**Module 9: Social Engineering**

**Concept**

* The art of convincing people to reveal confidential info

**Phase of a Social Engineering Attack**

* Research the Target Company
* Select a Target
* Develop a Relationship
* Exploit the Relationship

**Social Engineering Techniques**

* **Human-based Social Engineering:** 
  + Sensitive info is gathered by **interaction**
  + Techniques:
    - **Impersonation:** Pretend to be someone legitimate or an authorized person
    - **Vishing:** An impersonation technique in which the attacker tricks individuals to reveal…using voice technology such as VoIP, telephone system.
    - **Eavesdropping**
    - **Shoulder surfing**
    - **Dumpster diving**
    - **Reverse social engineering:** The attacker presents him as an authority and the target seeks his advice before or after offering the info that the attacker needs
    - **Piggybacking:** An authorized person intentionally or unintentionally allows an unauthorized person to pass through a secure door
    - **Tailgating:** Wear a fake ID badge, enter a secured area by closely following an authorized person through a door that requires key access
    - **Diversion theft**: Trick a person responsible for making a genuine delivery into delivering the consignmnet to a location other than the intended location
    - **Honey trap:** Attacker target a person online, pretending to be an attrative person. They then begin a fake online relationship to obtain…
    - **Baiting:** Attackers offer end users sth alluring in exchange for important info such as…A physical device such as USB flash drive containing malicious files is left in a location where people can easily find it.
    - **Quid Pro Quo:** Call numerous random numbers within a company, claiming to be from technical support. Offer their service to end users in exchange for confidential info
    - **Elicitation:** Extract info from the victim by engaging him in normal and disarming conversations. Based on the victim’s interests, attackers much work to taraget their elicitation approach to extract the relevant info.
* **Computer-based Social Engineering**
  + Sensitive info is gathered with the **help of computer**
  + Techniques:
    - **Phishing:** 
      * **Spear Phishing:** A targeted phishing attack aimed at **specific individuals** within an org.
      * **Whaling:** Target **high profile executives** like CEO.
      * **Pharming:** Redirect **web traffic** to a fraudulent website by installing a malware on a personal computer. Also known as “phishing without a lure”, and perform by using **DNS Cache Poisoning** or **Host File Modification**
      * **Spimming:** Exploit Instant Message platform to flood spam. Atttackers uses bots to harvest Instant Message Ids and spread spam
    - **Hoax Letters:** Emails that issue warnings to the user about new malware that may harm the user’s system
    - **Chain letters:** Emails that offer free gifts that the user forwards the mail to a specificied number of people
    - **Pop-up windows attacks:** Windows that suddenly pop up while surfing the Internet and ask for user info to login.
    - **Spam mail**
    - **Scareware:** Malware tricks users into visiting malware infested websites, or downloading potentially malicious software
    - **Instant chat messenger**
  + Phishing Tools: **ShellPhish**
* **Mobile-based Social Engineering**
  + Sensitive info is gatherted with the **help of mobile apps**
  + Techniques
    - Publishing malicious apps
    - Using fake security apps
    - Repacking legitimate apps
    - Sms phishing

**Insider Threats/Attacks**

* Using privileged access to intentionally violate rules or cause threat to the org’s info.
* Can be performed by a privileged user, disgruntled employee, terminated employee, accident-prone employee, third party, undertained staff, etc
* Types:
  + Malicious Insider:
  + Negligent Insider
  + Professional Insider
  + Compromised Insider

**Countermeasures**

* Good policies and procedures are ineffective if they are not taught and reinforced by empoyees.
* Password policies, Physical Security Policies, Defense Strategy
* Train invididuals on security policies
* Implement proper access privileges
* Presence of proper incidence response time
* Availability of resources only to authorized users
* Scrutinize info
* Background check and proper termination process
* anti-virus/phishing defense
* MFA
* Adopt documented change management
* Ensure software is regulary updated
* Detect Insider Threats
  + Insider risk controls
  + deterrence controls
  + detection controls
* Insider Threat Countermeasures
  + Separation and rotation of duties
  + Least privileges
  + Controlled access
  + Logging and auditing
  + Employee monitoring
  + Legal policies
  + Archive critical data
  + Employee training on cyber security
  + Employee background verification
  + Periodic risk assessment
  + Privileged users monitoring
  + Credentials deactivation for terminated employees
* Detect phishing emails
  + It seems to be from a bank, company, or social networking site and has a generic greeting
  + It seems to be from a person listed in your email address book
  + It has an urgent tone or makes a veiled threat  It may contain grammatical or spelling mistakes
  + It includes links to spoofed websites
  + It may contain offers that seem to be too good to be true
  + It includes official-looking logos and other information taken from legitimate websites
  + It may contain a malicious attachment
* Anti-Phishing Toolbar: **Netcraft, Phish Tank**

**Social Engineering Tools**

* SET (Social Engineerint Toolkit)

**Audit Organization’s Security for Phishing Attacks:**

* Tools: **OhPhish**, **a web-based** protal to test…