



Mechanisms of influence

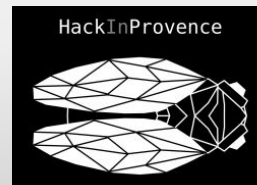
A short guide to social engineering

Who am I ?



Volker Carstein

- Student in the last year of a Master's degree in Cybersecurity
- Passionate about social engineering and offensive security
- Penguin lover
- Member of HackInProvence



Plan for today

1. What is Social Engineering ?
2. Investigate-Hook-Play-Exit
3. Pretexting
4. Establishing contact
5. Can I KISS you ?
6. Elicitation
7. Influence tools
8. Cognitive biases
9. On the universality of Layer 8 problems



What is Social Engineering ?

“Any act that influences a person to take an action that may or may not be in their best interest”

- Social-engineer.org

- Can be used for *good causes* as well as **malicious ones**
- Used by various kinds of people
 - Hackers & Pentesters
 - Spies & secret services agents
 - Sales people & managers
 - Scam artists
 - You and me ;)

Typical non-ethical goals

- Money
- Cause or ideology
- Entertainment
- Knowledge
- Ego
- Revenge

Most powerful tool in social engineering : ***Empathy***



A word of warning from Uncle Ben



Investigate-Hook-Play-Exit



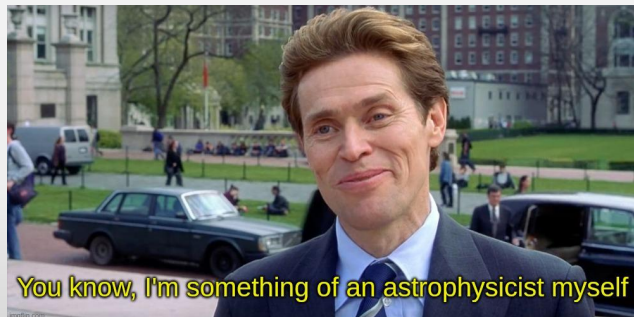
1. Investigate
 - a. Choose the target (aka “person of interest”/POI)
 - b. Gather information about POI and context
 - c. Create the *pretext*
 - d. Plan the attack
2. Hook
 - a. *Establish contact* and rapport with POI
 - b. Take control of the interaction (according to plan)
3. Play
 - a. Execute the plan
 - b. *Get what you wanted*
4. Exit
 - a. Close the interaction
 - b. Avoid arousing suspicion

Pretexting

Creating a context to help you achieve your goal.

Pretexts work by triggering emotions in your person of interest (either positive or negative ones)

- Role/Identity
- Props
- Language
- Vocabulary
- Location
- etc.



Truth-Default Theory

(Malcolm Gladwell in *Talking to Strangers*)

“our operating assumption is that the people we are dealing with are honest.”



Don't go with something too far fetched !



Pretexting

PREPARE : Framework for creating a strong pretext (Christopher Hadnagy in *Human Hacking*)

1. **Problem:** Identify the issue you're trying to solve.
2. **Result:** Specify your desired outcome.
3. **Emotional State:** Identify the emotions you want to see in your subject.
4. **Provocation:** Anticipate the emotions you need to project or display in order to generate the desired emotions in your subject.
5. **Activation:** Define your pretext, which should be very clear by now.
6. **Rendering:** Determine the specifics of where, when, and how best to deliver or render the pretext.
7. **Evaluation:** Mentally evaluate your pretext to make sure it's strongly rooted in truth and allows you to leave people better off for having met you.

A pretext fails when suspicion is raised, either by blunders or by giving away signals.

A common blunder is trying *too much* to sound convincing, which creates doubt in the POI's mind.

"Overproving kills the magic"
- Daniel Madison, card magician

Let your POI complete your
pretext in their head

Establishing contact

Hooking your target and creating common ground to get the interaction started

Internal questions in your POI's mind

(Christopher Hadnagy in *The Science of Human Hacking*)

- Who are you ?
- What do you want ?
- How long this will take ?
- Are you a threat ?

Biopsychology

Positive emotions:

- Dopamine
- Serotonin
- ***Oxytocin***

Negative emotions:

- Cortisol (stress hormone)
- Adrenaline

Rapport building -> Oxytocin -> Trust -> Win !



Establishing contact

Ten techniques to build rapport

(Robin Dreeke in *It's not all about me*)

1. Establishing artificial time constraints
2. Accommodating nonverbal
3. Slower rate of speech
4. Sympathy or assistance theme
5. Ego suspension
6. Validation
7. How ? When ? Why ?
8. Using quid pro quo
9. Reciprocal altruism
10. Manage expectations

"Sorry to bother you : I'm waiting for someone but they are a bit late. While I stand, mind if I ask you what you think of X..."

- Answer 3 of 4 of the previous question
- Validate their opinion

Appear open and friendly (body language & voice tone)

Simple technique to avoid overproving

You're not here to show off : you're here to **listen**. Most difficult technique

Elicitation questions

Reciprocity

Every interaction as an agenda. Mask it or make it about your POI

Can I KISS you ?



Keep It Simple, Stupid



Want something ? Just ask for it ! Great attacks don't have to be complicated to work well

"Give a reason, any reason..." : the printer experiment

(Ellen Lange, social psychologist)

"Can I use the copying machine before you because I'm in a rush ?" -> 94% effectiveness

"Can I use the copying machine before you ?" -> 60% effectiveness

"Can I use the copying machine before you **because I have to make some copies ?**"
-> **93% effectiveness**

Elicitation

"Act of obtaining information without directly asking for it." - *Social-engineer.org*

"Process of extracting information from something or someone" - *National Security Agency*

- **Open ended** -> "What do you think about today's weather ?"
- **Close ended** -> "The weather's beautiful today isn't it ?"
- **Neutral** -> "What do you think about today's weather ?"
- **Leading** -> "The weather is pretty hot isn't it ?"
- **Assumptive** -> "What is the biggest sum you've ever stolen from your company ?"
- How/When are good to use for open ended questions
- Why is also good but can put up your POI defenses
- *Too many questions can shut down the interaction*
- *Too little questions may make your POI uncomfortable*
- Ask only one question at a time
- A narrowing approach generally functions well
 - Neutral -> Open -> Closed -> Leading
- Assumptive questions are powerful but must be used with caution



Elicitation

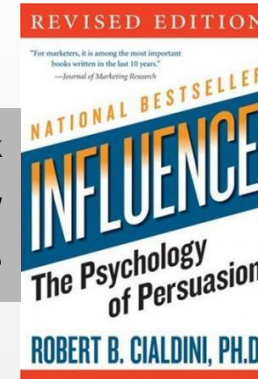
5 powerful elicitation techniques (Christopher Hadnagy in *Human Hacking*)

1. **Make illogical statements**
2. Give a bracket
3. **Help them to assume you know something or someone you don't**
4. **Feign incredulity/Make them justify themselves**
5. Use reported facts

Influence tools

1. Reciprocity
2. Concession
3. Sympathy & liking
4. Korman's self-consistency
5. Scarcity
6. Social proof
7. Authority / Expertise

One of the major book
in social psychology
and influence



Influence tools n°1 : Reciprocity

Doing something or giving a gift to your person of interest to create an “obligation”

- Asking a question : this creates an obligation to respond
- Divulging a piece of info : may create an obligation in your POI mind to do the same
- The exchange of gifts and services increase trust, which lead to even bigger gifts and services, etc.

Coke bottle experiment

Case 1 : Person B offers a Coke bottle (10 cents) to Person A

Case 2 : No gift giving

In both cases, Person B says that they sell lottery tickets (25 cents each) and if they sell a lot of them they'll win 50\$.

Then Person B asks Person A if they want tickets.

In case 1, Person B sold **two times more tickets** than in case 2.

The experiment reported that in case 2, number of tickets bought was correlated with Person A appreciation of Person B. But it wasn't the case in case 1 : **Person B created an obligation**

Influence tools n°2 : Concession

Conceding on something to make your person of interest do the same
Sometimes considered to be a variation of Reciprocity

- Same rule as in Reciprocity
 - You make a concession to create an obligation in your POI to do the same
- The concession must be on something that matters **to your POI** (remember that empathy is key)
- If your POI refuses something, give them a choice : they'll be more likely to comply after



Influence tools n°3 : Sympathy & liking

Your person of interest is more likely to comply to your requests if they like you

Like-inducing techniques

- Physical appearance
- Similarity
- Compliments/Positive reinforcement
- Cooperation
- Association

Tribe mentality

We like more people that appear to be like us.

To be liked, seem to be from the same "tribe" as your POI.
Use vocabulary, expression, social codes, appearance, etc.

Appear supportive of your POI to make them like you.
Must be at least a bit sincere otherwise will backfire

Make your POI think you're both in the same team

Your POI will like you more if they associate you with things they like



Influence tools n°4 : Korman's self-consistency

An individual behaves to stay consistent with their decisions, the image they have of themselves and with what others think of them. Failing to stay consistent causes internal conflict.

- Cognitive routine to avoid too much decision-making
- Horse race gamblers example
 - Before betting : not sure about the outcome
 - After betting : absolutely convinced their horse will win
- Commitments are affected too !

Commitment escalation



Foot-in-the-door technique : Make your POI agree to something minor to make them agree to something bigger after

Influence tools n°5 : Scarcity

What is rare is desirable



- Make offers limited in time
- Appear busy to make your time seem more valuable
- Implant the idea in your POI that they're special for you
 - Say a "little secret" or something you won't go and tell everyone -> Also uses Reciprocity !

Make your POI act without thinking too much, bypassing usual cognitive processes involved in decision-making

Influence tools n°6 : Social proof

We believe something is good or appropriate if peers think it is

“Top 50 songs effect”

- Songs are branded as popular
- So people think they're good and listen to those songs...
- ... making them even more popular

How to exploit : brand something as popular or validated by known peers of your POI

“Looking-up experiment”

(Milgram, Bickman, and Berkowitz)

A certain number of accomplices stand looking up at the sky on 42nd Street, New York City
How many passersby will look-up too ?

One accomplice : 45% of passersby
15 accomplices : **85%** of passersby (blocking the sidewalk)



Influence tools n°7 : Authority/Expertise

We follow and listen more to people appearing to have legitimate authority or expertise

- Three types of **authority**



- **Legal** : law enforcement and military

- **Organizational** : company hierarchy

- **Social** : a person which appear to have legitimacy to be the leader in any social group



- This status is usually obtained by confidence and social proof

Influence tool to be used in a pretext,
tailored to your POI (and laws)

Expertise

Appear to be knowledgeable or competent in a domain to be considered as an expert of it

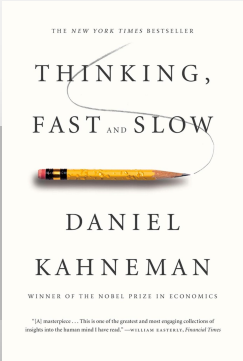


Your POI will not have suspicion about what you say in your domain of expertise

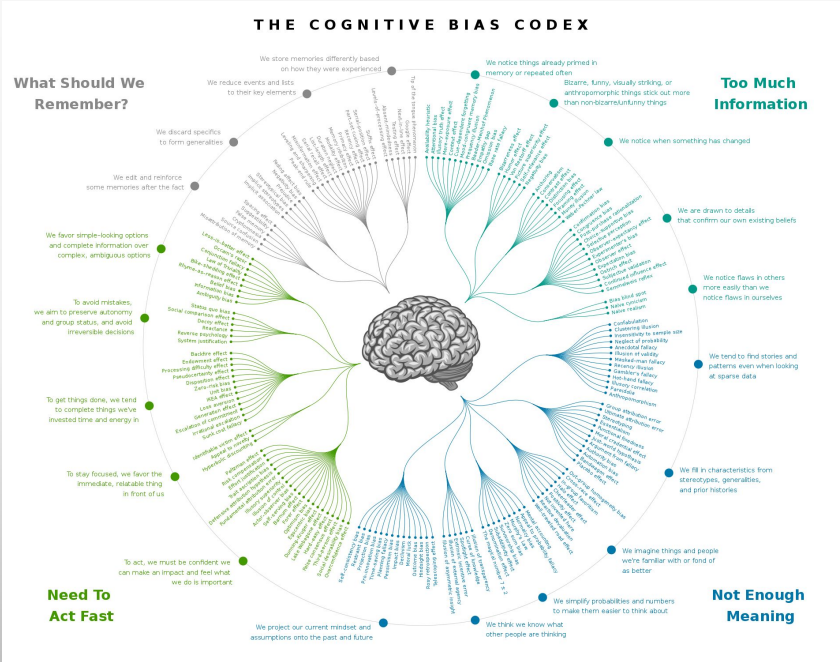
Cognitive biases

- 1. Halo effect
- 2. Loss aversion
- 3. Framing effect
- 4. Primacy effect

Great book about cognition and cognitive biases



Shortcuts used to speed up and facilitate cognition, at a cost



Cognitive bias n°1 : Halo effect

Tendency for positive impressions of a person, company, brand or product in one area to positively influence one's opinion or feelings in other areas

Based on stereotypes and mental images of things

- Well dressed
 - Seriousness
 - Credibility
 - Higher status
 - Educated
 - etc.
 - Intelligent
 - Supposed authority



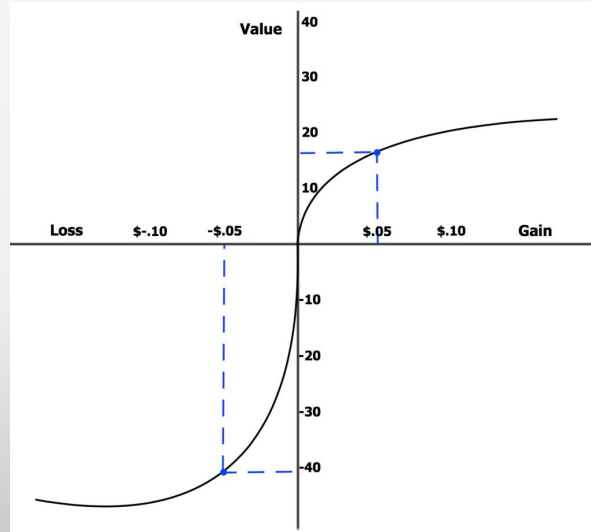
Part of the pretext

Found in

- Authority/Expertise
- Sympathy & liking

Cognitive bias n°2 : Loss aversion

Tendency to prefer avoiding losses than acquiring equivalent gains



We fear to lose what we have

If something threatens a thing we possess, Loss aversion kicks in and forces immediate action



Attack exemple : if you don't do X, your account for Y will be permanently locked

Cognitive bias n°3 : Framing effect

Processing of information through certain senses depending on the individual

99¢

£3.99



Present information in an appealing way or a way that orientates the choice

Seeing a picture of their kids on your POI's desk, instead of saying "What's your kids names ?" (which can appear creepy), say "Is the one on the right the oldest ?"

Cognitive bias n°4 : Primacy effect

Tendency to recall primary information presented better than information presented later on

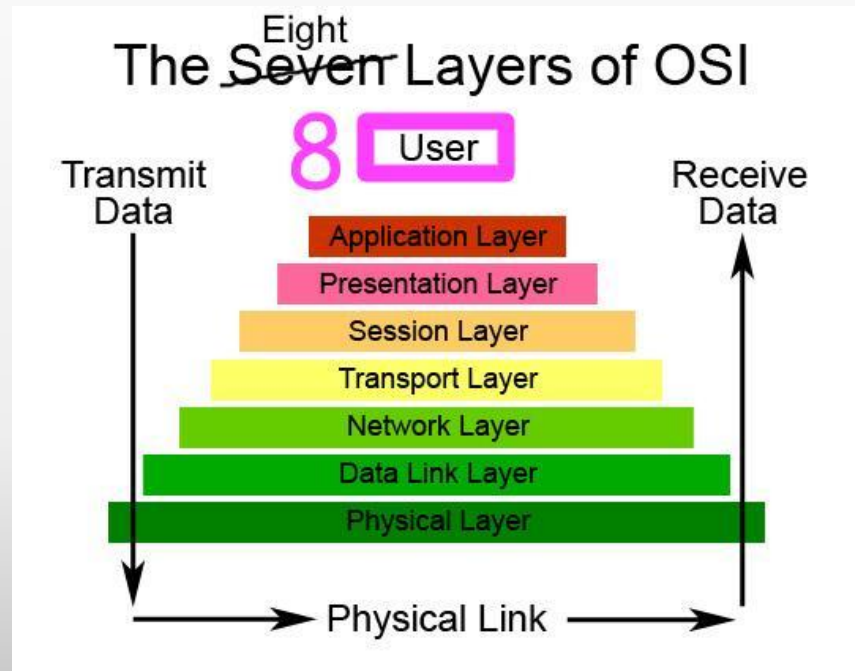
Principle of
*"first-impression-that-is-difficult-
to-change-afterward"*

Largely used during advertising
campaigns for a new product

Used when establishing contact or
when trying to convince the POI



On the universality of Layer 8 problems



- Humans make mistakes and are vulnerable to social engineering
- We are humans
- **Therefore, we make mistakes and are vulnerable**

Blind spot bias: Tendency to believe that only others are affected by cognitive biases and we are not.

Solution : Awareness & Regular Training

References and acknowledgment

- Christopher Hadnagy (All of his books, mainly *The Science of Human Hacking* and *Hacking Humans*)
- Robert Cialdini (*Influence : the psychology of persuasion*)
- Christina Lekati (*Beyond Influence Techniques* talk at Layer 8 Conference)
- Dale Carnegie (*How to win friends and influence people*)
- Vincent Joule et Jean-Léon Beauvois (*Petit traité de manipulation à l'usage des honnêtes gens*)
- [Cognitive Bias Codex](#)
- Daniel Kahneman (*Thinking, Fast and Slow*)

Thank you !



SecSea crew, HackInProvence, and you all !



Volker Carstein

 @volker_carstein

Feel free to send me a message if you want the slides and/or want to talk, DMs are open !