**In simple terms, what is the best way to trick someone into revealing information?**

Social engineering is a con. A confidence scheme, in that you need to get a potential victim to believe you are someone else who has the necessary privileges to access certain information. The vast majority of individuals have experience with social engineering attacks – the spam phone calls or text one gets usually from an authority of some sort claiming some impropriety on your part in an effort to get you to give them money. This works similarly for organizations, with attackers targeting employee email systems or even personal phones or computers with malicious communications. As for the most effective strategy, a simple answer for a not so simple question is that *it depends*. It depends on what your target is, what type of information you are getting, what organization your target belongs to, etc. The most essential characteristic of an effective attacker is confidence. The target must believe that you are authorized or deserving of access, whether that be to physical location or information.

**Would there be any ethical considerations to take into account when legally performing an act of social engineering?**

Consent is always an important consideration when considering the ethics of doing something to another party that is deceptive in any form. A victim, whether it be a legal victimization, is still participating in something that they have no prior awareness of or agreement to. In psychological research, we remedy this by including a thorough debriefing process in cases where deception is required (just as it would be in the case of social engineering attacks) and an opportunity to withdraw any data or information gained from that participant (American Psychological Association, Ethical Principles of Psychologists and Code of Conduct, 2017, sec. 8.01, 8.07-8.08). It seems to me that this should be an essential consideration in legal social engineering as well, as not only does it remedy the issue of informed consent, but also provides an avenue of education for the victim/organization.

**What would be a good standard procedure to follow when trying to get a target to reveal information? What related theories would be good to research?**

Mouton et al. (2016) outlines a good procedure for attacks, suggesting that the attacks begin long before contact with the target is made with planning and research. Once contact is made, one must endeavor to gain the trust of the target, after which that trust and the information gained can be used to manipulate the target into revealing information. Once this information is obtained, one must disengage from the target (hopefully leaving no evidence to tie them to the attack) (Mouton, et al., 2016). In this process, specifically the step of gaining the targets trust, it may be relevant to look at the literature related to the therapeutic alliance between a psychotherapist and a client, as trust is an essential element required for the client to reveal information of their own volition. Further topics such as self-esteem, motivation, and personality theory may lend more information insofar as knowledge concerning the social side of humanity allows for better manipulation of people.

Mouton, F., Leenen, L, Venter, H. S. (2016). Social engineering attack examples, templates, and scenarios. *Computers and Security, 56*, 186-209. <https://doi.org/10.1016/j.cose.2016.03.004>

**What existing techniques in the cybersecurity industry provide the greatest chances of success? What are some related tips.**

Off the top of my head, I am disinclined to say that there is one perfect social engineering relies not on weaknesses of technology, but weaknesses of users. As such, attacks must be tailored to the target – i.e., it is not one size fits all. The most essential component is research. Know as much as humanly possible about the target as this will increase your options for attack and manipulation, such that you can select one which is most effective. For example, regarding phishing attacks, which most people are familiar with in some way, they are most effective in situations where the victim is not technologically literate (alas, this usually means the older-adult population). So, if your target is not well versed in internet security, a phishing attack may be highly effective.

**What are your thoughts on the incorporation of psychological practices into cybersecurity? What are the upsides, or downsides of such a methodology?**

People often regard cybersecurity as a technological game –about securing hardware, networks, access, etc. However, it is important to consider the fact that the people using this technology are *human*, which means they are subject to the inherent weaknesses of humanity. A system can be as secure as possible, but it is impossible to divorce the human element from it, thus the user will always be an avenue of exploitation (and may even be the easiest option in high security applications). This begins to articulate some of the upsides of social engineering considerations in cybersecurity – we need to find a way to shore up the threat of human weakness to security. It provides opportunities for training, reduces the likelihood of successful attacks on people, and helps cybersecurity professionals in the recognition of attacks.

I suspect that similar downsides to the whole of cyber security apply to social engineering as well – that sometimes it seems as though it is a zero-sum game, in that there will always be a new weakness to exploit or a new manipulation tactic and thus the whole process doesn’t actually matter. Social engineering may be even more so, as it is logistically impossible to make certain that every employee or member of an organization knows everything to look out for or protect against. Networks can be secured, buildings can be locked, but we cannot depend on people not to make mistakes.

**Do you have any recommendations?**

I think that, in social engineering, it might be easy to get lost in the goal and forget that we are dealing with humans – ethical considerations should be considered paramount. It might be tempting to fall into the use of malicious manipulation strategies to gain information. These strategies, while potentially effective, can have extremely deleterious effects on victims. As such, I believe it is best to ensure that the mistakes employees make during a social engineering attack conducted by the organization should not be punished – it should be an opportunity for education and training. If employees are always worried about making a mistake, productivity and general wellbeing may be negatively impacted.