COSC 34122

Phishing Simulation & Response Plan

PS/2021/103
K.G.R. KAVEESHA

1. **Phishing Email Example**

Subject: *Password Expiry Notice – Action Required Immediately*

From: IT Support it-helpdesk@secure-it-support.com

Message:

Dear User,

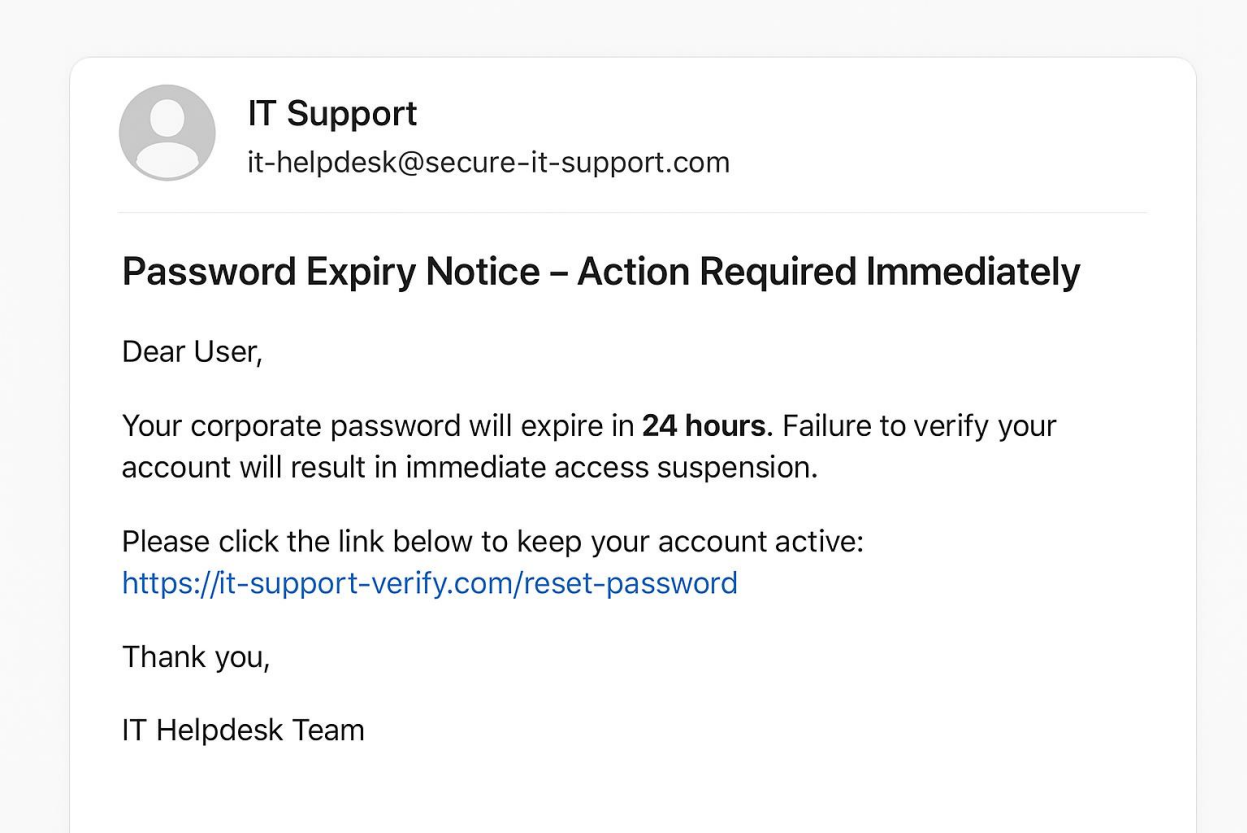
Your corporate password will expire in **24 hours**. Failure to verify your account will result in immediate access suspension.

Please click the link below to keep your account active:

https://it-support-verify.com/reset-password

Thank you,

IT Helpdesk Team



2. Identify Red Flags

Red Flag	Description	Risk Level
Urgent / Fear Tactic	Message threatens account suspension within 24 hours to induce panic clicking.	High
Suspicious Sender Domain	"secure it support.com" does not match the organization's real domain.	High
Generic Greeting	Uses "Dear User" instead of recipient's name.	Medium
Fake Reset Link	URL "it support-verify.com" does not match real corporate IT domain; resembles a credential harvesting site.	High
Grammar/Formatting Errors	Minor issues such as inconsistent spacing and tone reduce legitimacy.	Low
Sender Display Name Trick	"IT Support" is generic and can be easily spoofed.	Medium

3. Email Header Analysis

From a typical phishing header found in email security labs.

```
Return-Path: <mailserver@randomhost.xyz>
From: IT Support <it-helpdesk@secure-it-support.com>
Received: from unknown123.randomhost.xyz (185.32.55.21)
Authentication-Results: spf=fail; dkim=none; dmarc=fail
Message-ID: <98374hgfh8374@randomhost.xyz>
```

Header Field	Explanation	Relevance to Authenticity
From: vs Return-Path	"From" claims to be IT Support, but "Return-Path" shows `randomhost.xyz`.	Mismatch indicates spoofing. Legitimate emails rarely come from unrelated servers.
Received: Path	Shows the email originated from `185.32.55.21`, a foreign, unknown server.	Indicates sender infrastructure is not part of the organization. Helps trace true origin.
Authentication-Results (SPF/DKIM/DMARC)	SPF=fail, DKIM=none, DMARC=fail.	Clear indication that sender failed authentication checks and is likely malicious.
Message-ID Domain	Message ID references `randomhost.xyz`, not the corporate domain.	Another sign email was generated outside legitimate mail servers.

Conclusion

All header checks strongly support that the message is spoofed and malicious.

4. Incident Response Plan

1. **Threat Description:** This is a credential theft phishing attack. The attacker attempts to trick users into clicking a fake password reset link to harvest login credentials to corporate systems.
2. **Potential Impact Assessment:** If a user clicks the link and enters credentials
    - Unauthorized access to corporate email or internal systems
    - Data theft or exfiltration
    - Account takeover
    - Lateral movement within the network
    - Potential deployment of malware or ransomware
    - Compromise of sensitive business information
3. **Immediate Response Actions:** For the SOC / Helpdesk
    - Alert the security team and log into the incident
    - Advise recipients NOT to click the link, issue a companywide warning
    - If someone clicks the link: reset their account passwords immediately, invalidate active sessions, Review authentication logs for suspicious login attempts
    - Block the phishing domain and IP at the firewall, proxy, and email filters
    - Report domain to web hosting and threat intelligence services
4. **Preventive Actions**

    Technical Controls
    - Enforce SPF, DKIM, and DMARC for all corporate email
    - Enable advanced email filtering: sandboxing, URL rewriting, attachment scanning
    - Deploy endpoint protection with anti-phishing and anti-malware capabilities

    User Awareness
    - Quarterly phishing awareness training
    - Teach staff to identify red flags: suspicious domains, urgencies, generic greetings
    - Simulated phishing exercises to reinforce safe behavior
    - A “Report Phishing” button in the email client
5. **Future Recommendations**
    - Establish a formal Email Security Policy
    - Implement continuous monitoring of email gateways and security logs
    - Enforce least-privilege access to reduce account takeover impact
    - Regular audits of password policies and authentication logs
    - Maintain an updated incident response playbook for email-based threats