Social Engineering

Stefano Longari, Stefano Zanero

What will be in this course?

We'll discuss what is Social Engineering, and specifically what you can prevent and what you can detect.

We'll comprehend the steps, techniques, tools and elements that we can use to implement a social engineering attack.

Please be mindful that although the knowledge and explanation of many of these topics is legal and ethical, the implementation of these in the real world is illegal unless with compliance of the other attacked part.

What is Social Engineering?

What is Social Engineering?

“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 D. MITNICK & William L. Simon - Art of Deception

“The art, or better yet, science, of skilfully manoeuvring human beings to take action in some aspect of their lives”

- Christopher Hadnagy

“The psychological manipulation of people into performing actions or divulging confidential information”

- Wikipedia

What is Social Engineering?

Basic Example:

- Convince a “friend” you would help fix his/her computer
- Fix minor problems on the computer and secretly install control software

S.E. Is composed of many different topics, and is a complex matter overall. Besides, it highly relies on the imagination, goals and knowledge of the attacker, hence it is hard to “define” a set of possibilities, but it is still important to comprehend the means that an attacker can have.

Knowing the weapons, you can learn how to defend from them.

What is Social Engineering?

Basic Examples:

The Nigerian Prince Scam

- Email/Letter requesting the victim to help a Super rich “nigerian prince” into retrieving the money from an account. In exchange for only some little help.
- After some work, a small issue comes out and the victim should pay a little to overcome it
- ...and other issues on, and on, and on


PBS
NEWS
HOUR

What is Social Engineering?

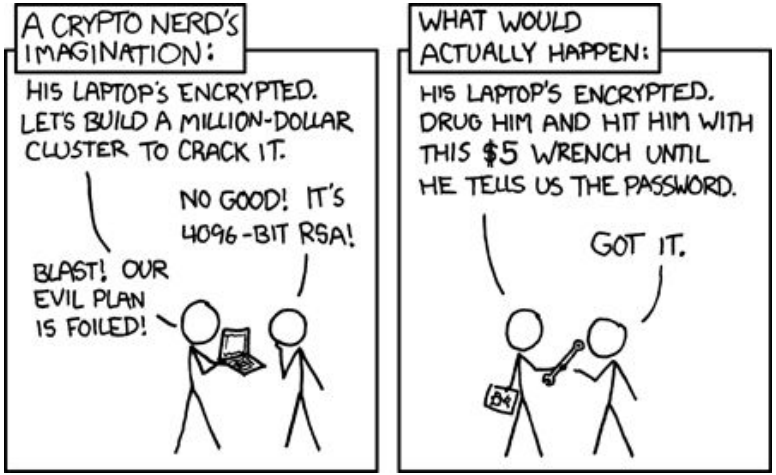
Basic Examples:

Politicians and the “power of scarcity”

- Scarcity of a resource scares and inherently leads people to “vote” for whoever promises to bring said resource, e.g., jobs, food, security...
- Can be exploiting an existing situation
- Can create a situation to exploit its bad results

Why Social Engineering?

It consistently works, while technology vulnerabilities are hardened and solved



“You could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain vulnerable to old-fashioned manipulation.” -Kevin Mitnick

Why Social Engineering?

People are the largest vulnerability in any network or security chain!

- No technology in the world can prevent social engineering!
  - There is no patch for human stupidity!
- Path of Least Resistance
  - Why spend hours, days, weeks to crack a password when you can just ask for it?

TECNICHE DI ATTACCO PER TIPOLOGIA	2011	2012	2013	2014	2015	2016	Variazioni 2016 su 2015	Trend 2017
SQL Injection	197	435	217	110	184	35	-80,98%	↓
Unknown	73	294	239	199	232	338	45,69%	↑
DDoS	27	165	191	81	101	115	13,86%	↗
Known Vulnerabilities / Misconfigurations	107	142	256	195	184	136	-26,09%	↓
Malware	34	61	57	127	106	229	116,04%	↑
Account Cracking	10	41	115	86	91	46	-49,45%	↓
Phishing / Social Engineering	10	21	3	4	6	76	1.166,67%	↑
Multiple Techniques / APT	6	13	71	60	104	59	-43,27%	↓
0-day	5	8	3	8	3	13	333,33%	↑
Phone Hacking	0	3	0	3	1	3	200,00%	↑

Goals of a Social Engineer:

Mainly two Goals:

- Obtain Data / Information
- Obtain Actions

Mainly two Risks (or Assets, generally for companies/entities):

- Money
- Power
- “Terror”

Types of Social Engineers:

- Hackers (“black hats”)
- Penetration Testers (“white hats”)
- Spies
- Identity Thieves
- Scam Artists
- Salespeople
- Governments / Politicians
- Doctors/Psychologists/Lawyers
- Friends/Children/Lovers

... Basically everyone

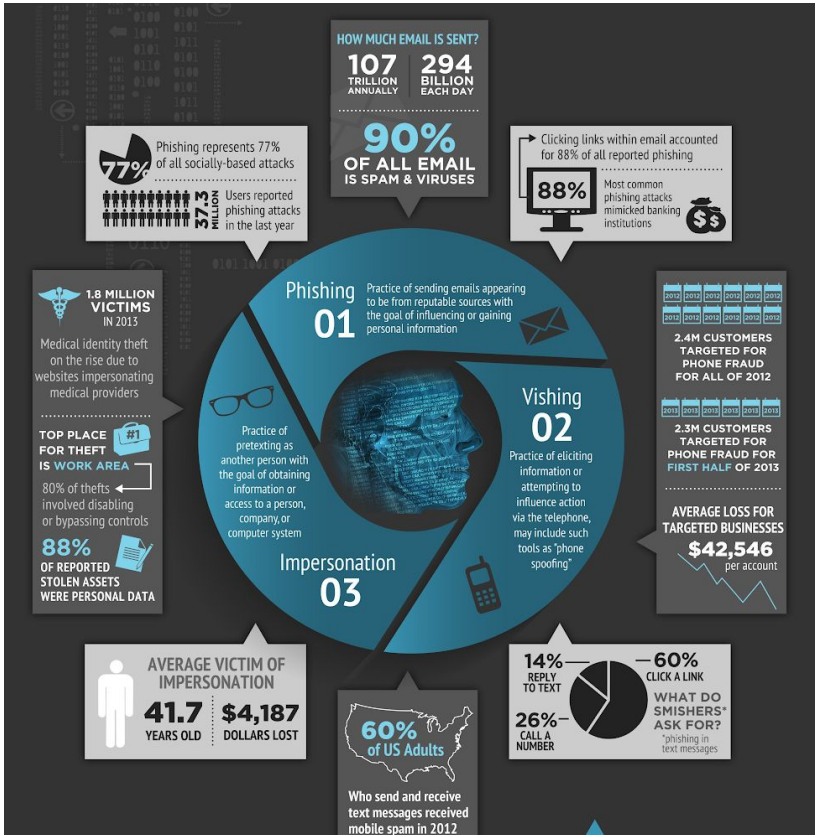
Requirements of a Social Engineer:

Even just a fraction of these can make you capable of doing some SE attacks.

- Academically, nothing.
- Charisma / Good acting
- Psychology knowledge / Behavioral analysis / Empathy
- Computer Security / Physical Security Skills
- Experience
- AUTHORIZATION.

Most common techniques for S.E. Attacks

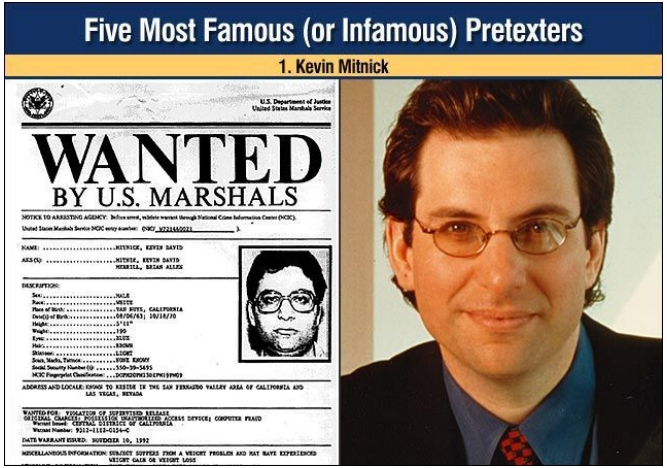
- Phishing (and a whole set of subcategories)
- Vishing
- Impersonation / Physical



Most common techniques for S.E. Attacks

Famous Social Engineering Case: Kevin Mitnick

American computer security consultant, author, and convicted hacker, best known for his high-profile 1995 arrest and five years in prison for various computer and communications-related crimes



Famous Social Engineering Case: Frank Abagnale

- Currently American security consultant
- Background as a former con man, check forger, and notorious impostor while he was between the ages of 15 and 21.
- Claims to have assumed no fewer than eight identities, including an airline pilot, a physician, a U.S. Bureau of Prisons agent, and a lawyer.
- Abagnale escaped from police custody twice (once from a taxiing airliner and once from a U.S. federal penitentiary) before turning 22 years old.
- He served less than five years in prison before starting to work for the federal government.

Step 1: Information Gathering

OSINT - Open Source Intelligence

Refers to everything that can be found just by “searching”, usually to build a profile

Company Websites
Social Media
Collaboration Websites (forums, markets...)
Google
Maltego

Whois
Nmap

Public Reports

OSINT - Open Source Intelligence

General goal is to find one of two things:

Information that can be used to impersonate or “trick” the target
Information that can be used to find the above information

What can be useful depends strongly on context.
Family and friends are often useful
Interactions with people outside the NET
Events he/she participated in
Interests, hobbies, sports and so on...

Reconnaissance

Physical reconnaissance is extremely useful, specifically if the goal is that of physically entering the place.

Points to look out for:

- What do the employees use to access the building
- Are there “weak” locks? - answer is probably yes
- Are there smoking areas
- Cameras, Elevators
- Exposed keys/Common keys
- Paths to points of interest
- Badges appearance, Security Company Logos…

Exercise 1:

Make groups of 3-5 people. https://docs.google.com/spreadsheets/d/1uayujogCsRrulktJBahvHUCv4twqi9s_jfnYyc6-4Ek/edit?usp=sharing

Context: Imagine your goal is to find a way to force someone to click on a fake website and to insert its credential.

First step is that of discovering as much as possible on the target. Assuming that the target could be:

- Me (Stefano Longari)
- You
- A well known public figure of your choice

Produce a report with all the information that you deem interesting on me and the public figure. Do the same for you, but don't share it with me.

Send both as attachments to this email, with the title EXE1_group(number)
secoursepolimi@gmail.com

7:55

Step 2: Pretexting

What is Pretexting?

“The practice of presenting oneself as someone else to obtain private information”

Pretexting means creating a scenario that helps the attacker justify the requests and obtain the final goal he had.

Importance of Pretexting?

- One of the most important aspects of social engineering is **trust**.
  - If you cannot build trust you will most likely fail.
- Pretexting is often used to gain **trust**
  - A solid pretext is an essential part of building trust.
  - Trust doesn't mean that the victim has to like you, but has to trust that you are telling the truth
- Used by federal and local law enforcement, private detectives, reporters, interrogators.

Pretexting basic principles

The two common requirements to create a pretext are

1) A character, a person you're acting as, whether it is real or fake
2) A plausible situation in which there is reason for the victim to bring you to your goal

Pretexting Basic Principles

- A crucial aspect is planning and research
  - Know your target
- Good acting definitely helps
  - Your pretext should appear spontaneous
  - Authoritative voice, earnest tone
- Keep it simple
- Use information that needs no verification
- Adapt to the scenario on the fly in response to interactions with the target.
  - Create a pretextual scenario if the target decides to be more careful

Pretexting Planning

- While planning your pretext it is imperative to consider a few key questions:
  - What problem am I trying to solve? Aim to achieve ?
  - What questions am I trying to answer?
  - What information do I seek?
    - Sensitive, non-sensitive, privileged
  - The nature of the person whom we will be contacting

Pretexting: Character Creation

- Developing a pretext -> Essentially creating a character.
- Complexity of the character is determined by the planned depth of interaction with people at target site
  - A pretext can be as simple as just being friendly to someone during a conversation or ...
  - as complicated as a full blown fake identity complete with ID's, public records, and all the trappings of a normal person's life
    - social networking pages, blog postings.

Example: Stanley Mark Rifkin

One of the biggest bank heists in American history.

Rifkin was a computer geek that ran a computer consulting business out of his apartment

One of his clients was a company servicing the computers at Security Pacific Bank

What did he do?

He entered the bank's building as a computer worker

Through the elevator he reached the level where the wire transfers were done

Memorized the secret code of the day for wire transfers and left

Ordered a transfer for 10.2 Million dollars to himself through phone by impersonating someone from the bank's international division

Example: Stanley Mark Rifkin

Premeditation

Props

Confidence/Comfort

Believable story

Spontaneity to go with the flow of questions

Exercise 2:

Create your Pretext:

Consider the previous analysis that you did on me. Imagine you're an attacker that now wants to plan the actual attack. Remember that the final goal of the attack is to convince me to click on a link and to insert my credentials in the linked page.

- Create a character, which has to be a person / company / similar, and create its own social media page, comprised of fake images, some posts…
- Create a report where you briefly describe what you did in the page (Information you put in and so on) and what is your overall strategy.

2 things i DO NOT WANT YOU TO DO:
1) do not add friends, especially people from the actual company you're claiming to be. (it would be a smart tactic for the actual attacker)
2) do not claim to be "Facebook", "Instagram", to work for any firm or company that you know. If you want to fake being a big company or a person working for it, write it to me in the report and invent a name.
I.E. you want to fake being facebook's CEO Mark Zuckerberg: On the report, the first thing you write is "We fake being Facebook's CEO Mark Zuckerberg, we changed Facebook name into Armmovie and Zuckerberg into Walter White"

Send the report, the link to the social media page and a couple of screenshots of the important parts of the social media page to this email, with the title EXE2_group(number)
secoursepolimi@gmail.com

Step 3: Elicitation

Elicitation

“Elicitation is the process of extracting information from something or someone without directly asking for it”

...Or without the person understanding the outcome of giving such informations

Exploit Human Nature

Most people want to:

- be polite, helpful;
- appear well informed;
- be appreciated;

Elicitation

In the case of an individual or group of people, this is something we do everyday by talking, listening, and asking questions.

- Get to know people better.
- Make mental judgments of **IF** and **HOW** to develop a relationship with a person.

Elicitation techniques

- Educate yourself before approaching the target
- Appeal to the target’s ego
- Express Mutual Interests
- Build Rapport
- Volunteer Information
- Assume Knowledge
- Preloading
- Alcool
- Questioning Techniques

Questioning Techniques

Neutral | **Open** | **Closed** | **Leading** | **Assumptive**

Does not direct the target on how to answer

No leading or directing

“How do you like the weather today” ?

Questioning Techniques

Neutral | **Open** | **Closed** | **Leading** | **Assumptive**

Encourage a full, meaningful answer using subject's own knowledge and/or feelings

"Tell me about your relationship with your father"

"How do you feel about election candidates"

Questioning Techniques

Neutral | **Open** | **Closed** | **Leading** | **Assumptive**

Give us control of the conversation and allow us to lead where it may not go

“Who are you going to vote for ?”

Questioning Techniques

Neutral | Open | Closed | **Leading** | Assumptive

Question that subtly prompts the respondent to answer in a particular way.

“You were at the bar with her last night, weren’t you?”

Questioning Techniques

Neutral | Open | Closed | Leading | **Assumptive**

Questions that assume some knowledge is already in the possession of the target.

“Where does Mr. Smith live?”

Elicitation: Key Points

- Important key points in mind:
  - Too many questions can shut down the interaction
  - Too little may make the person uncomfortable
  - Participate in the interaction, it shouldn’t feel like an interrogation
  - Ask only one question at a time, too many will cloud the answer you get
  - Use a narrowing approach to questions to gain the most information (adapt yourself):
    - i.e. Neutral Questions ---> Open Ended ---> Closed Ended ---> Leading ---> Assumptive

Attack Vectors

Attack Vectors

What are the most common ways to obtain the attacker's goal?

"Cyber"

- Phishing
  - Spear Phishing - Targeted phishing
  - Whaling - Targeted phishing towards VIPs
  - Angler Phishing - Spoofing customer service
  - Fee Scams - you give you receive e.g. nigerian
- Smishing - SMS/Message phishing
- Vishing - Phone Call phishing/scam
- Scareware - Detect a fake virus, ask to download smt

"Physical" and general

- Piggyback / Tailgating
- Baiting - Free giveaways / Drop USBs on the ground
- Honey Traps - Romance / Sexual scams
- Quid pro Quo - Give something to receive something

Vishing Example

Phishing Test - Shorter Exercise

- https://phishingquiz.withgoogle.com/?hl=en

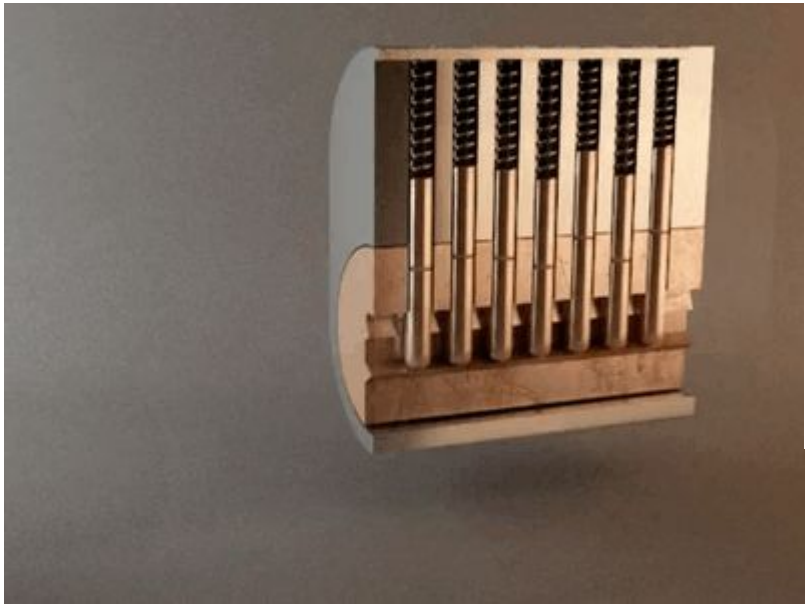
- https://www.phishingbox.com/phishing-iq-test

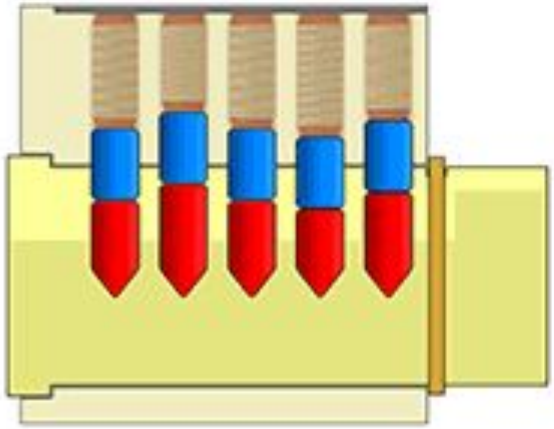
Send me (**secoursepolimi@gmail.com**) the sequence of answers you gave to the second one, justifying the phishing ones with a sentence that explains why it was phishing. send an email with “EXE3_(surnamename)” as title

Attack Tools

Physical Tools: Costumes, Badges and Logos

Physical Tools: Lockpicks

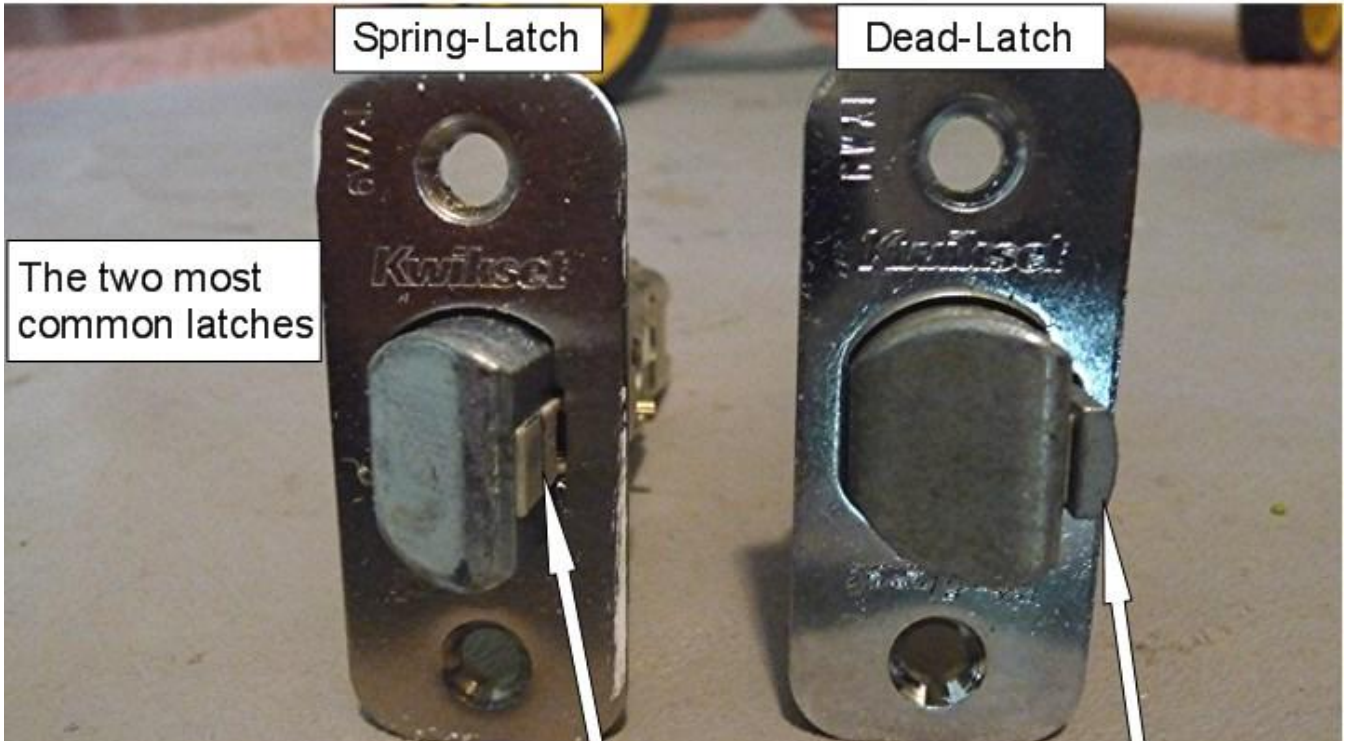




Physical Tools: Shims and similar

Physical Tools: Shims and similar

Physical Tools: Shims and similar



Physical Tools: Access Related Stuff

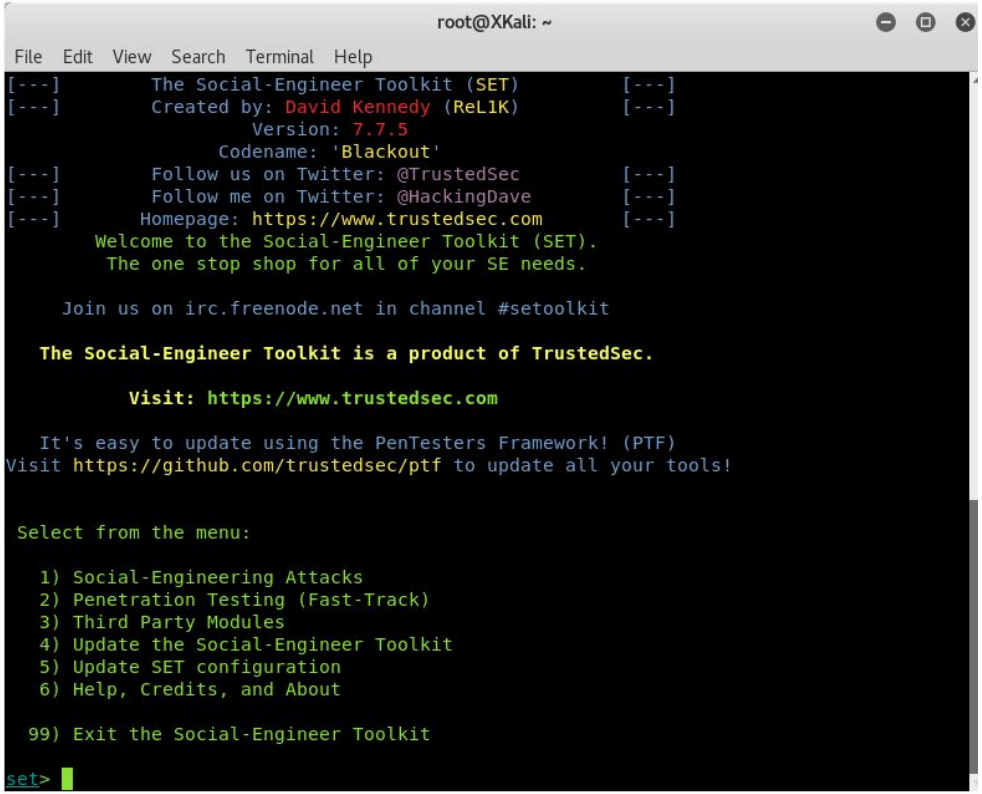
Physical Tools: Access related stuff

Informatic-ish Tools: Cameras and GPS trackers

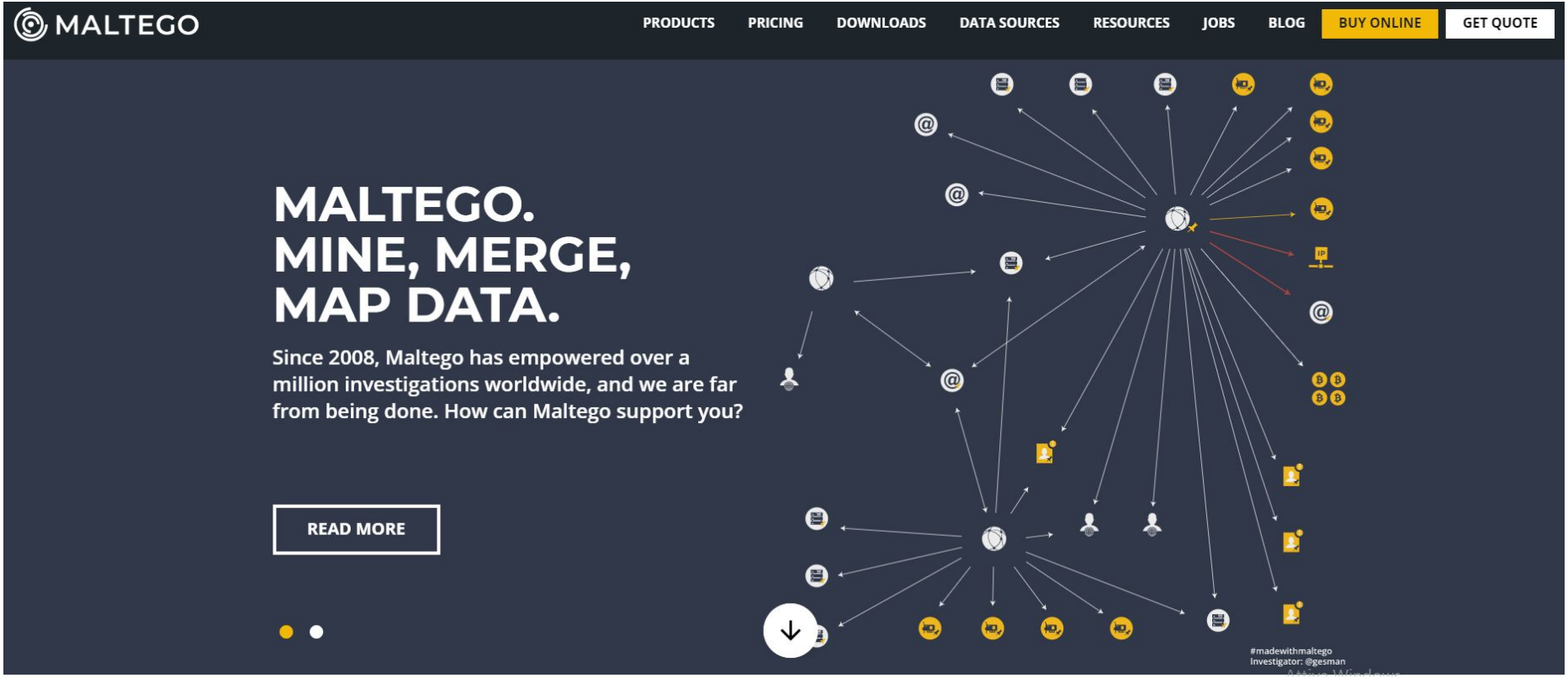
Informatic-ish Tools: NFC Spoofer (Badge Cloner)

22:45

Informatic Tools: Social Engineer Toolkit (SET)



Informatic Tools: Maltego & Info Miners



Informatic Tools: EMKEI's Mailer

Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

From Name:

From E-mail:

To:

Subject:

Attachment: Scegli file Nessun file selezionato

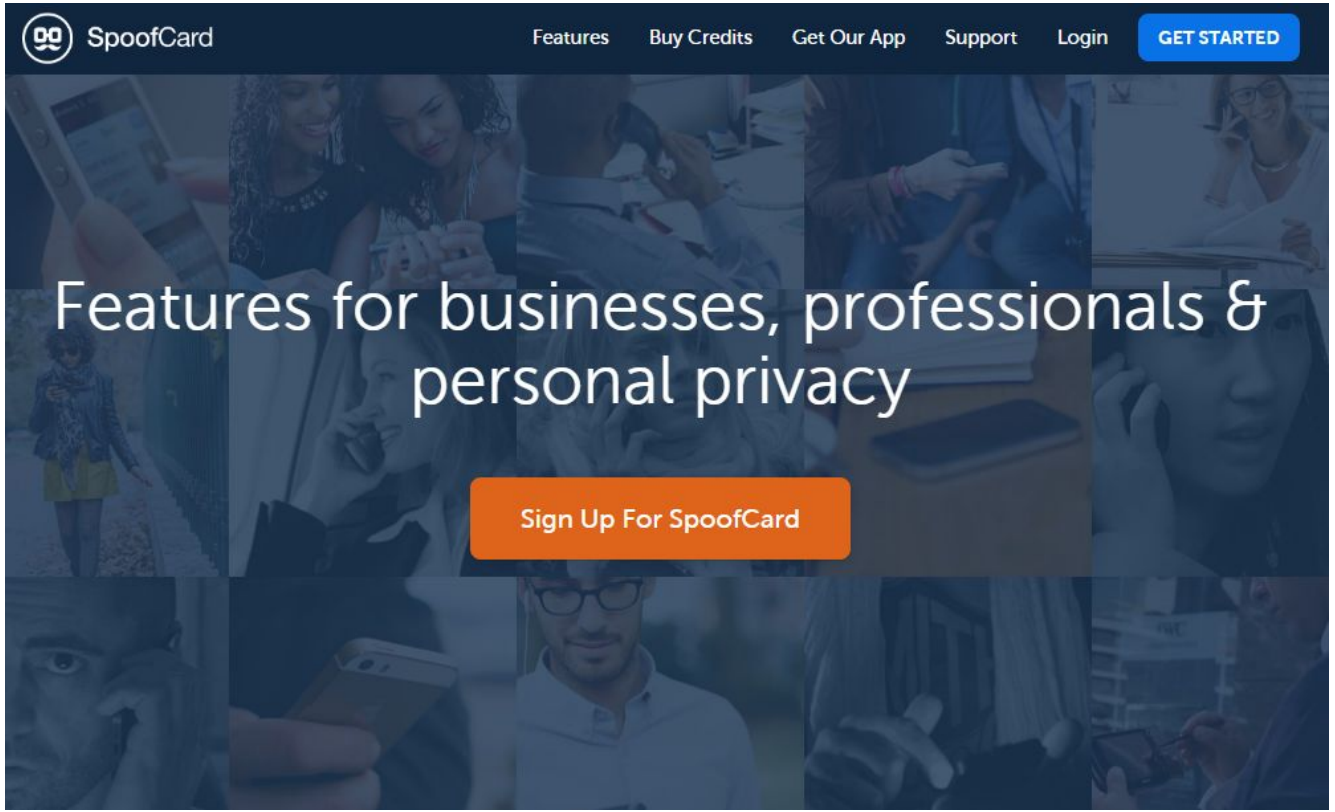
Attach another file

Advanced Settings

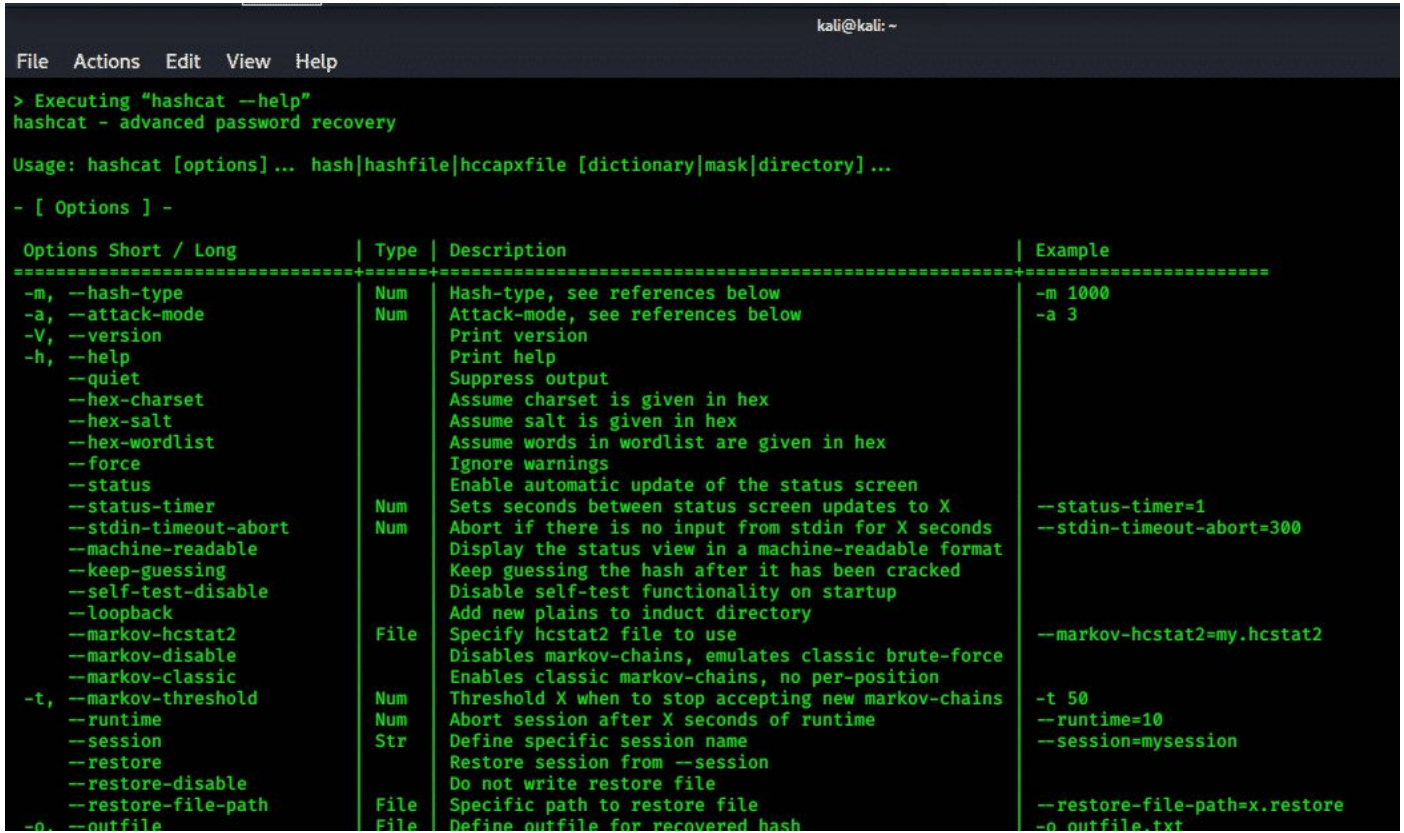
Content-Type: text/plain text/html Editor

Text:

Informatic Tools: SpoofCard



Informatic Tools: Password Crackers



“Psychological” Principles

“Psychological” Principles

Brief disclaimer: I’m not a psychologist, hence if you want to know the details of what I’m going to explain please read related books or discuss with behavioral psychologists

Communication Models:

Communication is the process of transferring information to one entity to another.

It entails a two way process between at least two agents, an exchange of information, and the development of some “ideas”.

A sender generates a “package” and sends information through a medium to the receiver, which decodes the message and in some way sends a feedback to the sender.

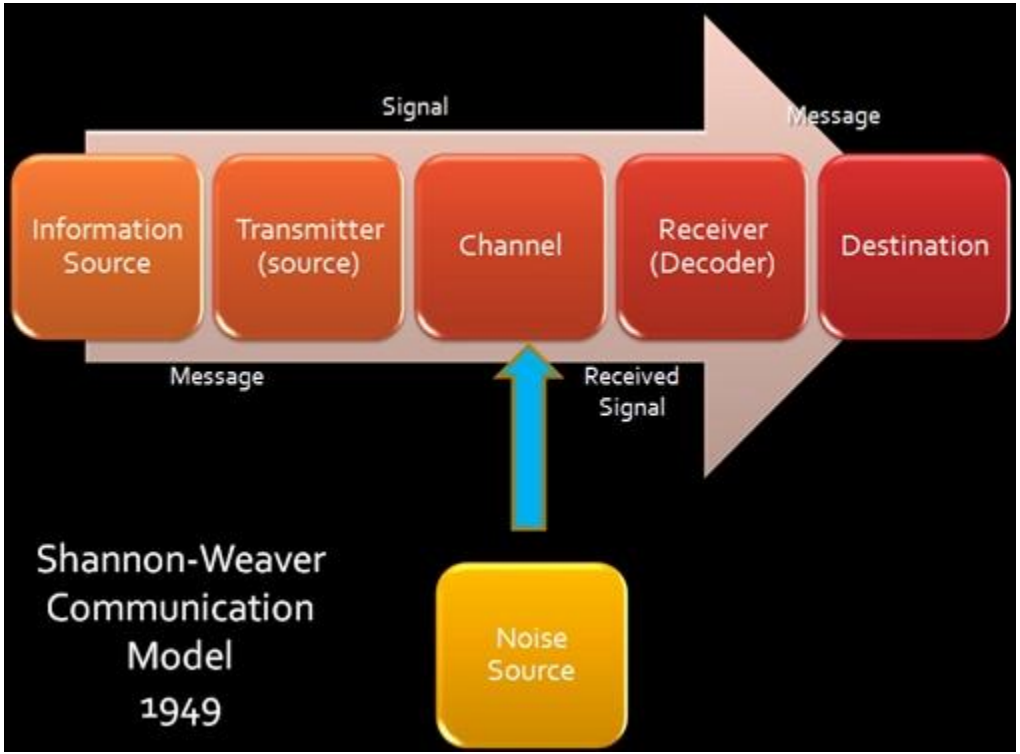
... So?

Communication Models:

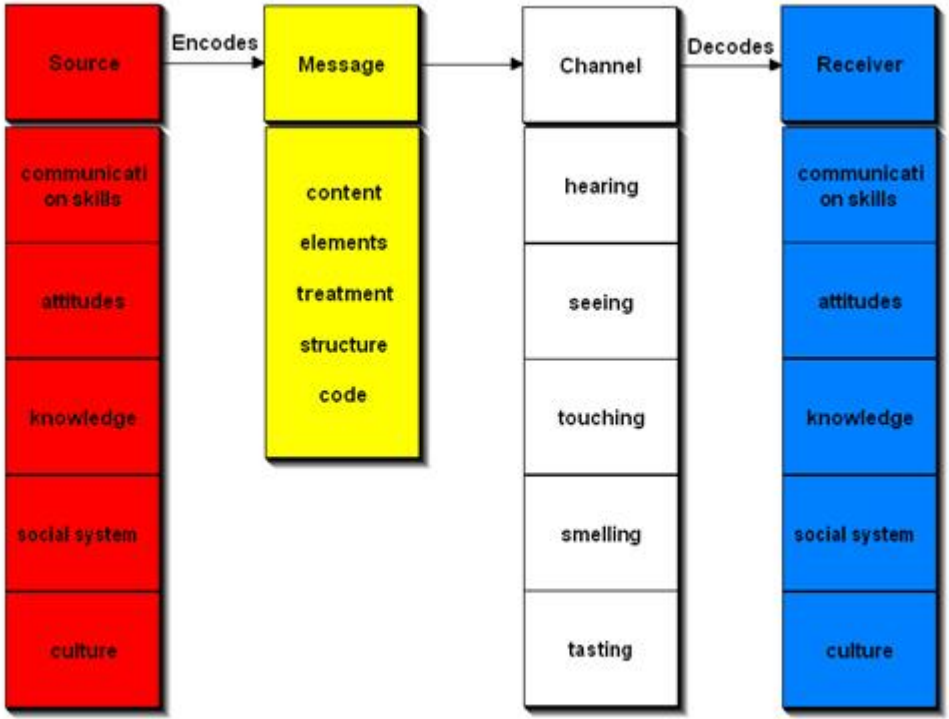
Understanding communication models means understanding what’s going on in our brain but most importantly in the brain of the other entity.

The better you are at understanding how the other part’s reasons, the easiest it is to transfer a concept

Communication Models:

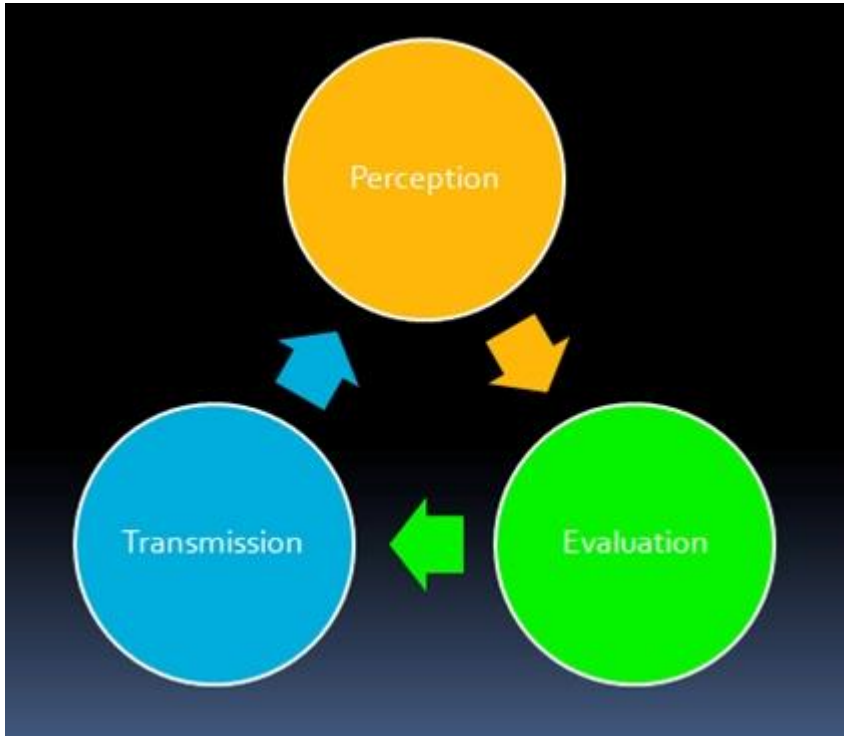


Berlo's Model of Communication

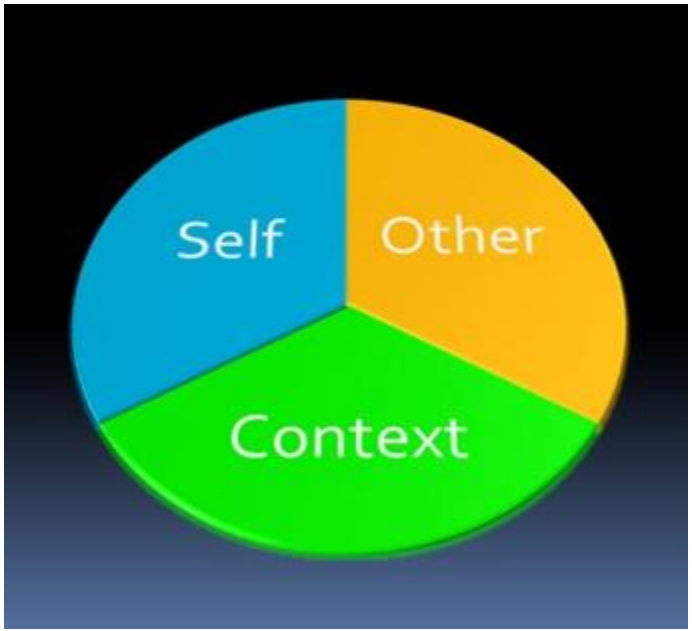


A Source encodes a message for a channel to a receiver who decodes the message: S-M-C-R Model.

Communication Models: Phases



Communication Models: Coping Stances



BLAMING

PLACATING

SUPER REASONABLE

IRRELEVANT

Body Language and Nonverbal Communication

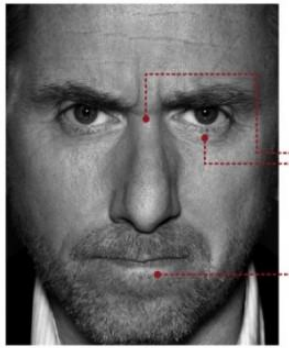
Body language refers to non verbal signals we use to communicate

Conveys a lot of information without speaking

Automatic process, both for the “speaker” and the “receiver”

All about conveying the correct emotion and understand the other’s reaction

“Micro”expressions

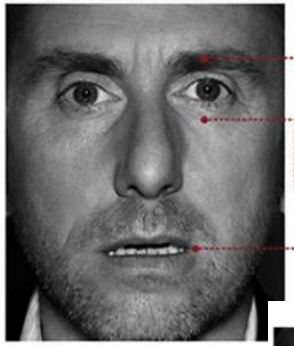


anger

1. eyebrows down and together
2. eyes glare
3. narrowing of the lips

fear

1. eyebrows raised and pulled together
2. raised upper eyelids
3. tensed lower eyelids
4. lips slightly stretched horizontally back to ears



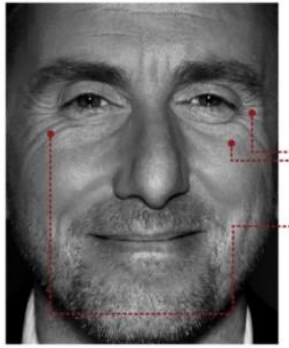
surprise

Lasts for only one second:

1. eyebrows raised
2. eyes widened
3. mouth open

contemp

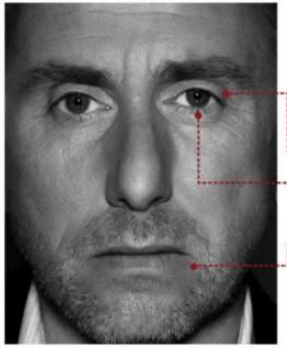
1. lip corner tightened and raised on only one side of face



happiness

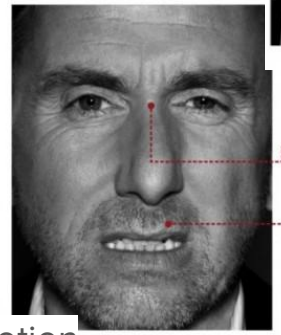
A real smile always includes:

1. crow's feet wrinkles
2. pushed up cheeks
3. movement from muscle that orbits the eye



sadness

1. drooping upper eyelids
2. losing focus in eyes
3. slight pulling down of lip corners



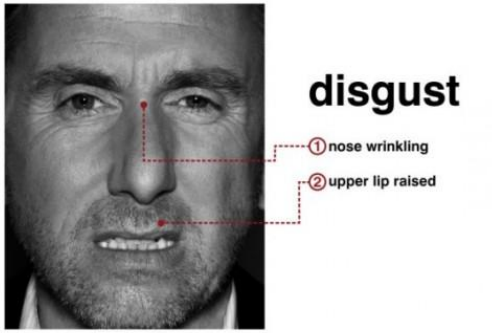
disgust

1. nose wrinkling
2. upper lip raised

A **micro expression** is an involuntary facial display of one's true emotion

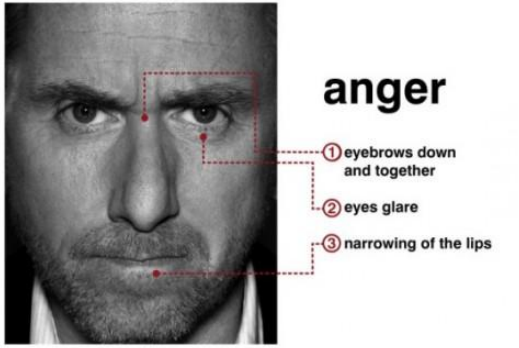
Examples

Examples

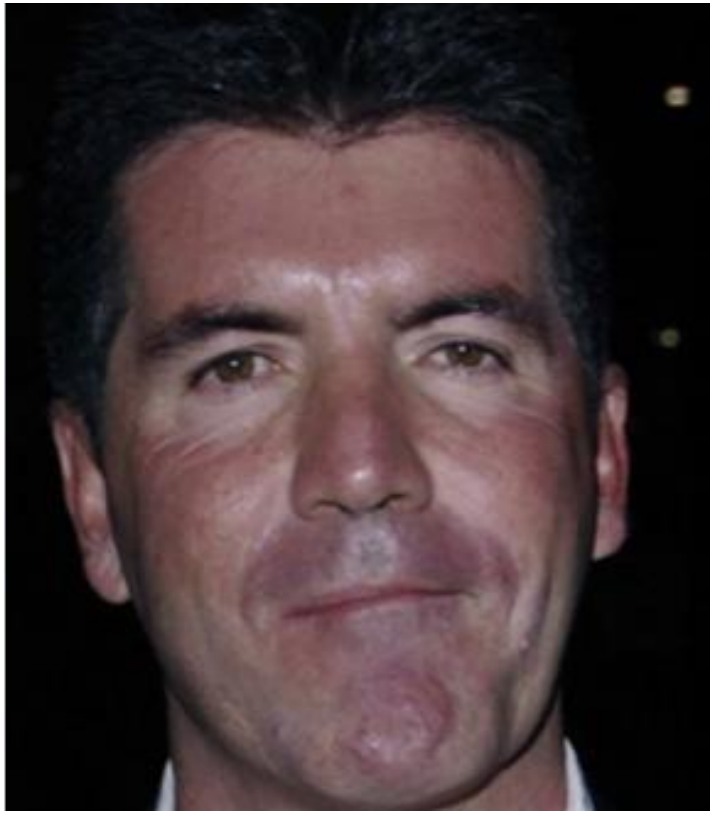


Examples

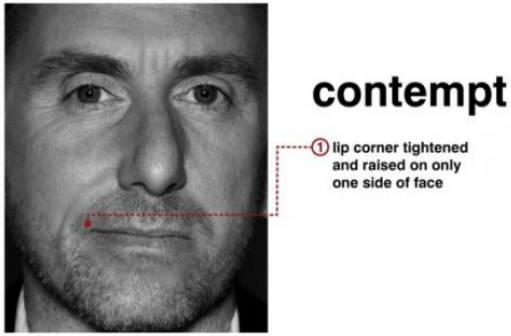
Examples

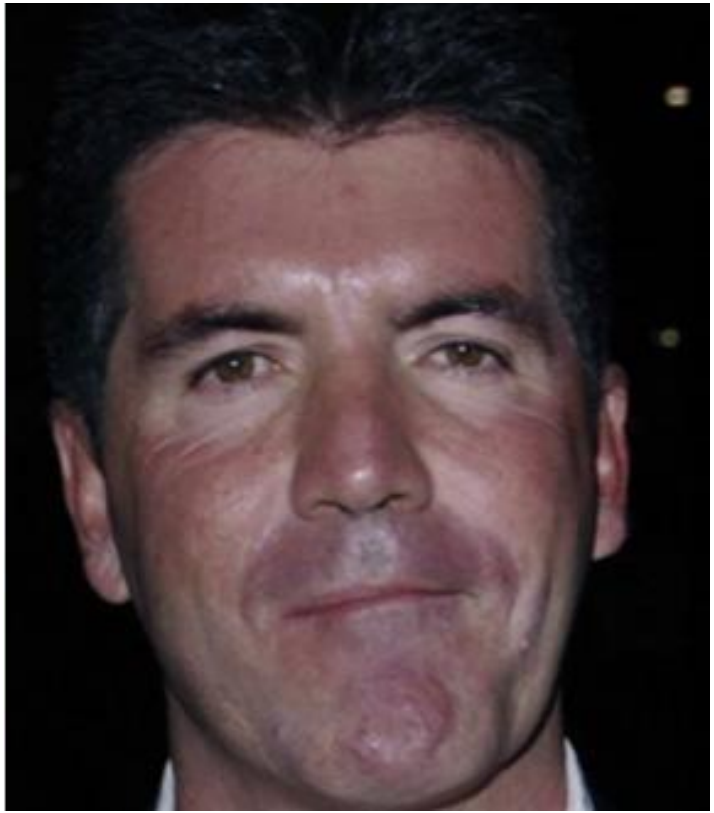

anger
1 eyebrows down and together
2 eyes glare
3 narrowing of the lips

Examples

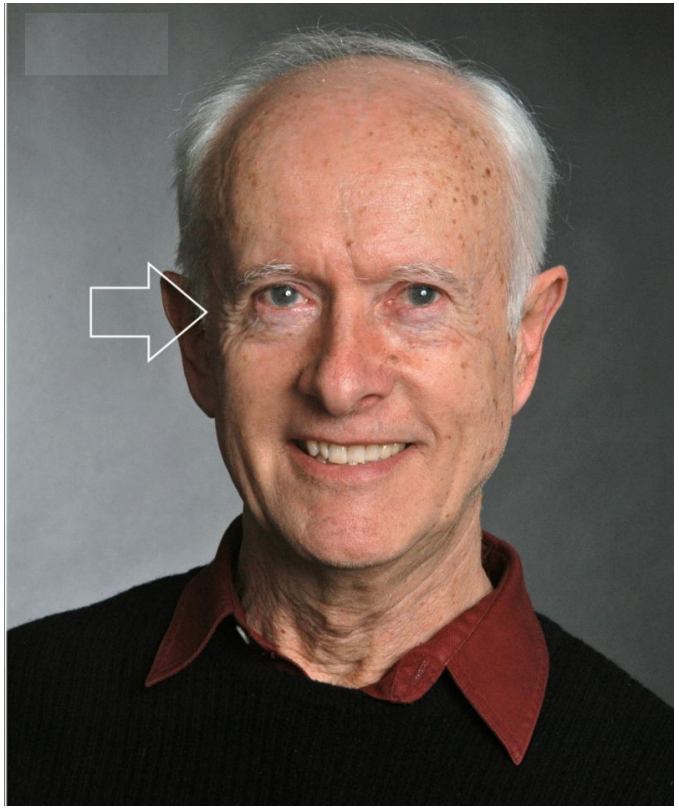


Examples

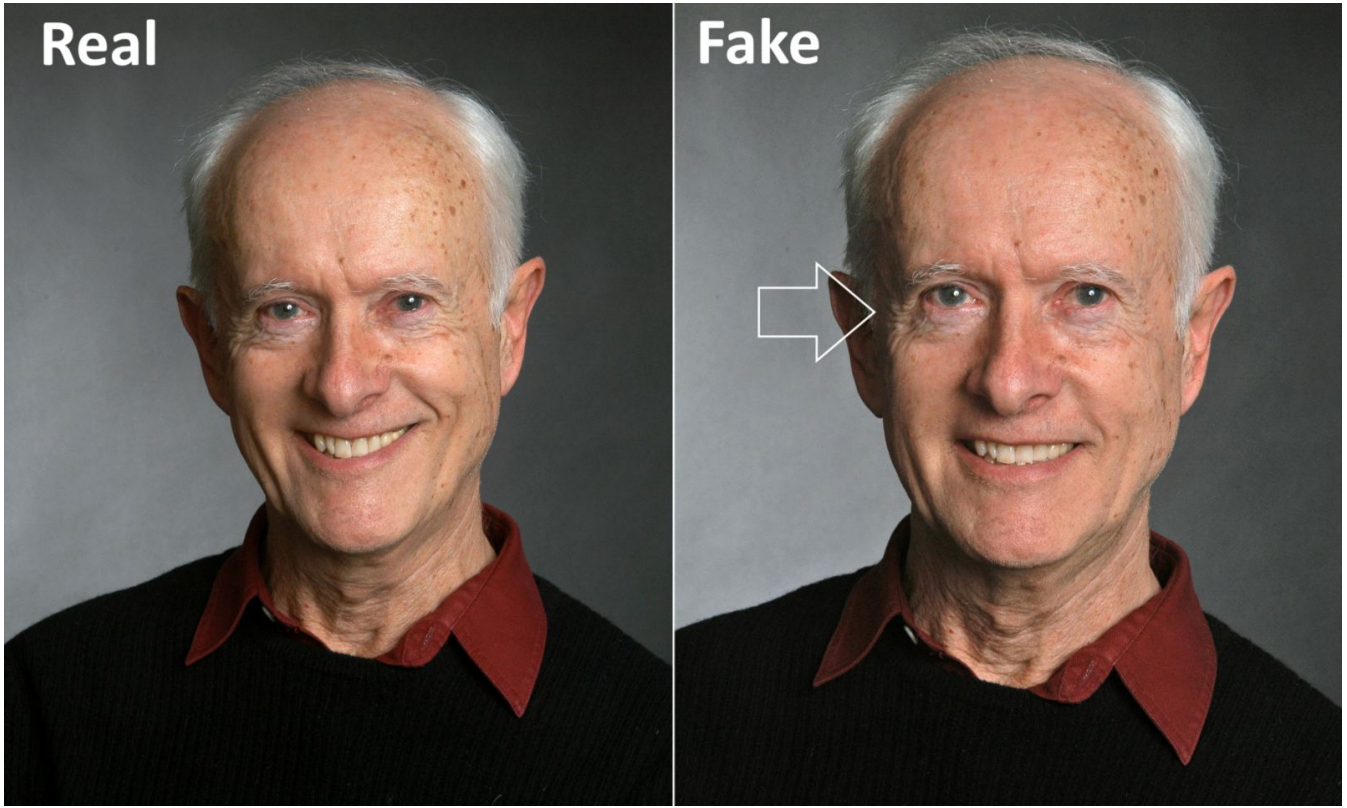

contempt
1 lip corner tightened and raised on only one side of face



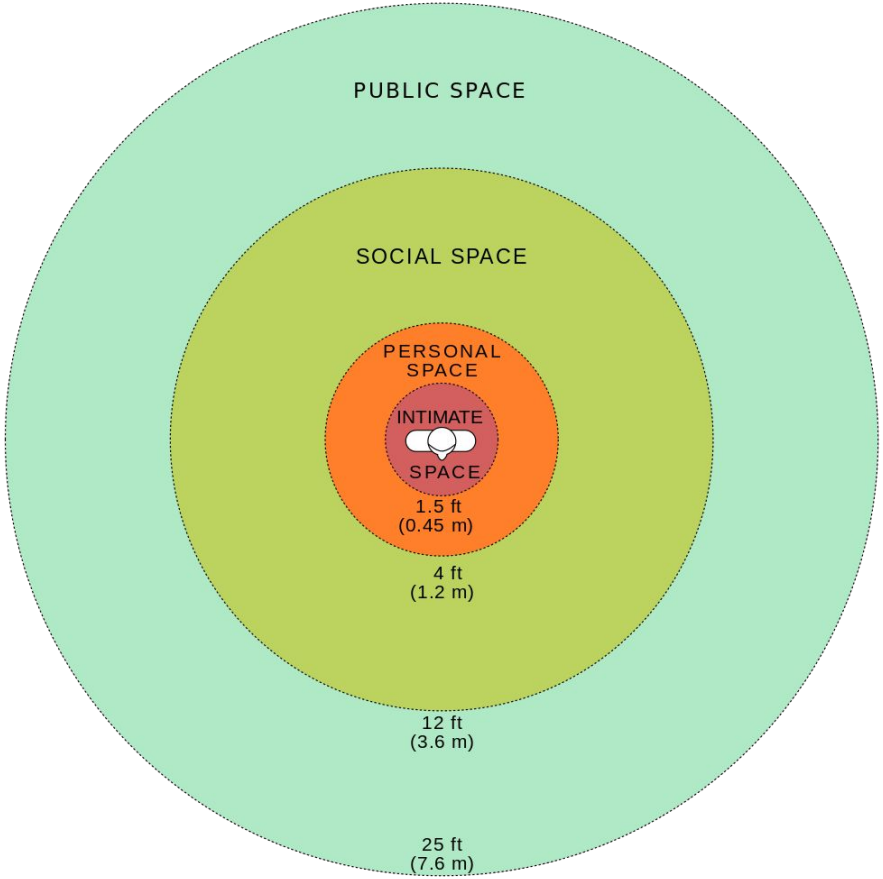
Examples



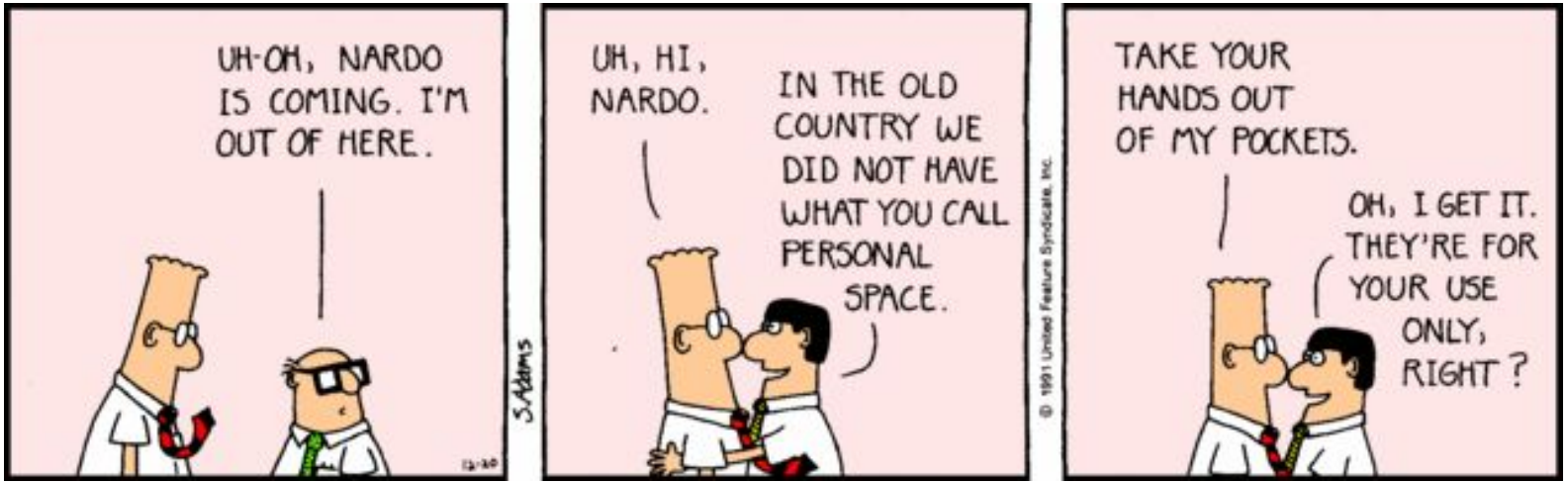
Examples



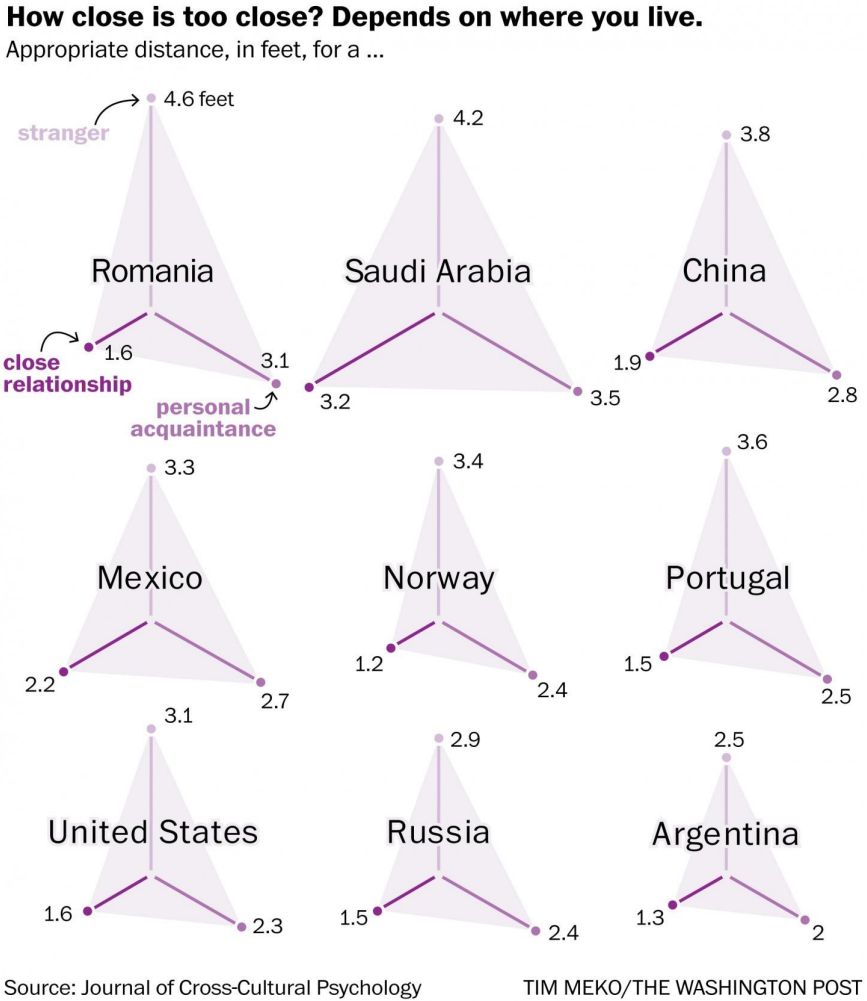
Proxemics


PUBLIC SPACE
SOCIAL SPACE
PERSONAL SPACE
INTIMATE SPACE
1.5 ft
(0.45 m)
4 ft
(1.2 m)
12 ft
(3.6 m)
25 ft
(7.6 m)

Proxemics


UH-OH, NARDO IS COMING. I'M OUT OF HERE.
UH, HI, NARDO.
IN THE OLD COUNTRY WE DID NOT HAVE WHAT YOU CALL PERSONAL SPACE.
TAKE YOUR HANDS OUT OF MY POCKETS.
OH, I GET IT. THEY'RE FOR YOUR USE ONLY, RIGHT?
S. Adams
© 1993 United Feature Syndicate, Inc.

Proxemics


How close is too close? Depends on where you live.
Appropriate distance, in feet, for a ...
stranger
4.6 feet
Romania
close relationship
1.6
3.1
personal acquaintance
4.2
Saudi Arabia
3.2
3.5
3.8
China
1.9
2.8
3.3
Mexico
2.2
2.7
3.4
Norway
1.2
2.4
3.6
Portugal
1.5
2.5
3.1
United States
1.6
2.3
2.9
Russia
1.5
2.4
2.5
Argentina
1.3
2
Source: Journal of Cross-Cultural Psychology
TIM MEKO/THE WASHINGTON POST

Body Language Tips/Examples

One sign is not enough

Comfort vs Discomfort, don’t get too specific

Arms and Legs Position

Eyes and looks

Feet Position

Genital Framing & Ventral Display

Manipulators / Pacifiers

Emblems

(Usually) Hand gestures whose meaning often depends on culture.

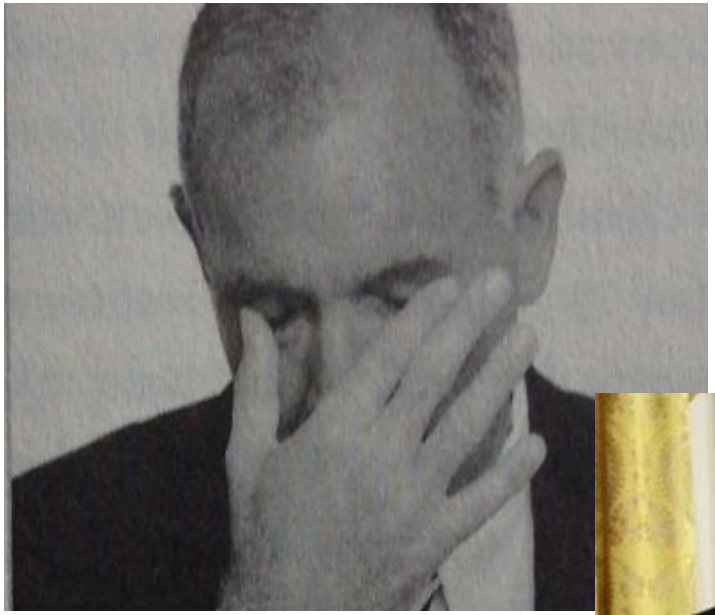
Emblems

ESL

Eye blocking

Shoulder shrugging

Lip locking



ESL

Eye blocking

Shoulder shrugging

Lip locking

ESL

Eye blocking

Shoulder shrugging

Lip locking

(or hands behind back)


DENVER abc


#MattyXz

Handshake

Mimicking

How to use non-verbal communication in SE

- Causing emotions
- Detecting deception / Understanding emotions
  - Contradictions
  - Hesitation
  - Changes in behavior
  - Body gestures
- Combine the skills with
  - Elicitation
  - Questioning techniques


copyright (c) 1999 Daniel J. Simons. All rights reserved.

Cognitive Blindness and Misdirection

Cognitive Blindness and Misdirection

Manipulation

Manipulating vs Influencing

Influencing - Influence someone to change their mind in a way that is good for them

Manipulating - Influence someone to change their mind in a way that is NOT good for them

Manipulation - Fear

- Fear then Relief technique

Manipulation - Fear

- Fear then Relief technique

“Hi this is the tech support. We detected a virus on your machine that could delete all your files. We need to install an antivirus. Can you please tell me your password so we can remove the virus ?”

Manipulation - Guilt

- Use guilt as a way to comply: Do someone a favor and then use it against them later

Manipulation - Guilt

- Use guilt as a way to comply: Do someone a favor and then use it against them later

“You owe me a favor after, I kept X secret for you”

Manipulation - Foot in the door

Ask the victim to do a very small request first. Once they comply, follow with the real larger request.

Manipulation - Foot in the door

Ask the victim to do a very small request first. Once they comply, follow with the real larger request.

“Could you tell me the time?”

Manipulation - Scarcity

Leverage on the fact that what you offer is rare / only available for a limited time.

Neurolinguistic Programming

“a model of interpersonal communication chiefly concerned with the relationship between successful patterns of behavior and the subjective experiences (esp. patterns of thought) underlying them”

or also

“NLP is the practice of understanding how people organise their thinking, feeling, language and behaviour to produce the results they do.”

Social Engineers can use it to convince people to act in specific ways and, in general, to manipulate minds similarly to hypnosis

DISCREDITED

“Psychological” Principles Recap

- Interact with target with a pretext (next chapter)
- Use previous knowledge regarding the target to ask questions that lead down the path you want
- Use Elicitation techniques to convince target to “follow your lead”
- Understand non-verbal communication of target and adapt
- Aling your non-verbal communication with your story

Countermeasures, Mitigations, Remediations

Weakest Link?

No matter how strong is your:

- Firewalls
- Intrusion Detection Systems
- Cryptography
- Anti-virus software

You are the weakest link in computer security!

People are more vulnerable than computers

"The weakest link in the security chain is the human element" - Kevin Mitnick

Personal Mitigation

Corporate Mitigation

Personal Mitigation Techniques

Common Targets

Junior Staff

Contractors

Admin Staff

Support Staff

Personal Mitigations 1/2

- Always ask for IDs
- Do not let guests roam free in the building
- Don’t plug USB keys you find around
- Before transmitting personal information over the internet, check the connection is secure and check the url is correct
- If unsure if an email message is legitimate, contact the person or company by another means to verify

Personal Mitigations 2/2

- Be paranoid and aware when interacting with anything that needs protected
    - The smallest information could compromise what you're protecting (Be aware of what you are saying)
- Shred documents
- Encrypt documents
- Educate

Corporate Mitigation Techniques

- Policies and Procedures
- Staff Awareness
- Technical Prevention and Detection Controls

Corporate Mitigation Techniques

- Identify what information or assets are most valuable (Check confidentiality)
- Write corporate security policies
- Keep software update and patched
- Never assume your company is too small to be a target

Policies and Procedures

Security procedures can prevent social engineering attacks, by providing examples of good behaviour to follow:

- Do not allow to divulge private information
- Prevents employees from being socially pressured or tricked
- Follow a prescribed, secure and considered procedures
- Not use work email addresses or passwords when registering for websites

Staff Awareness

Making users aware of the threats and risks that they face, they can make decisions that are more informed.

Training and Education (Certification)

- **3rd Party test - Ethical Hacker**
    - Have a third party come to your company and attempt to hack into your network
    - will attempt to glean information from employees using social engineering
    - Helps detect problems people have with security

Technical Prevention and Detection Controls

Users can often be easily compromised if their workstation software contains exploitable weaknesses

Mitigations

- Patch management.
- Workstation and device hardening are also highly important.
- Establishing a capability to identify and respond to security breaches as they occur.

Final Exercise

Create a Phishing Website & Email/Message

The final objective is to send me a message or email on which, clicking on a link, i'll be redirected to actual phishing website you'll have created on a fake github account.

The website should be able to email you at least the username that I insert.

To create the website:

1) create a new github account (use https://temp-mail.org/ or another fake email)
2) setup the github pages organization site (brief guide https://pages.github.com/)
3) Find the login page of the website you wanna emulate (i.e., Facebook.com) and copy it
4) modify it with a form to send yourself an email (to the fake email if possible)
5) load it as your own index.html

To create the phishing email (or you can use a social message) - send it to secoursepolimi@gmail,com or on my personal social media account.
- go to https://emkei.cz/ and fake the email with the link (hide the link behind an hyperlink)

Create a Phishing Website & Email/Message

To submit your work you need 2 steps:

1) Let me know once you've sent me the email / fake message, i'll click on it and insert a random username
2) Send me a final email named EXE4_GROUPx with inside:
   a) the username i used to answer you
   b) a screenshot of the index page
   c) a screenshot of the phishing email or message

REMEMBER TO DELETE THE INDEX AND THE PROFILE ONCE WE FINISH THE PROJECT

The End

Social Engineering