## Social Engineering Techniques

**Social Engineering Basics**

* “Hacking” people instead of systems
* Identifying appropriate targets including:
  + Receptionists
  + Help Desk
  + Finance and Purchasing
  + Information security (IT) staff
  + Vulnerable employees
* Conducting research, using:
  + Reconnaissance
  + Public information
  + Social networking sites
  + Dumpster diving
  + Cold calling
  + Insiders
* Communication methods including:
  + In-person
  + Telephone
  + E-mail
  + Web sites
  + Social media and communication apps
* Goals include manipulating targets into:
  + Revealing sensitive information, including logon credentials
  + Downloading malware
  + Reconfiguring systems
  + Granting unauthorized logical or physical access
  + Transferring money

**Common Social Engineering Techniques**

* Impersonation, including:
  + Management
  + Law enforcement
  + Maintenance technicians
  + Vendors or clients
  + Employees
  + Tech support staff
* Reciprocity (that is a favor for a favor)
* Phishing
* Bribing
* Fake news (print, video, audio)
* Manipulating emotions (for example, creating a sense of fear or urgency)
* Building relationships with targets and then, exploiting them