PHISHING DETECTION & AWARENESS REPORT

Q4 2026 EDITION

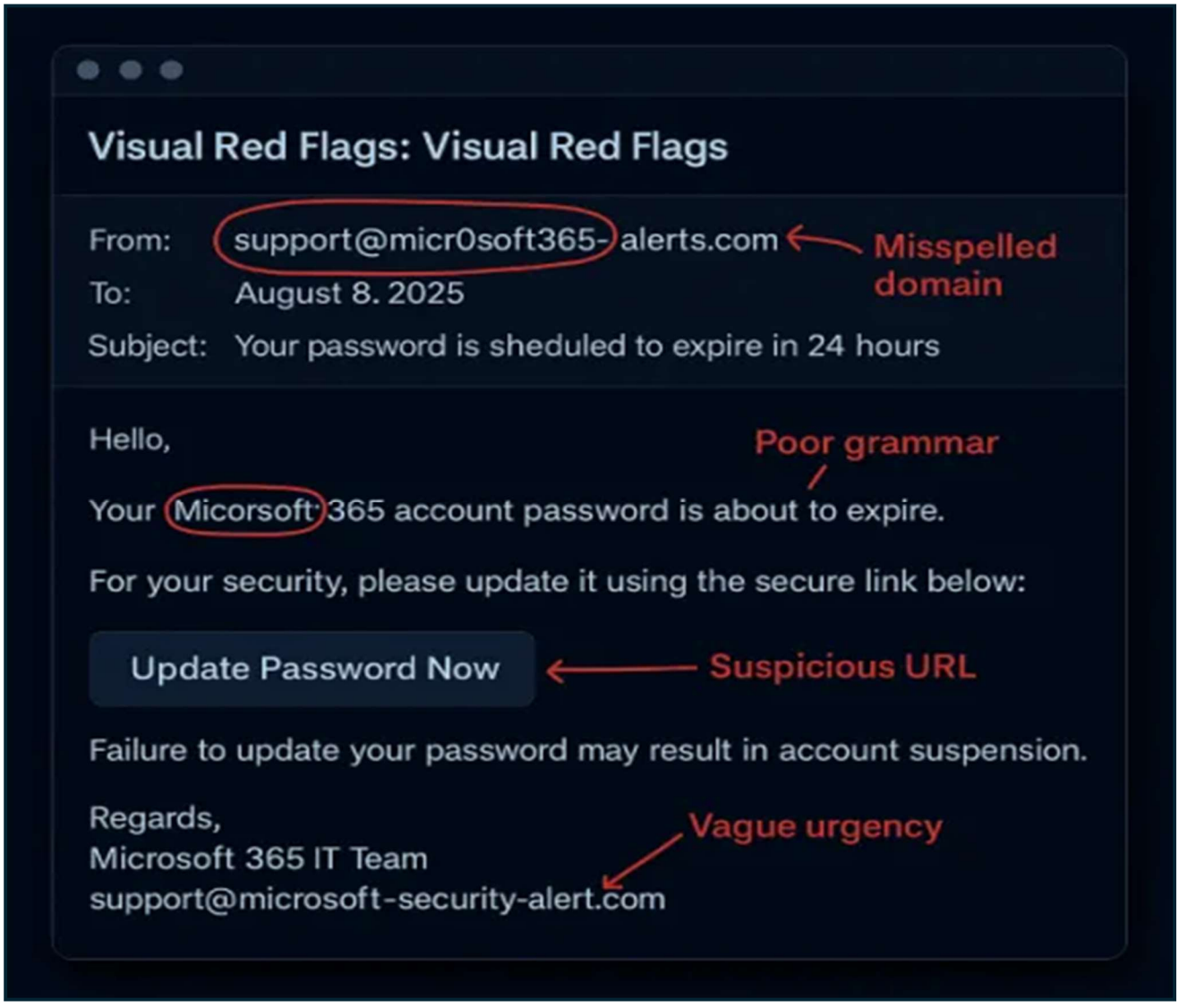
Submitted By: Shailesh Kumar

Executive Summary

This report analyzes a suspicious email claiming to be from **Microsoft 365 Security** that warns the recipient about an imminent password expiration. The investigation reveals that the email is a **high-risk phishing attempt** designed to deceive users into disclosing their login credentials.

Multiple phishing indicators were identified, including a **misspelled sender domain**, **urgent and threatening language**, a **suspicious password update link**, and **unprofessional grammar**. The email attempts to create panic by giving a short deadline and falsely claims that account suspension will occur if immediate action is not taken.

The attack follows a common **credential-harvesting technique**, where users are redirected to a fake Microsoft login page controlled by attackers. If credentials are submitted, attackers can gain unauthorized access to corporate email accounts, potentially leading to data breaches, internal phishing campaigns, and financial or reputational damage to the organization.



Identification of Phishing Indicators

The analyzed email contains multiple **high-confidence phishing indicators**, as listed below:

a) Spoofed / Misspelled Sender Domain

- Legitimate Microsoft domains end with @microsoft.com
- The sender domain microsof365-alerts.com is **misspelled and fraudulent**, designed to trick users visually.

b) Sense of Urgency

- Phrases like *"expire in 24 hours"* and *"account suspension"* pressure the user into acting quickly without verification.

c) Suspicious Call-to-Action (CTA)

- Button: **"Update Password Now"**
- The actual destination URL is unknown and likely leads to a phishing website.

d) Poor Grammar & Formatting

- Unprofessional language and awkward phrasing are common in phishing emails and not typical of official Microsoft communications.

e) Generic Greeting

- The email does not address the recipient by name, which is unusual for legitimate corporate security emails.

f) Fake IT Signature

- Claims to be from *"Microsoft 365 IT Team"* without verifiable contact details.

Email Risk Classification

🟥 **Classification: PHISHING (High Risk)**

This email is a **credential-harvesting phishing attack** intended to steal Microsoft 365 login credentials.

How the Attack Works (Simple Explanation)

1. The attacker sends a fake security alert email pretending to be Microsoft.
2. The email creates panic by claiming the password will expire soon.
3. The victim clicks the malicious link.
4. A fake Microsoft login page appears.
5. If credentials are entered:
    - Username and password are sent directly to the attacker.
6. The attacker can then:
    - Access corporate email
    - Launch internal phishing
    - Steal sensitive company data

Prevention Tips for Users

- Always check the sender's email domain carefully
- Hover over links before clicking to verify the real URL
- Remember: Microsoft never asks for passwords via email
- Use Multi-Factor Authentication (MFA) on all accounts
- Report suspicious emails immediately to the IT/Security team

Do's and Don'ts for Employees

✅ Do's

- ✓ Verify alerts by logging in directly at https://portal.office.com
- ✓ Report phishing emails using the "Report Phishing" option
- ✓ Delete suspicious emails immediately
- ✓ Keep systems and browsers updated

❌ Don'ts

- ❌ Do NOT click links in urgent security emails
- ❌ Do NOT download attachments from unknown senders

- ❌ Do NOT enter credentials on pages reached via email links
- ❌ Do NOT ignore suspicious emails — reporting helps protect others

Final Conclusion

This email is a **clear phishing attempt** using brand impersonation, urgency, and fake security messaging to steal user credentials.
Immediate deletion and reporting is strongly recommended.