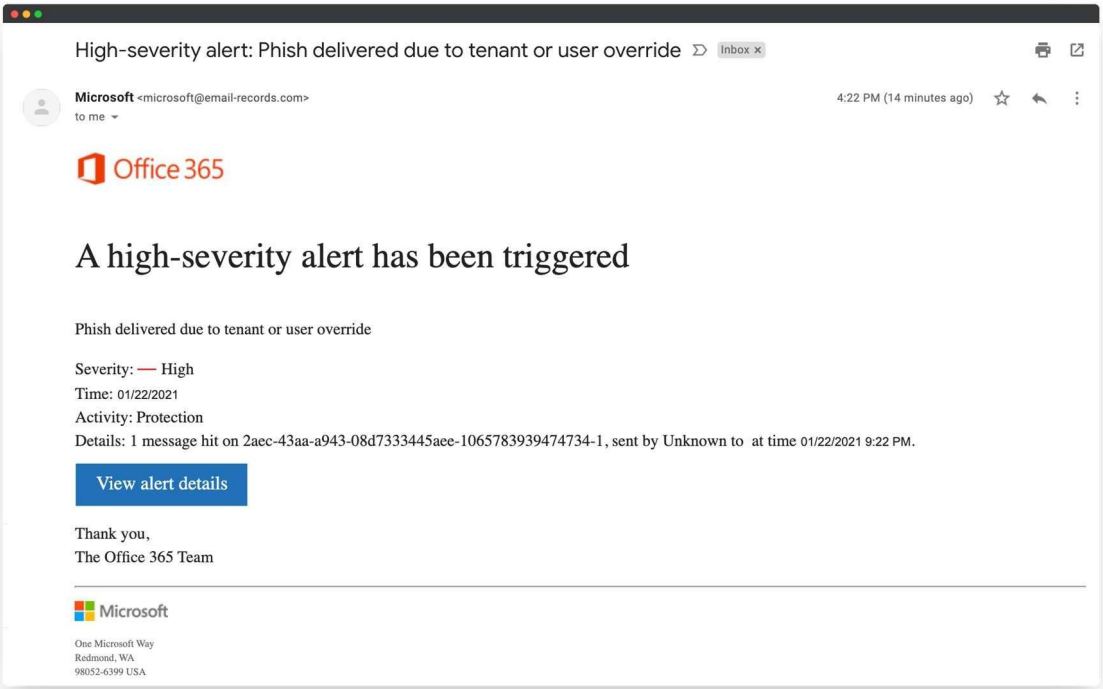
"Phishing Alert: An email impersonating PayPal is malicious. Do NOT click links or open attachments. Report suspicious emails immediately to security@company.com."

10. Conclusion

The examined email demonstrates multiple phishing indicators (spoofed sender, failed authentication, mismatched links, malicious attachment, urgency). It is confirmed as phishing and must be handled as a high-priority threat.

The main **learning outcome** :

1. **Awareness of phishing tactics:**
    - Recognize common phishing strategies such as spoofed sender addresses, urgent or threatening messages, mismatched URLs, suspicious attachments, and poor grammar or spelling.
    - Understand the psychological techniques attackers use to manipulate recipients into taking immediate action.
2. **Email threat analysis skills:**
    - Inspect email headers for authentication failures (SPF, DKIM, DMARC).
    - Identify and evaluate suspicious links and attachments safely.
    - Summarize and document phishing indicators clearly for reporting purposes.
    - Make informed recommendations to prevent compromise and educate users.



This email is a **phishing attempt**. Here's a detailed breakdown of red flags that prove it:

---

1. Suspicious Sender Email

- The email is from microsoft@email-records.com.
- Legitimate Microsoft emails come from @microsoft.com or @office.com, not email-records.com.
- This is a classic sign of phishing: the sender tries to appear official but uses a fake domain.

---

2. Urgency and Fear Tactics

- Subject: *"High-severity alert: Phish delivered due to tenant or user override"*
- Content uses phrases like "high-severity alert" to panic the user into clicking the link.
- Phishing emails often try to create a sense of urgency.

---

3. Generic Greetings

- The email doesn't address you by name; it just says *"to me"*.
- Legitimate alerts from Microsoft usually include your account name or organization.

---

4. Suspicious Links

- The "View alert details" button is a classic phishing tactic.
- Hovering over it (without clicking) likely shows a URL that **does not go to Microsoft**.
- Phishing links usually redirect to malicious websites to steal login credentials.

---

5. Inconsistent Formatting & Errors

- The email contains awkward phrasing: *"sent by Unknown to at time…"*.
- Legitimate Microsoft emails are professionally formatted and free of such grammatical mistakes.

---

6. Unnecessary Details

- It provides a long message ID and time, which is unusual for normal Microsoft alerts.
- Phishers often include technical-looking details to make the email appear authentic.

---

7. **Conclusion**

- **Do not click any links or download attachments.**
- Report it to your IT/security team.
- If in doubt, log in directly to your Office 365 account from a browser (not via the email) to check alerts.
