**Phishing Email Analysis**

**1. Sender Address**

* The email claims to be from **LinkedIn**, but the sender is:  
  **support@careerbuildcompany.com**
* Official LinkedIn emails come from domains like @linkedin.com or @email.linkedin.com.
* This mismatch is a **major phishing indicator** (spoofing).

**2. Brand Impersonation**

* The email uses the **LinkedIn logo and styling** to trick the user into believing it’s legitimate.
* Phishers often copy the branding of trusted companies.

**3. Suspicious Links**

* The screenshot shows clickable text like **“See what’s new”**, **“1 message”**, **“2 invitations”**, etc.
* Without hovering, we can’t see the actual URL, but these are classic lures to redirect users to a fake login page that steals credentials.
* Legitimate LinkedIn notifications usually link to linkedin.com domains.

**4. Urgency & Engagement Tricks**

* The email shows **“28 notifications and updates”** to **trigger curiosity and urgency**.
* Phishing often uses such **psychological tactics** to make you click without thinking.

**5. Language Style**

* The text is simple and generic: *“Demo, see what your network has been up to”*.
* Real LinkedIn emails typically personalize content (e.g., use your name).
* Lack of personalization is a **red flag**.

**6. Email Structure**

* The design looks **too basic** compared to real LinkedIn emails, which include footers with:
  + Privacy policy links
  + Company address (LinkedIn Corporation, Sunnyvale, CA)
  + Unsubscribe options
* The **absence of these standard elements** suggests it’s fake.