Phishing Traits in the Email

1. **Suspicious Sender Address (Email Spoofing)**
    - From: "LearnOnlinePro Support" support@learnonlinepro-courses.com
    - Uses a domain that looks similar but is **not the official** learnonlinepro.com domain.
2. **Urgent & Threatening Language**
    - Subject: *"Urgent: Your LearnOnlinePro account will be deactivated!"*
    - Body threatens account deactivation *within 24 hours* to pressure quick action.
3. **Spelling & Grammar Errors**
    - "unusuals" → should be "unusual"
    - "acccount" → extra 'c'
    - "permanantly" → should be "permanently"
    - "inconvinience" → should be "inconvenience"
    - "saftey" → should be "safety"
4. **Malicious Links Disguised as Legitimate**
    - **Reset Password button**: http://secure-update.learnonlinepro-login.info/reset (fake domain intended to steal credentials).
    - **Login link**: Text shows https://learnonlinepro.com/login but goes to http://learnonlinepro.verify-account.ddns.net/login — mismatched URL.
5. **Dangerous Attachment**
    - Invoice_Statement.pdf.exe — appears to be a PDF but is actually an executable file, which can install malware.
6. **Social Engineering**
    - Exploits fear of losing access to purchased courses.
    - Uses authority ("Security Department") to appear official.