Advanced / Multimedia / Social Engineering

These are modern social-engineering attacks where attackers use audio, video, or realistic digital media to trick victims. Instead of just emails or texts, they use tools like:

- Deepfake voices or videos to impersonate real people
- Synthetic media to fake instructions or approvals
- Pretexting calls or in-person approaches that feel authentic
- Watering-hole and supply-chain tricks that target specific groups

These methods feel more believable because they use realistic media and personalized context, making them harder to detect.