CSI
COMPUTER
SECURITY
INSTITUTE

Psychology of Social Engineering:
Training to Defend

John G. O'Leary, CISSP
Computer Security Institute

Abstract

- Historically, Social Engineering has been non-technical, but most insidious, playing upon our workers' sincere desire to get the job done and help others to do the same. The use of "phishing" via e-mail and phony websites and redirections, etc., adds a technical component to this psychological attack. A clever social engineer can make a target trust him or her to such an extent that they casually reveal sensitive internal information. Some browbeat, frighten or threaten for specific data. Others just flat out ask for it. It may not be a significant disclosure in and of itself, but the information gleaned by such manipulation can easily be combined with other small bits to produce a detailed and dangerous roadmap to our organizational treasures.

CSI
COMPUTER
SECURITY
INSTITUTE

Abstract

- Because a social engineering attacks leverage characteristics of human nature, they're hard not only to defend, but even to teach people how to resist. Find out why social engineering works so well, and why it is so hard to defend against, and why, in spite of our own use of the technique, we are also all subject to being successfully manipulated. More importantly, learn how to incorporate defense against social engineering into your organization's security awareness program.

Agenda

We'll use exercises including some role playing to cover:

- Types of threats
- Recognizing an attack
- Responding

We'll also focus on how to convey effective defense techniques to our co-workers without making them overly suspicious and unhelpful to legitimate customers.

Definition

- ***Social Engineering*** is the purposeful manipulation of an individual or group in an effort to gain information or effect certain behavior. It may or may not involve the use of technologies, but almost invariably includes some form of deceit and concealment of its actual goal.

J O'L

Other Definition #1

- Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology.

Kevin Mitnick

Other Definition #2

- Social Engineering is the attempt to talk a lawful user of the system into revealing all that is necessary to break through the security barriers. The alternate term for this is "bull*****ing the operator."

The Knightmare

Why it Works

- **Human Nature**
- In most instances, the request is genuine, not a ruse
- If we haven't been directly burned before, we're not suspicious
- Don't want to seem paranoid
- Don't want to be uncooperative

Why it Works

- We can see ourselves in the other person's unfortunate position …

- *And he seemed like such a nice guy*
- *And she knew the internal terms we use around here*
- *And he mentioned some of the people I know or have heard of who work here*

Why it Works

- And it doesn't seem like such a big deal

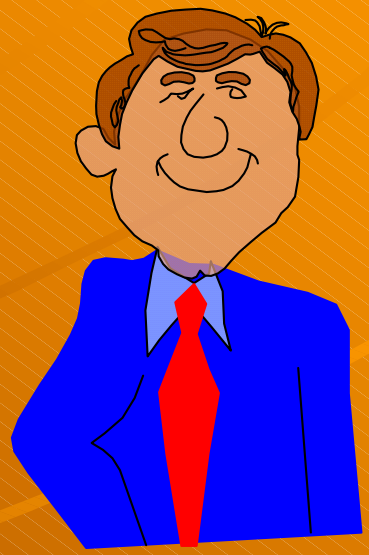
- *I'm a people person, I like to help*
- *Hey, aren't we called the **help** desk?*
- *I'm the only one who can do this correctly, and the caller mentioned that*

Why it Works

- *I don't want to get in trouble for letting this fall through the crack*
- *She said it was for the Director*
- *He was really apologetic about putting another item on my plate, said he knew how busy we are around here*
- *She was really thankful*

Why it Works

- Preys on distinct qualities of normal human nature
  - Tendency to trust people
  - Disinclination to be, or even seem unpleasant
  - Desire to help others
  - Fear of consequences for doing something wrong or not doing something right



Exercise 1

- **Phone call:**
  - "This is Chad in network support. We're having some intermittent server issues down here … at least they look like server issues, … maybe Apache, and we're trying to avoid bringing your segments down. We had to kill the A/P intranet for a couple of hours. But they're back up now… Anyway, I need you to back out, then walk through your login sequence……"

Exercise 1A

- **Analyze this phone call from a social engineering perspective**
  - What is the caller trying to make the receiver believe?
  - How may he have augmented this perception?
  - What emotions/experiences/perceptions is he bringing into play?
  - What does the caller really want?

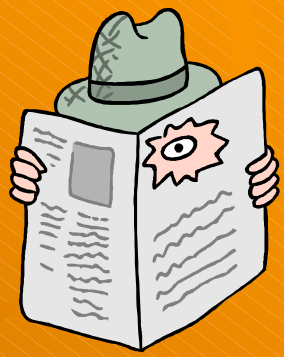
Exercise 1B (role playing)

- **You are the social engineer**
- Walk the called person through the logon sequence
- Be ready to respond to his or her objections
- Devise ways to avoid or reduce the call receiver's anxiety and suspicion during and after the call

Exercise 1C (defense)

- **You are the Security Awareness coordinator/trainer**
- Explain to an audience of users, in language they can understand, what just happened and why it's a real threat
- Be ready to respond to their objections
- Give them strategies for responding that don't make them look or feel like "paranoid security geeks"

Defense is Difficult



- ***Perception of paranoia***
  - *You security guys need to get out more*
  - *What I do is only a tiny part of the picture. I couldn't give away any trade secrets or anything like that. I don't even know any*
  - *Even if he got in with my ID, he couldn't do much. I can never get at anything I really need.....stupid #@!*& security*

Defense is Difficult

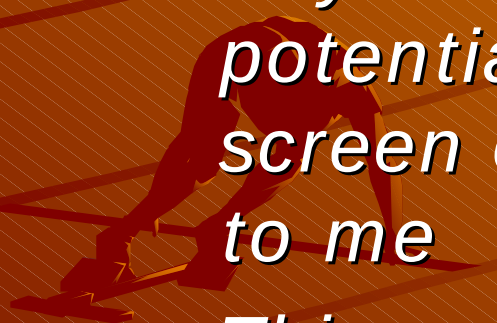
- ***Perception of business reality***
  - *We work with this stuff every day. Everyone here knows what it says and how it works and how to handle it*
  - *We get inquiries like that all the time. They do lead to sales, y'know*
  - *We can't afford to alienate a potential big buyer just because the security people are worried*

Defense is Difficult

- ***Organizational Culture***
  - *One of the really nice things about working here is that we all help each other*
  - *I used to work in a place that was all suspicious and grim. It was lousy*
  - *We're all on the same team. We gotta pull together and help each other*
  - *I'm not gonna start giving security quizzes to a VP. Are you nuts?*

Defense is Difficult

- ***Someone Else's Job***
  - *You security types get paid to handle that stuff. I've got a **real** job to do*
  - *Anyone who calls in here I treat as a potential customer. Security has to screen out the bad guys before they get to me*
  - *This group brings money in. You're supposed to provide us service*



Defense is Difficult

- ***Can be viewed as Career-endangering***
  - Don't want to get on the wrong side of someone
  - Especially if they're in high places
  - Don't want to get a reputation as a naysayer

Defense is Difficult

- **Human Nature (again)**
  - Most people don't want to refuse a request
  - It's nice to be nice
  - Say yes, it's done and out of the way
  - Say no, you have to explain
  - Don't want to have to explain why or why not
  - Fear of being ridiculed

We're all vulnerable

- All of us have buttons that can be pushed
- Competent social engineers can and will find our buttons
- We'll still have to work with these people tomorrow,... we assume
- Don't see the downstream ramifications of our actions

We're all vulnerable

- Not enough time to completely analyze a situation
- Normal tendency is to cooperate and help, not to throw up roadblocks
- Don't want to make someone else feel bad
- Don't want the grief from saying no
- Faster and easier to say yes (for most, but not all people)

Methods Used

- Telephone
- E-mail
- Dumpster Diving
- Snail mail
- Personal contact

Rationale

- Hacking is viewed as highly technical
- Some hackers truly are “elite”
- Most aren’t
- Technical controls are getting better every day (though they’ll never be perfect)
- *Homo Securitus* is not evolving that quickly

Rationale

- Humans tend to be one of the weakest links in the security chain
- Authorized humans still need ways to legitimately bypass technical controls
- If I can “hack the human,” I don’t have to wrestle with the control
- Human logging mechanisms aren’t that consistent or accurate

Rationale

- Makes sense to try to exploit people before spending time and effort on more complicated methods

- Why analyze the tumbler mechanisms on locks when you can get someone to leave the door open?

Exercise 2

- **Message from eBay**
  - "We're sorry to inform you that someone has been corrupting your account and violating our User Agreement……..(explanation of agreement – lifted from eBay – follows) ……."
  - "Other members have had their service interrupted"

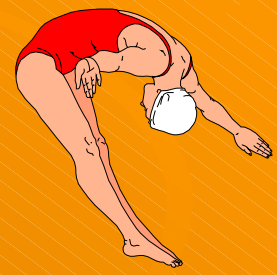
Exercise 2

- **Message from eBay**
  - "To avoid having your account turned off, please verify your account information at
  - http://verify_ebay.ppalinvestig.com
  - Standard blurbs regarding trademarks follow.

Exercise 2A

- **Analysis of the Message**
  - Might this be real?
  - What are they looking for?
  - What makes it credible?
  - Who's targeted?
  - Why might they be susceptible?
  - What could make this work or not work?

Exercise 2B



- **Website form (bad guy exercise)**
  - Build the “Investigation report”
  - How will you allay suspicion?
  - What information do you really want?
  - How will you mask your intentions?
  - What must you not ask?
  - What follow-up will you describe?
  - What follow-up will you actually do?
    - Formal “closing of inquiry” message?

Exercise 2C

- **Defense**
  - For this scenario (abstracted from Chapter 7 of Kevin Mitnick's book), who is your target awareness program segment?
  - How will you make them understand that this can happen?
  - How much time will you spend on this?
  - What techniques will you use?
  - Is this directly related to your organization?
  - What benefit does security get from covering something like this?

Alternate version

- E-mail from “AOL Billing Department”

Dear AOL® Member,
We recently noticed one or more attempts to log in to your AOL® account from a foreign IP address and we have reasons to belive that your account was hijacked by a third party without your authorization.

If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you. However,if you are the rightfull holder of the account, click on the link below, fill the form and then submit as we try to verify your identity.

http://my.aol.com/login

The log in attempt was made from:
IP address: 205.188.209.166
ISP host: cache-dq04.proxy.aol.com

We ask that you allow at least 72 hours for the case to be investigated and we strongly recommend not to make any changes to your account in that time.

If you received this notice and you are not the authorized account holder, please be aware that it is in violation of AOL® policy to represent oneself as another AOL® user. Such action may also be in violation of local, national, and/or international law. AOL® is committed to assist law enforcement with any inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft. Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the fullest extent of the law.

*Please do not respond to this e-mail as your reply will not be received.

Thanks for your patience as we work together to protect your account.

Regards,

AOL® Security Department.

Red Flags

- Cites technology that's similar, but not what you use
- Really in a hurry, needs information right now
- Mentions extreme negative consequences for the organization if you don't comply
- "They said you were the one who really knew this stuff"
- No possible callback

Indicators

- Refusal to leave a phone contact #
  - "I'll call you back in a few minutes"
- Quick on and quick off the line
- Chattiness, though you've never met
- Quickly brings up office gossip to establish bona fides & insider status
- Meandering conversation leading to an urgent request

Subtle Signs

- Failure to use standard corporate buzzwords and jargon
  - Sound like an outsider
  - Don't know how things really get done here
  - Sounds unnatural, stilted
  - Erroneous phrasing of standard things
- Heavy referencing of higher-ups as drivers of the request for information

Gold in the Middle

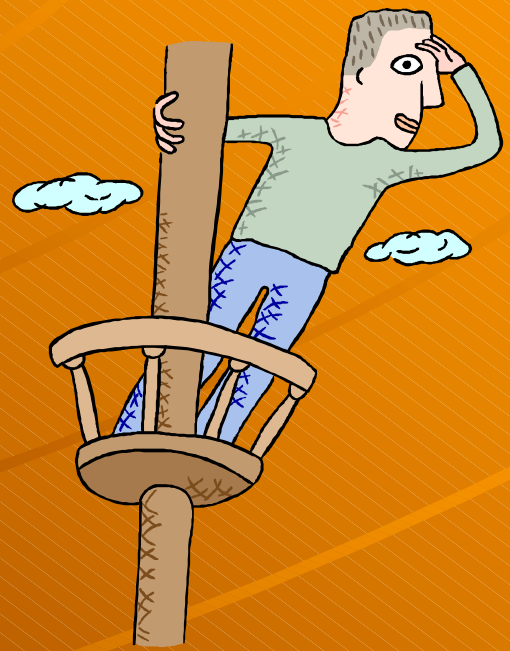
- Start conversation with innocuous subjects
- Chit-chat, sports, gossip, movies, …
- Multiple subjects – very light
- Quick question on a current project
- Ease back to movies, gossip, sports, …
  - "How much is Soriano getting' from the Nats!?"
  - "Didja see Federer in that last match?"
  - "That Holmes kid musta hit it 400 yards"
  - "I'm glad Brittney isn't driving my kid around"
  - "Abramson never offered me any trips"

Gold in the Middle

- Those refs shoulda been wearin Steeler Jerseys
- That Roethlisberger TD never hit the goal line... and that phantom interference call on the pass!?
- Is that guy Wilson still interfering with the event correlation project you guys were working on?
- Which vendor'd you choose anyway?
- They gonna make the date?
- Hasselbeck outplayed Big Ben, but he sure couldn't beat the zebras, could he?
- It was kinda nice though that Jerome Bettis won in front of his home town fans... then retired
- Hines Ward made a coupla nice catches, but I think their defense was MVP, eh?
- And Art Monk still isn't in the Hall of Fame!

Responding to an Attack

- Ongoing vigilance
- First responses
- Do's and don'ts
- Limiting damage
- Evidence collection
- Cleanup
- Recurrence prevention



First Responses

- Even when they know they're being "conned," most people will avoid confrontation and try to be "nice"
- Social engineers make heavy use of **reciprocation**, even if we never asked for the initial favors they did for us
- Policy, not perceived indebtedness, must guide the first responses
- People must know and be reminded of the policies --- regularly
- Specified contacts must be designated and publicized

Do's

- Do check policy
- Do ask others
- Do offer to call back
- Do check with "owner" of data requested
- Do ask why this is needed
- Do log what happened

Do's

- Do ask probing questions
- Do trust your judgment: if it sounds fishy, it probably is
- Do remember the sensitivity of the information you deal with regularly

Don’ts

- Don’t be bullied
- Don’t respond to “Right now” pressure
- Don’t assume others’ responsibilities in trying to help
- Don’t make “owner” decisions
- Don’t give away seemingly unrelated bits of information

Don’ts

- Don’t say yes just to get him off the phone
- Don’t view policy violation as an owed favor
- Don’t forget your responsibility to secure organizational resources

CSI
COMPUTER
SECURITY
INSTITUTE

Training

- Cannot prevent all attempts
- Can “harden” the target by educating staff
- Might involve a change to the organizational culture
- Go slowly
- Exercises can help make it real

Training Objectives

- Overcome denial of the issue
- Recognize the value of information
- Analyze requests
- Understand relevant policies and procedures

Training Objectives

- Trust, but verify
- Look at the big picture
- Report possible incidents
- ***Comply with policies***

Defensive Techniques

- Healthy suspicion
- Request a callback number on inquiries
- Check before volunteering information
- Ask “Why do you need this?”
- Report suspected incidents
- Write down details as soon as possible

Defensive Techniques

- Resist “Right now” time pressures
- Check **policies**, and follow them
- Refer questioner to IT Security
- Callback to the boss of the area
- Afterchecks

Summary

- *We have covered:*

- Types of threats
- Recognizing an attack
- Responding

CSI
COMPUTER
SECURITY
INSTITUTE

- Thank you for your patience, attention and participation