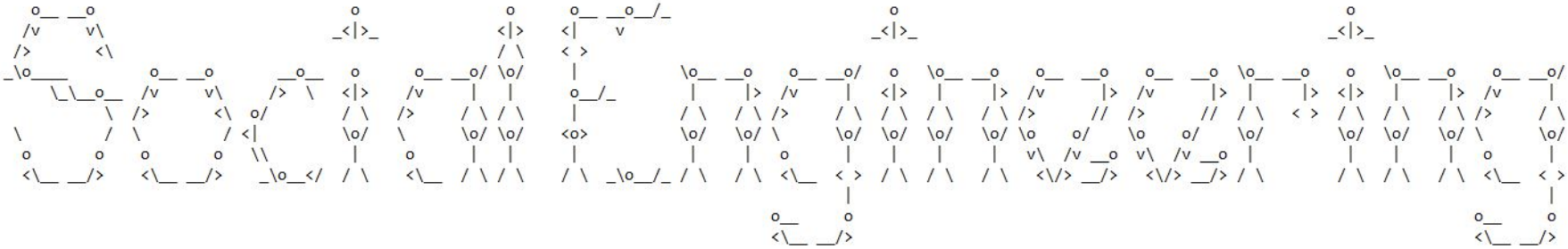

# What is Social Engineering?

- “Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.”

# Social Engineering

- Considered the weakest link in Security
- Based on Cognitive Biases
  - Trust
  - Appeal to Authority
  - Accepted Norms

# Lifecycle

- Pretexting
- Establish Trust
- Extract Information
- Exit
- …
- Use data for next phase of attack

# Research

- The first step!
  - The more you know, the easier it is
  - Use information to establish Trust
  - Can “engineer” softer targets for information

# Targets

- People with data
  - Credit Cards
  - Passwords
  - PII
- Systems with data
  - Passwords
  - Confidential Data
  - Trade Secrets

# What else?

- Can you think of any other things that can be stolen?
- Who would you get them from?

- Janitor
- Employee Family
- Security Guard

# Common Methods

- Trojan Horses
- Phishing
- Tailgating
- Quid Pro Quo
- Observation
- Disguises
- Dumpster Diving

# Trojan Horses

- A type of Computer Virus
  - Disguised as an innocuous file
- Can be distributed many ways
  - Email Attachment
  - Rogue disk
  - USB

# Phishing

- Phishing
- Vishing
- Smishing
- Spear Phishing
- Cat Phishing

# Quid Pro Quo

- Everyone needs help!
  - Instantly more trustworthy
- How can you help someone…

  … And steal information?

# Quid Pro Quo

- Pose as Help Desk
  - Call people in organization
  - Find someone who needs help
  - Help them fix their problem!
  - (and in the process, get their password)

# Observation

- The act of “spying” on someone
- Shoulder Surfing
- Recording
  - Security Cameras
  - Smartphones
  - News Cameras

# Disguises

- The simpler, the better
  - Avoid Uniqueness
- Used to establish Trust
  - Repairman
  - Another Employee
  - Maintenance
  - ???

# Dumpster Diving

- It’s exactly what you think it is
- Unshredded documents
- Items of knowledge
  - Names
  - Employee IDs
  - System Names
  - IPs

# Mitigations

- Employee Training
- Principle of Least Privilege
- Data Shredding
- Physical Security

# Sources / References

- http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics
- http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/all/