Phishing Indicators Identified

1. **Suspicious Sender Address**

   - Domain: securesupportcloud[.]com (not the company's actual domain)

   - Legitimate IT support would typically use the company's official domain

2. **Urgent/Threatening Language**

   - "Immediate Software Update Required"

   - "Failure to do so will result in being locked out of your system"

   - Creates artificial pressure to act without thinking

3. **Suspicious Link**

   - The "Update Now" button likely points to a malicious URL

   - No actual URL is visible, requiring hovering to reveal the true destination

4. **Generic Greeting**

   - "Dear all Contoso Corp employees" - lacks personalization

   - Legitimate company communications often address employees by name

5. **Credential Harvesting Attempt**

   - Instructions to "use your company credentials to verify your identity"

   - This is a classic tactic to steal login information

6. **Download and Execute Instructions**

   - "Download and run the update file" - could install malware

   - Legitimate updates typically come through official channels

7. **Grammar Inconsistency**

   - "Dear all Contoso Corp employees," - awkward phrasing

   - Minor but noticeable language issues