**Module 7 Social Engineering**

**7.0 Social Engineering**

**Social Engineering**

1. Use of deception to manipulate individuals into divulging confidential/personal info that may be used for fraudulent purposes
2. Attack phases
   1. Research target company
      1. Dumpster diving, websites, employees, tour company etc
   2. Select victim
      1. Identify frustrated employees of target
   3. Develop relationship
   4. Exploit relationship
      1. Collect sensitive acc info, financial info & current tech

**Human-Based Social Engineering**

1. Impersonation
   1. Pretend to be someone else
   2. Normally in authority
2. Vishing
   1. Use telephone (voice phishing)
   2. Tech support scam
3. Eavesdropping
4. Shoulder surfing
5. Dumpster diving
6. Reverse social engineering
   1. Eg. browser redirect, tech support scam etc.
7. Piggybacking
   1. Asks someone to let them in
8. Tailgating
   1. Fake badge
9. Phishing
   1. Send fake emails to induce people to reveal personal info/send money
10. Smishing
    1. Don’t click text msg links

**Insider Threats**

1. Employees
2. Former employees
3. Contractors or business associates
4. Types
   1. Non-responders – consistent negligence
   2. Inadvertent insiders – comply with policy
   3. Insider collusion
   4. Persistent malicious insiders – second streamers
   5. Disgruntled employees – sabotage, IP theft

**Social Media**

1. Fake profiles

**Social Engineering Countermeasures**

1. Research
2. Reject requests for help
3. Do not post personal data or photos
4. Do not reveal sensitive data
5. Follow policies & procedures

**Insider Threat Countermeasures**

1. Deterrence
2. Know your weak links
3. Identify valuable info
4. Monitor ingress & egress points