Contents

[1.7] Deference to Technical Authority Claims

1. Operational Definition: The automatic acceptance of instructions or requests from individuals who use technical jargon or claim specialized expertise, without questioning the legitimacy or security implications of the request.

2. Main Metric & Algorithm:

- **Metric:** Jargon-Induced Compliance Rate (JICR). Formula: `JICR = N_jargon_successes / N_jargon_attempts`.
- **Pseudocode:**

  python

  ```
  # Best measured via targeted phishing simulations.
  def calculate_jicr(simulated_attack_data, start_date, end_date):
      # Query simulation results for campaigns using technical pretexts
      tech_pretext_campaigns = query_simulations(
          theme=['it_support', 'system_upgrade', 'security_patch'],
          date_range=(start_date, end_date)
      )

      total_attempts = tech_pretext_campaigns.total_recipients
      success_count = tech_pretext_campaigns.clicked_count + tech_pretext_campaigns.complied

      JICR = success_count / total_attempts if total_attempts > 0 else 0
      return JICR
  ```

- **Alert Threshold:** `JICR > 0.1` (i.e., over 10% success rate for technical pretext attacks).

3. Digital Data Sources (Algorithm Input):

- **Phishing Simulation Platform API:** Data from campaigns where the lure involves technical authority (e.g., "IT Helpdesk needs you to run this script", "Cloud Team requires password verification").
- **Email Gateway/Proxy Logs:** To detect real-world attacks with similar lures that were not caught by filters.

4. Human-To-Human Audit Protocol: In training sessions, present a scenario: "You get a call from 'Mike from IT' who says your PC is infected and he needs you to go to a website. What do you do?" Role-play the conversation to see if the employee asks for verification (e.g., ticket number, calling back the official helpdesk line).

5. Recommended Mitigation Actions:

- **Technical/Digital Mitigation:** Implement a centralized IT portal where all legitimate requests are logged and can be verified by employees. Use digital signatures for official scripts.

- **Human/Organizational Mitigation:** Train employees on a simple verification protocol: "Hang up, find the official number yourself, and call back to verify." Train them to recognize social engineering tactics that use jargon to create confusion and urgency.
- **Process Mitigation:** Establish a clear, well-publicized process for how IT will and will not communicate with employees, setting expectations for legitimate interactions.