**Module 7 Social Engineering**

**7.1 Social Engineering Lab Intro**

**Pretexting**

1. Build sense of trust with victim
2. Eg. pose as IT auditor then manipulate people at company’s front door to let them in

**Baiting**

1. Similar to phishing but user promised some type of good
2. Get baited with USB device with cat but keylogger running in bg

**Quid Pro Quo**

1. Similar to baiting but promise of a service
2. Eg. tech support scam – ask for access then deactivate AV & install malware

**Tailgating**

**Piggybacking**

**Reconnaissance**

1. Just stalk their social media and google them (lol)
2. Usually security questions ask for doggo names so look out for pets