Title: Notes about Social-Engineering
Author: losingmoreyears
Created 2021-11-13 19:11:45 UTC
Permalink: /r/ratioatblessons/comments/qt7yjl/notes_about_socialengineering/
Url: https://www.reddit.com/r/ratioatblessons/comments/qt7yjl/notes_about_socialengineering/

Most is via [The Strategy Bridge](https://thestrategybridge.org/the-bridge/2018/7/18/social-engineering-as-a-threat-to-societies-the-cambridge-analytica-case) & reformatted for Reddit with additional commentary.

What is social engineering?
Social engineering is utilizing deception in order to get someone to admit something. The obvious techniques are used such as hacking, phishing, placing back doors on computers and servers. In person, psychological manipulation is used to gain information or coerce the target into an admission.

Principles of Influence
Social engineering relies heavily on the six principles of influence established in *Robert Cialdini's Influence: The Psychology of Persuasion.*

1. Reciprocity – People tend to return a favor, hence the pervasiveness of free samples in marketing.

2. Commitment and consistency – If people commit to an idea or goal (orally or in writing), they are more likely to honor that commitment because it's now congruent with their self-image. Even if the original incentive or motivation is removed after they have already committed, people will continue to honor the agreement.

3. Social proof– People will do things that they see others doing.

4. Authority – People will tend to obey authority figures, even if they're asked by those figures to perform objectionable acts.

5. Liking – People are easily persuaded by others that they like.

6. Scarcity – Perceived scarcity will generate demand. For example, by saying offers are available for a "limited time only," retailers encourage sales.

Techniques to Watch Out For

Elicitation is the subtle and indirect gathering of information. Remember that anything public is free domain. Be careful in chats.

Framing is forcing information into a certain context. You may share additional information in attempting to clarify and correct the person who appears to be drawing the wrong conclusion. Sometimes, you may not be aware it is happening at all. If you've ever felt misunderstood in a conversation, then take a short pause to think about the goal of the conversation.

Pretexting is the conjuring of stories and excuses for asking questions. Also called emotional positioning. Someone may pretend to be sad about something or pretend that they are in crisis. They will then ask you to share your experience.

Cold-calling is gaining information from a seemingly random interaction. Typically, the person is super friendly and you might instantly connect over an interest or topic. Often, that interest or topic is well-researched in advance.

Gaslighting describes the technique involving misdirection, persistent denial, and lying to confuse a target and disrupt their sense of reality. The term is derived from the 1944 movie *Gaslight* in which a husband plays around with the lighting in the house to frame his wife as delusional.

Experiencing Social Engineering

Defenses are many-to-many while offenses are one-to-many. In short, the attacker has the advantage. The target may feel like the whole world is conspiring against them when in fact it is typically a very small group. Much of it works based off the power of suggestion. Most people fear rumors and gossip, so they try to correct it. However, they do this with people who have no clue as to what is occurring; thus perpetuating the cycle.

More extensive campaigns involve years of data collection and are initiated when the target does a certain behavior.

How to Protect Yourself Against Social Engineering

1. Evaluate your cybersecurity protocol. Look at your password management, firewalls, DNS address, antiviral/malware applications, browser plug-ins (tracker blockers, script blockers, and more) and etc.

2. Evaluate *how* you use the internet. Are you sharing identifiable information such as your name, age, hometown, location, friends, family members and more? Social-engineering happens over time and the groups may have an extensive, convoluted network that is partitioned. These days it is most likely automated. They may use social media to scrape data.

3. Be cautious when meeting strangers. Most people want to be liked and connect with others. Sit down and decide for yourself how much you're willing to share when first meeting someone. If the conversation goes too perfectly, then it might be a red flag.

4. Disengage. Anything you say or do is more data. It's not feeding the trolls, it's a copy-pasta or screenshot or written account of the interaction. This post is getting saved. A few members are uploading all the posts to Github.