**Phishing Email Analysis Report**

**Prepared by: Aryanshu Saha  
 Date: June 24, 2025  
 Subject: Analysis of a Suspicious Email Purporting to Be from IT Support**

**1. Introduction**

This report presents a comprehensive analysis of a suspicious email believed to be a phishing attempt. The objective is to identify phishing indicators and provide insights into common tactics used by cybercriminals to deceive users. The analysis is conducted using a sample email and includes header examination, content review, and technical verification of embedded elements such as links**.**

**2. Email Sample Overview**

**2.1 Email Header (Key Fields)**

* From: IT Help Desk <it-support@corp-it.help>
* To: [Redacted]
* Subject: Urgent Email Account Suspension Notice
* Return-Path: <mailer123@random-mail.com>
* Reply-To: <support@corp-it.help>

**2.2 Email Body**

Dear Valued Employee,

Your mailbox has been flagged for suspicious activity and will be suspended within 24 hours if not verified. Please click the link below to secure your account:

[Verify My Account Now]

Failure to comply will result in permanent loss of access. We apologise for any inconvenience.

IT Security – corp-it.help

**3. Phishing Indicators Identified**

**3.1 Header Discrepancies**

* The From address uses a domain (corp-it.help) that closely mimics a legitimate organization but is unofficial.
* The Return-Path (random-mail.com) does not align with the sender’s email domain, indicating potential spoofing.
* SPF, DKIM, and DMARC records (if analyzed via a header analyzer) are likely missing or misconfigured, which is typical of spoofed emails.

**3.2 Suspicious Domain Usage**

* The sender’s domain, corp-it.help, is not recognized as part of the organization’s official domain (corp.com).
* This technique is a form of “typosquatting” or domain impersonation.

**3.3 Urgency and Emotional Manipulation**

* Language such as “Your mailbox… will be suspended within 24 hours” and “Failure to comply will result in permanent loss of access” is designed to instill fear and provoke hasty actions.
* Use of deadlines and penalties is a hallmark of phishing.

**3.4 Generic Salutation**

* The greeting “Dear Valued Employee” is impersonal. Legitimate internal communications typically address employees by name.

**3.5 Grammatical and Stylistic Errors**

* The phrase “We apologise for any inconvenience” contains inconsistent tone and grammatical errors.
* Such mistakes are frequently found in phishing emails and signal unprofessional origin.

**3.6 Suspicious Link Behavior**

* The call-to-action button labeled “[Verify My Account Now]” masks the actual URL, which points to a non-corporate IP or a suspicious domain (e.g., http://212.58.12.33/verify).
* Hovering over or inspecting the hyperlink in the email’s source reveals the deception.

**3.7 Missing Corporate Branding**

* No official logo, no privacy policy, no IT department contact information, or any form of validated identity.
* Real IT communications would include formal signatures, contact methods, and secure links.

**4. Risk Assessment**

* Threat Type: Credential Phishing
* Risk Level: High
* Potential Impact: Unauthorized account access, data breach, identity theft

**5. Recommendations**

1. Do not interact with the email content. Do not click links or download attachments.
2. Report the email to the IT department or use your organization’s phishing reporting mechanism.
3. Block the sender’s domain and the IP address at the email gateway and network firewall.
4. Educate staff on identifying phishing attempts using this report as a reference.
5. Update security policies to include routine header checks and link inspection protocols.

**6. Conclusion**

This analysis confirms the email in question is a phishing attempt. The attack uses a combination of domain spoofing, urgency tactics, and deceptive links to lure the recipient into disclosing sensitive information. Prompt recognition and reporting of such threats are essential to maintaining a secure communication environment.