1. Concept Definition

Display Name Spoofing is a type of email impersonation attack where a threat actor modifies the "friendly" name shown to the recipient while using a legitimate, unrelated email address. It exploits the **User Interface (UI)** design of modern email clients rather than a technical flaw in the email protocol.

---

2. Step-by-Step Process (The "Attack Chain")

Step A: Reconnaissance & Target Selection

The attacker identifies a **trusted entity** (e.g., Zetech Finance Office) and a **target** (e.g., a lecturer). They find the lecturer's email via public faculty directories.

Step B: Account Preparation (The Ghosting Setup)

The attacker creates or uses a free, legitimate email account (e.g., `scammer123@gmail.com`).

- **The Trick:** They go into the account **Settings → "Send Mail As."**
- **The Input:** In the "Name" field, they type: `Zetech Finance <finance@zetech.ac.ke>`.

Step C: Email Composition

The attacker crafts a message using **Social Engineering** triggers:

- **Urgency:** "Your salary is on hold."
- **Authority:** "Official Audit Requirement."
- **Call to Action:** A malicious link to a credential-harvesting site.

Step D: Transmission & Filter Bypass

The email is sent. Because it originates from a **legitimate Gmail server** with valid **SPF** and **DKIM** records for *Gmail*, it passes technical "spam" checks. The filters see a valid "Passport" from Google and allow the email into the **Primary Inbox**.

Step E: Victim Reception (The Mobile Trap)

The lecturer receives a notification. Due to limited screen real estate, the mobile app prioritizes the **Display Name**.

- **Visual Output:** `From: Zetech Finance <finance@zetech.ac.ke>`
- **The Result:** The lecturer trusts the bold name and clicks the link.

---

3. Why it Bypasses Traditional Security (Exam Focus)

Security Protocol	Why it Fails to Stop "Ghosting"
SPF (Sender Policy Framework)	SPF only checks if the **Server IP** matches the **Sending Domain** (`gmail.com`). It doesn't check the "Name" field.
DKIM (Digital Signatures)	DKIM proves the email wasn't changed *after* it left the Gmail server. It doesn't prove the "Name" inside is truthful.
DMARC (Policy Control)	DMARC checks for "Alignment." Since the attacker used a Gmail address to send a Gmail email, it **Aligns perfectly** and passes.

4. Key Terminology for your Exam

- **Social Engineering:** Manipulating people into performing actions or divulging confidential info.
- **Metadata Deception:** Hiding the true sender identity behind a "friendly" label.
- **Mobile UX Vulnerability:** The design choice of mobile apps to hide full email addresses to save space.
- **False Alignment:** When an email passes technical checks because the technical sender matches the server, even if the "human" sender is a lie.

5. Summary Diagram

The "Golden Rule" for Identification:

The "Tap" Test: In a mobile app, you must tap the sender's name to unmask the hidden email address. If the **Display Name** claims to be "Finance" but the **Email Address** is `@gmail.com`, it is a confirmed spoof.