Compromising Wetware – Plugging the Human Leaks

Social Engineering 101

Ron Woerner, CISSP

CERTConference 2004

Who Am I?

How do you know?

How can I prove it to you without compromising my privacy?

Theme

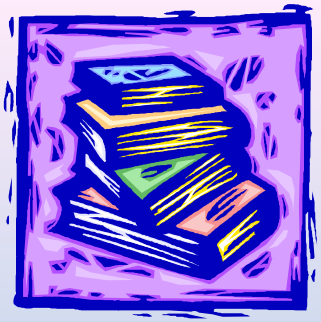
People will use almost any method to get what they want.

Trust, but verify

Agenda

- Definitions, Goals & Thoughts
- How social engineers do it
  - Persuasion methods & techniques
  - Attack levels
- How to prevent it

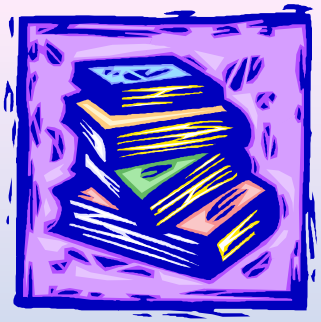
Definitions



Social Engineering: n.

- "The art and science of getting people to comply to your wishes." (Bernz 2)
- "Getting needed information (for example, a password) from a person rather than breaking into a system" (Berg).

Definitions



Trust

- (noun) **a:** assured reliance on the character, ability, strength, or truth of someone or something. **b :** one in which confidence is placed. (Merriam Webster)
- (verb) To have or place confidence in; depend on.

Obsequious: adj

- Attempting to win favor by flattery.

Social Engineering Goals

- To obtain information that will allow him/her to gain unauthorized access to a valued system and the information that resides on that system.
- To trick someone into providing valuable information or access to that information or the system on which it resides.

Introduction

Social engineering preys on qualities of human nature:

- The desire to be helpful
- The tendency to trust people
- The fear of getting into trouble

The sign of a truly successful social engineer is they receive information or access without raising any suspicion.

Plausibility + Dread + Novelty = Compromise

Introduction

- People are still the weakest link in the security chain.
- Social engineering is the most effective method of circumventing obstacles.
  - It is the hardest form of attack to defend against.
  - It is often quicker and easier than most other hacker techniques.
- Question: What's the easiest way to get inside information?

Social Engineering Thoughts

- Perception is reality
- Opinions tend to become facts.
- People generally want to meet your expectations.
- Every action human beings take is motivated either out of a need to avoid pain or the desire to gain pleasure – or both.

Social Engineering Scenarios

- The help desk receives a request to reset a VP's password.
- A copier repairman comes to your front door insisting he be allowed to enter.
- A competitor finds your company phone book in the trash.
- An administrator calls a user requesting their password to fix an application.
- You receive an email from your bank asking you update your personal information.

Persuasion Techniques

A social engineer will

- Misrepresent their objectives to trigger acceptance without thinking.
- Appear to be trustworthy
- Make statements at the outset that triggers a strong emotion such as:
  - Excitement
  - Fear

Vulnerability Points

- Unaware / Untrained Users
- Admin Assistants
- Help Desk Analysts
- Telephone Operators

Soc. Eng. Attack Levels - 1

Computer-based

- Mail attachments
  - Viruses, Worms, Trojan Horses, Malware
  - “I love you” & Anna Kournakova
- Spam, chain letters and hoaxes (email)
  - Phishing attack
  - Virus alerts
  - Urban Myths
- Anatomy of a hoax

Soc. Eng. Attack Levels - 1

Computer-based – Phishing

- Uses email to appear to come from a legit source to solicit personal information
- Uses fraudulent web sites that appear legit
- Example

Soc. Eng. Attack Levels - 2

Computer Based – Popup windows when web browsing

Soc. Eng. Attack Levels - 3

- Web sites
  - Similar names but misspelled or mislabeled
    - Whitehouse.com
    - Paypal-secure.com
    - http://www.respectedco.com@thisisascam.com
  - Stolen sites
    - www.aitpomaha.org

Soc. Eng. Attack Levels - 4

Human-based

- Impersonation
  - Average user in need of help
  - Important user
  - Outside service provider or guest
- Third-part authorization (transferring responsibility)
- Dumpster diving
- Shoulder surfing

Bernz's Social Engineering Tips

http://www.defcon.tv/docs/social-engineering/tips.html

- Be professional
- Be calm
- Know your mark
- Do not try to fool a superior scammer
- Plan your escape from your scam
- Try to be a woman
- Manipulate the less fortunate, the unaware and the stupid
- Use a team if you have to

How to Win Friends and Influence People*

- Fundamental Techniques in Handling People
- Six Way to Make People Like You
- How to Win People to Your Way of Thinking
- Be a Leader: How to Change People Without Giving Offense or Arousing Resentment

*By Dale Carnegie, 1936

Fundamental Techniques in Handling People

- Don't criticize, condemn or complain.
- Give honest and sincere appreciation.
- **Arouse in the other person an eager want.**

From How to Win Friends and Influence People

Six Way to Make People Like You

- Become genuinely interested in other people.
- Smile.
- Remember and use other people's names.
- Be a good listener.
- **Talk in terms of the other person's interests.**
- **Make the other person feel important.**

From How to Win Friends and Influence People

Win People to Your Way of Thinking

- Begin in a friendly way.
- Get the other person saying "yes, yes" immediately.
- Let the other person feel that the idea is his or hers.
- Appeal to the nobler motives.
- Dramatize your ideas.
- Throw down a challenge.

From How to Win Friends and Influence People

Be a Leader:
Change People without Offense

- Begin with praise and honest appreciation.
- Ask questions instead of giving direct orders.
- Use encouragement. Make the fault seem easy to correct.
- Make the other person happy about doing the thing you suggest.

From How to Win Friends and Influence People

Persuasion Methods - 1

- Diffusion of responsibility
  - Dilute personal responsibility for decision making.
  - Drop names
  - Claim someone higher up has made the decision
- Chance for ingratiation
  - Gaining advantage over a competitor
  - Getting in good with management
  - Giving assistance to a sultry sounding female

Persuasion Methods - 2

- Trust Relationships
  - Usually following a series of small interactions
- Identification
  - Build a connection with the target based on information gathered.
  - Informality
- Desire to help
  - Holding the door
  - Logging on to an account
  - Lack of assertiveness or refusal skills

Persuasion Methods - 3

- Cooperation
  - Voice of reason
  - Logic
  - Patience
  - Stresses the positive
- Moral duty
  - Requires prior information gathering
  - Tries to get the target to believe that there will be a wrong that compliance will mitigate

Persuasion Methods - 4

- Guilt
  - Create situations designed to:
    - Tug at the heartstrings
    - Manipulate empathy
    - Create sympathy
  - If granting a request will lead to avoidance of guilt, target is more likely to comply.
  - not granting the request will lead to significant problems to the requestor

Common Defenses

- Confirm identification of unknown people
- Make a policy that passwords are not
  - to be left lying around;
  - to be spoken over the phone.
- Implement caller ID technology
- Develop and use policies and procedures
- Protect sensitive documents appropriately

Common Defenses

- Be suspicious of unsolicited phone calls, emails, or visits
  - Trust, but verify
- Don't send sensitive information before checking a web site's security
- Pay attention to the URL of the web site
- Install & maintain anti-virus software, firewalls
- Know what to do if you are a victim

Common Defenses

- Recognize the signs
- Education, training and awareness
- If it's too good to be true, then it probably is.
- Look for the persuasion methods

Social Engineering Scenarios

- The help desk receives a request to reset a VP's password.
- A copier repairman comes to your front door insisting he be allowed to enter.
- A competitor finds your company phone book in the trash.
- An administrator calls a user requesting their password to fix an application.
- You receive an email from your bank asking you update your personal information.

Resources

- FTC – Consumer Information (http://www.consumer.gov/)
- FTC – Information Security (http://www.ftc.gov/bcp/conline/edcams/infosecurity/)
- CERT – Home User (http://www.cert.org/homeusers/)
- Privacy Rights Clearinghouse – (http://www.privacyrights.org/)
- GetNetWise – (http://www.getnetwise.org/)

Questions

Ron Woerner, CISSP

ron.woerner@conagrafoods.com