④ i) Physical Social Engineering & It attempts to gain access to a Physical location.

- Piggybacking - used to enter restricted area by Convincing an authorised personal.
- Eavesdropping - Attacker can gain information by hearing a discussion b/w two people or by reading emails and listening to telephonic Conversation.
- Impersonation - The attacker acts like someone else to trap the victim.
- Dumpster Driving - Valuable information can often be found on trash, printers and pieces of paper.
- Reverse Social Engineering - In this the attacker creates a scenario where the victim ends up asking for information to the cracker and in this process ends up providing the required information to the attacker. Reverse Social Engineering requires a good preattack research and planning, however if executed well it is more successful in attaining gaining quality information.

ii) Remote Social Engineering & It involves pointed and real time Communication with the target over the phone or via email or instant messaging.

- Computer-based SE - It is implanted by using software or programming applications like email, websites, pop-ups.
- SE by Email - It tries to build rapport as

a precussor to the actual breach, or ~~the~~ it tries to elicit information or spread malware by tricking the email recipient into opening a malicious attachment or visiting a malicious website.

- Phishing - It take the form of fake notification purporting to be from a well known organization, asking for the recipient's personal information including user credentials credit card number, or banking information
- SE By Phone - The caller generally assumes a false identity and may use various techniques to convince the victim, such as being overly friendly, acting in an authoritative manner or pressure. In many business cultures, challenging someone's identity is not socially acceptable and may be seen as impolite, so getting away with assuming a false identity may be easier than you think.