```
   o__ __o                            o                o      o__ __o__/_                        o                                                 o
  /v     v\                         _<|>_             <|>    <|    v                           _<|>_                                             _<|>_
 />       <\                                          / \    < >
_\o____         o__ __o       __o__   o      o__ __o/ \o/     |           \o__ __o    o__ __o/   o   \o__ __o    o__  __o    o__  __o  \o__ __o    o   \o__ __o    o__ __o/
     \_\__o__  /v     v\     />  \   <|>    /v     |   |     o__/_        |     |>  /v     |   <|>   |     |>  /v      |>  /v      |>  |     |>  <|>   |     |>  /v     |
           \  />       <\  o/        / \   />     / \ / \     |          / \   / \ />     / \  / \  / \   / \ />      //  />      //  / \   < >  / \  / \   / \ />     / \
 \         /  \         / <|         \o/   \      \o/ \o/    <o>         \o/   \o/ \      \o/  \o/  \o/   \o/ \o    o/    \o    o/    \o/        \o/  \o/   \o/ \      \o/
  o       o    o       o   \\         |     o      |   |      |            |     |   o      |    |    |     |   v\  /v __o  v\  /v __o  |          |    |     |   o      |
  <\__ __/>    <\__ __/>    _\o__</  / \    <\__  / \ / \    / \  _\o__/_ / \   / \  <\__  < >  / \  / \   / \   <\/> __/>   <\/> __/> / \        / \  / \   / \  <\__  < >
                                                                                            |                                                                            |
                                                                                    o__     o                                                                    o__     o
                                                                                    <\__ __/>                                                                    <\__ __/>
```

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...”

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’s 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
- Un-shredded 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/

- https://www.youtube.com/watch?v=1kkOKvPrdZ4