Information Governance CIS3005

Social Engineering 1

Recap & introduction

This week looking at “Social Engineering” -> feeds into:

- LO7 of the module: “*Demonstrate a complex understanding of the breadth and depth of the physical and environmental security issues for a given scenario and demonstrate a critical awareness of current problems and issues informed by research findings and professional practice.”*
- Assessment Parts 1 & 2 - SE is a risk for the organisation (Pt1) & you will need to identify some ‘controls’ to combat SE attacks (Pt 2)

"Only amateurs attack machines; professionals target people" (Bruce Schneier, Oct 2000)

- "The Science of Human Hacking" – subtitle of recommended book by Christopher Hadnagy
- According to the Verizon 2023 DBIR report, humans account for 74% of security incidents.
  - Their 2023 report is worth a read
- SE targets human weaknesses:
  - Trusting
  - Greed
  - Longing & loneliness
  - Time poverty – we're always rushed
  - Altruism & kindness
  - Ego
  - Curiosity
  - Fear
  - Over-confidence (hubris)

Defining what it is - cont

- Good examples:
  1) https://www.youtube.com/watch?v=lc7scxvKQOo
  2) https://www.youtube.com/watch?v=PWVN3Rq4gzw or
  3) https://www.youtube.com/watch?v=FvhkKwHjUVg (longer video, but well worth watching)
- In video 1) What aspects of human nature was the scammer targeting?
- FBI & Comp Security Institute found that 77% of data breaches were down to a "disgruntled employee"
- 32% of people in organisations unaware of the internal computer policies to protect data (e.g. the ISMS)
- "Many of these attacks could have been avoided if people were educated [about information security]" (Hadnagy)

https://www.social-engineer.org/framework/general-discussion/ – Hadnagy's SE Framework

1. Information Gathering:
   a) Physical methods
   b) Technical methods
2. Influencing others:
   a) Elicitation
   b) Pretexting
   c) Influence tactics (the power of persuasion aka 'Persuasion Principles')
3. Attack Vectors
4. SE Tools

Information Gathering - Physical methods:

"War is ninety percent information" – Napoleon Bonaparte

- Dumpster Diving (i.e. looking at items that have been thrown away)
- Watch "Erasing David" – really good film about someone who tried to disappear for a month and how he hired a firm of private investigators to track him down, look at the techniques the detectives use to track him down. In particular look at his face as he goes into their office towards the end of the film (1.10 onwards).
- Intrusion/role play (see pre-texting)
- Tailgating (aka 'piggybacking')
- Shoulder Surfing

Information Gathering - Technical methods:

- Telephone call (you can get an awful lot of info from a phone call:
  - How do they answer the phone?
  - Probably the name of the person answering the phone
- Online searches
  - Good old Google search
    - Photos of buildings
    - Corporate documents
    - Email address protocols
    - Job vacancies
    - Financial Reports
    - Boards of directors
    - Companies House
    - Etc
- Social networking sites
  - Info about employees
  - Potentially useful for phishing attack
  - Location enabled posts
- Software Tools:
  - Maltego
  - OSINT Framework

Elicitation

- "**elicitation is the term applied to subtle extraction of information during an apparently normal and innocent conversation**" (NSA archived at https://www.social-engineer.org/wiki/archives/Elicitation/Definition_of_Elicitation.htm)
- An introduction to Elicitation by subliminal hacking (watch in own time)
- It really about being a *really* good communicator with *very* high-level social skills
- Hadnagy:
  - To become a successful elicitor it's crucial to understand how to communicate with people.
  - You must learn to be adaptive, this means your communication must be made to fit the environment and situation.
  - It is crucial to build a bond or relationship with the potential "target".
  - Your communications should also match your pretext, otherwise you might seem out of place to the people your communicating with.
  - Really it all boils down to this: You must know how to ask intelligent questions that will force a response. Questions that can be answered with a simple ***"Yes"*** or ***"No"*** are not good questions at all.

Communication skills

- A target shouldn't realise they are actually a target (think about the video at the start of the lecture)
- Elicitation usually works because:
  - Most people want to be seen as polite, helpful, sympathetic (this is human nature)
  - Professionals want to be seen as well informed, competent & intelligent
  - People respond to praise – if you're praised you will talk more and divulge more
  - Most people are not compulsive liars
  - Most people respond well to kindness
- To me elicitation seems to be about exploiting the better parts of human nature
- How do you educate and train a workforce to resist this? V difficult as it is going against their very nature.

Communication skills

- Watch the experts:
  - https://www.youtube.com/watch?v=5WAv0cs6oV4 (The Real Hustle)
    - What made this scam work?
  - Chris Hadnagy (12.35 minutes long)

  - How to have better communication skills

Goals of elicitation

1. Be natural – you need to feel very comfortable in the situation you are in. If you're not this will be reflected in your non-verbal communication and you'll end up being less convincing
2. Educate yourself – understand your target & the organisational/business world they operate in. Don't try and pretend something you can't follow through on. E.g. don't pretend you can speak Russian (?) or are an expert in a particular programming language if you're not. Do research (your information gathering), practice & be prepared
3. Don't be greedy – don't let your need to obtain information be the sole driver (only in the conversation for yourself), give a little back (reciprocation – later in the module)

What do you do with this information that you have carefully gathered?

You might create a pretext

"Honesty is the key to a relationship. If you can fake that, you're in" – Richard Jeni

- Pretexting is defined as the practice of presenting oneself as someone else in order to obtain private information. It is more than just creating a lie, in some cases it can be creating a whole new identity and then using that identity to manipulate the receipt of information. (Hadnagy)
  - More than just "pretending" to be someone else – you have to "***be***" the person in that moment (see goals of elicitation)
- Also used in sales, public speaking even Doctors, lawyers & therapists use a form of pretexting.
- *Must* build trust.

Can everyone do this?

- I doubt it
- I think you need a particular personality, perhaps with theatrical talents/abilities
- Have a look at "White Collar" – about a conman working for the FBI (not intended to be taken too seriously, but some of the episodes show pretexting in action)

Pretexting & the law

- Some reported hacking cases involve pretexting:
  - https://www.bbc.co.uk/news/uk-england-leicestershire-43840075
  - Victim of fraud? Why the authorities WON'T investigate
  - Romance Fraud –
    - Victims lost £41 million to romance fraud in 2017
    - Online dating conmen 'using love letter templates'

Persuasion & SE

- Hadagny “is the process of getting someone else to do, react, think, to believe in the way *you* want them.”
- Have a look at Kevin Hogan’s YouTube channel (from a sales perspective but the same principles apply)

Principles of Persuasion (see Cialdini (2009))

- **Authority** – people tend to comply with requests from figures in authority
  - Crisis and stress tend to make people defer to authority more
- **Conformity** (social proof) - people mirror behaviour of others
  - Especially important in situations where they are unable to determine the appropriate mode of behaviour
- **Reciprocity** – giving something in return
  - 'Gifts' (however small) for example put the 'requester' in a good position
  - Think about going down a corridor with a series of doors – what happens?
- **Commitment** – sticking to a cause or position (e.g. the company ISMS?)
  - People will agree with requests that are consistent with their beliefs
- **Liking** – liking someone puts that person in a favourable position
  - People like others who are similar to them in terms of beliefs, attitudes, interests etc
- **Scarcity** – when something (product or service) has limited availability
  - Used a lot in advertising & sales

Authority & SE

- Power of authority can be seen in the famous Milgram Experiment
- Different types of authority:
  - **Legal authority** – government & law – used in pretexting through uniforms & other symbols of authority
  - **Organizational authority** – organizational hierarchy – used in SE by people purporting to have authority from someone high up in the organisation e.g. CEO, CFO (see Hofling Hospital Experiment)
  - **Social Authority** – where people are influenced by a group taking the same action e.g. implied or stated how a previous person or group acted – "Joe let me through yesterday". Relies on how often people do their job in a "mindless" way – leaves them very susceptible to perceived authority

Conformity (social proof)

- People will do things they see other people doing
  - Used a lot in marketing
    - Why? – people follow people they admire & also equate brand as being “excellent” if their fav celeb uses it
    - Celebrity endorsements – why do people buy something simply because a celeb promtes it? (Celebrities losing brand endorsements & potential loss of sponsorship)
  - Canned laughter – used because it works!
  - People are very susceptible to social proof – see https://www.youtube.com/watch?v=MEhSk71gUCQ & influencing behaviour candid camera
    - Elevator experiment
- Used in SE by stating that others have taken a particular action before
  - E.g. getting a security guard to let you into a building because “Mike” had done so the day before.

Reciprocity

- Reciprocity is based on a universal understanding that people give back to others who have given first
- SE example: https://www.actionfraud.police.uk/alert/fake-tv-licencing-refund-emails getting something in return for giving bank account details.
- Reciprocity, if used in the right circumstances, is very difficult to resist
  - "give-aways"
  - Promotions
  - Etc
  - Must have value to the recipient *with no stings attached*!
  - Tacky gifts or sales literature don't work
  - Information also highly valued.
- As a SE look out for opportunities to give out free information, especially good if you can make the recipient indebted to you.
  - Read Hadagny p.191 for a good example of how he used reciprocity in a SE situation
  - Also see: Williams, E. J., Beardmore, A., & Joinson, A. N. (2017). Individual differences in susceptibility to online influence: A theoretical review. *Computers in Human Behavior*, *72*, 412–421. https://doi.org/10.1016/j.chb.2017.03.002
  - Don't ignore importance of a simple question – usually feel an obligation to reply

Commitment & consistency

- People have a desire to look consistent through their words, beliefs, attitudes and deeds and this tendency is supported or fed from three sources:
  - Good personal consistency is highly valued by society.
  - Consistent conduct provides a beneficial approach to daily life.
  - By being consistent with earlier decisions we can reduce the need to process all the relevant information in future similar situations. Instead, we just need to recall the earlier decision and respond consistently.
- *"The key to using the principles of Commitment and Consistency to manipulate people is held within the initial commitment. That is–after making a commitment, taking a stand or position, people are more willing to agree to requests that are consistent with their prior commitment. Many compliance professionals will try to induce others to take an initial position that is consistent with a behavior they will later request."*
- Other examples:
  - Auctions – people increase bids above what they initially set themselves
  - Business competing with one another (Coke & Pepsi)
  - Appeals – sending out a book mark or address labels with an appeal can increase rate from 18% to 35%

Liking

- People respond to people they like – sounds obvious
  - A politician(!)
  - A sales person
- But this is actually more nuanced:
  - “People like people who like them” (Hadagny)
  - As a SE (or sales person) *you* have to **like** people for them to like you
  - V difficult to fake, but charm can work on a short-term basis
  - Think about “Candle/Body Shop/book parties” – usually buy to help a friend
- What makes a person, object, organisation “likeable”?
  - Visual – people like what is visually appealing – but determining what this is to each person is not easy
    - Think about success of beauty b/vloggers
  - Familiarity – people like what is familiar (Heinz Salad Cream – brand change)
  - Positive Reinforcement - compliments

Scarc

- If things a desirable
  - Think
  - Adver
- Often use in a decision
  - Puttin

Conclusions

- LOTS to consider here – huge area
  - Explore some of the links and videos in the slides
  - Look at some of the papers I'll put on the reading list & other resources on Bb
    - Please send me links if you've got any good resources yourself
  - Plus, do your own research
- SE has massive implications for a business, how on earth do they combat these very human traits?
- This will be the subject of my next lecture
  - You will need to address this particularly in risk assessment of the assignment