



# Social Engineering

MARK SHTERN

# Social Engineering



- ▶ SE is manipulating a person into knowingly or unknowingly giving up information
  - ▶ Psychological manipulation
  - ▶ Trickery

# Goals

- ▶ Install spyware, other malicious software
- ▶ Trick persons into handing over passwords and/or other sensitive information

# Movie

- ▶ <http://www.youtube.com/watch?v=8TJ4XOvY7II&feature=related>
- ▶ <http://www.youtube.com/watch?v=-kW1DPPp1VQ>

# Attack Pattern

- ▶ Information gathering
- ▶ Developing relationship
- ▶ Exploitation
- ▶ Execution

# Human nature



- ▶ Reciprocity Principle - People tend to feel obliged to discharge perceived debts .
- ▶ Authority Principle – People tend to respond to authority figures
- ▶ Social Proof Principle – People tend to use people who are similar to themselves as behaviour models
- ▶ Scarcity Principle – People value things they perceive as scarce more than things they perceive as common
- ▶ Consistency / Commitment Principle – People tend to act to maintain their self image (even without conscious knowledge)

# Tactics



- ▶ Pretexting
- ▶ Phishing
- ▶ Fake Websites
- ▶ Fake Pop-up
- ▶ Phone Social Engineering
- ▶ Spoofing
  - ▶ CallerID
  - ▶ SMS
- ▶ TinyURL

# Examples

- ▶ Facebook
  - ▶ Made a fake Facebook account to get access to your friends list.
- ▶ Twitter
  - ▶ photo advertising a video with girls posted
    - ▶ “new version of Adobe Flash” is required to watch the video

# RSA: Phishing Attacks

- ▶ Sent phishing e-mail
  - ▶ Subject
    - ▶ "2011 Recruitment Plan"
  - ▶ Attachment
    - ▶ Excel spreadsheet with discovered Adobe Flash zero day flaw CVE 20110609
    - ▶ Trojan
- ▶ Harvested credentials
- ▶ Obtained privileged access to the targeted system

# Countermeasures

- ▶ Security policy
- ▶ Physical security
- ▶ Education/Awareness