Quiz 5 Rubric Blueprint

1. What is Spear Phishing? How does it work? [4 points]

- **(1 point)** Definition of Spear Phishing (targeted, context-aware).
- **(1 point)** Contrast with regular phishing (e.g., "more sophisticated" or "not mass mailing").
- **(1 point)** Explains the first step of *how* it works: Information Gathering (INTEL).
- **(1 point)** Explains the second step of *how* it works: Pretexting.

2. Why does elicitation work? [4 points]

- **(1 point)** Definition of elicitation (subtle extraction in normal conversation).
- **(3 points)** Mentions three psychological principles exploited (e.g., politeness, ego/praise, desire to appear well-informed, or trust).

3. Mention three ways in which you can de-anonymize the identity of an entity [4 points]

- **(2 points)** Traffic Analysis / Correlation Attack (1 point for the term, 1 point for the basic explanation of correlating entry/exit timing/volume).
- **(1 point)** DNS Leaks (mentioning DNS requests outside the anonymized channel).
- **(1 point)** Malicious/Rogue Exit Nodes (mentioning snooping on unencrypted traffic).

4. Can you block anonymization services? What are the implications of such actions? [4 points]

- **(1 point) Answer:** Yes, by blocking the publicly available IP addresses of known nodes (relays/directory servers).
- **(3 points) Implications:** Three distinct, correct implications (1 point each), such as endangering political dissidents/journalists, harming vulnerable individuals, stripping citizens of privacy, or hindering law enforcement/corporations.

5. How would you prevent re-identification attacks on anonymized data? [4 points]

- **(1 point)** Identify the core technique: Differential Privacy.
- **(1 point)** Explain the goal of Differential Privacy (allowing statistical queries while guaranteeing the output is similar regardless of one individual's data).
- **(2 points)** Describe a specific mechanism that achieves Differential Privacy.