Sender Information

- **Display name appears as “LinkedIn Support”**
- **Actual sender email: noreply@linkedln-security-check.com**
    - **Domain misspelled (“linkedln” instead of “linkedin”)**
    - **Not an official LinkedIn domain**

ŽŬĂHeader Analysis

- **Using a header analyzer, the following issues were detected:**
- **SPF authentication failed**
- **“Return-Path” domain: verify@linkedln-security-check.com**
- **Does not match the display address**
- **Server IP located in a region unrelated to LinkedIn operations**
- **Multiple unusual mail hops**
-

ỸŬĂSuspicious Links

- **The email contains a button labelled “Verify Your Account Now”.**
  When hovered, it leads to:
  http://lnkedln-verification-alerts.net/login
- **Non-HTTPS**
- **Misspelled domain (“lnkedln” instead of “linkedin”)**
- **Not owned by LinkedIn**

---

4. Attachments

- **Attachment included: LinkedIn_Account_Update.html**
  This file type is commonly used in phishing to steal login credentials.
-

- **This creates urgency and fear, a common phishing strategy.**

-

---

6. Grammar and Formatting Problems

- **Several spelling errors**
- **Inconsistent capitalization**
- **Poor alignment and mismatched fonts**
- **Legitimate LinkedIn emails have professional formatting.**

---

x Branding Issues

- **Logo is low quality and slightly distorted**
- **Footer lacks LinkedIn’s official contact details**
- **No valid copyright notice**

These findings confirm the email is a phishing attempt targeting LinkedIn users.