

Phishing Email Analysis Report

Email Summary:

Sender: "LinkedIn Customer Support"

Subject: "UPGRADE SUBSCRIBER"

Content: "Your account is temporarily unavailable. FAIL TO UPGRADE YOUR ACCOUNT, IT WILL BE AUTOMATICALLY CLOSED." User is asked to submit Email, Password, Confirm Password and click "Reply to UPGRADE".

Phishing Indicators:

1. **Urgent / threatening language:** Uses fear ("automatically closed") to pressure the user.
2. **Requests sensitive info:** Asks directly for password and confirmation.
3. **No personalized greeting:** Uses "Dear LINKEDIN Customer".
4. **Poor grammar and wording:** Robotic phrases like "upgrade your LINKEDIN Account to our new system".
5. **Fake branding:** LinkedIn logo used, but no verifiable sender.
6. **No valid contact info:** No support links, email addresses, or phone numbers.
7. **Suspicious call to action:** Button likely redirects to malicious site.

Conclusion:

This is a confirmed phishing attempt using impersonation, urgency, and credential harvesting. Do not click links or submit any information.

Screenshot of Phishing Email:

