Social Engineering: 6 Ways to Manipulate Humans

Jesus Christ was undoubtedly one of the best social engineers ever. He used many of the techniques that are covered in the article. The definition of social engineering for this article shall be "The use of thought or mood altering human borne stimuli to produce a desired outcome from a target human or group of humans". Simply put, social engineering is getting others to do stuff to get the result wanted. The content of this article is to discuss how to create manipulations to which people will respond favorably. It will not be discussing delivery mechanisms such as email, voice calls, instant messaging, in-person contact, mail, etc. Social engineering delivery mechanisms will be covered in a later article. There are far more many ways to manipulate people than can be covered in this article so we will limit this discussion to the following:

1. Fear
2. Greed
3. Lust
4. Love
5. Empathy
6. Anger

It is not unusual to watch the news and see something that suggests the world is in a battle for survival and all humans are under threat of personal devastation with possibilities of being maimed or murdered. Fear is a very powerful tool that is used to boost ratings, create entertaining movies and attractions, and even help humans survive various forms of harm; however, when fear is stoked and brought to a point where it is the dominant emotion controlling thought it can be leveraged to force a person to make specific decisions that might not otherwise be considered reasonable. There are many types of social engineering that are connected to fear such as fear of losing employment, blackmail related fear, fear of social or political changes, fear of losing out, and fear of rejection to name a few. If a manager, supervisor, boss, executive, or other person with a "fancy" job title asks an employee to do something that is not aligned with policies that employee may feel like job loss is a real possibility of denying the request and the fear they feel may permit them to ignore the policy. In the same vein, an outside attacker can mimic this by impersonating a position of authority and making improper request while threatening the employee with job loss. Blackmail is a very common fear technique that is not always the "we have your child" as depicted in the movies. Sometimes it is, but more often than not an attacker will threaten to lock or delete an account, prohibit access to funds, litigate, provide a negative review and/or negative PR, sell or release corporate data, or publicly release conditions that can be exploited. Fear of social or political changes is a very effective social engineering tactic against specific target groups and is usually pretty closely aligned with fraud. Attackers will often describe the

incredible personal harm that will befall all persons within a group if a policy or political change is permitted ("removing all police everywhere will leave rivers of blood in the streets when protesters become murders and decide to riot in your neighborhood and loot your home") followed by a request for donations towards efforts to fight the offending policy. Coincidentally, the fraudsters associated with this type of fear based social engineering will play both sides of the field and may send out another campaign that champions the cause ("if police are not removed from their colonization stronghold policies they will enter your home, they will abuse you, you will be the next one murdered in bed"). Fear of losing out is probably one of the oldest motivations for people to be convinced to take a particular action. Whether it be the fear of losing the chance to enter heaven, a great investment opportunity, or the last item for sale on the tv shopping program people get anxious as the risk of losing out becomes greater. As that clock winds down to zero the anxiety grows and the ability to think rationally diminishes. "It is better to have loved and lost than to never have loved at all" is a fairly famous quote but even when you have loved and lost that occasionally means you lost because you were rejected and that is never fun. Rejection is hurtful and unwelcome but all too common so people try to avoid it whenever possible. This condition can be used in a variety of ways from fear of being rejected by a potential employer, potential lover, family member, or group to name a few. There are recruiters whom are not really recruiters and job posting that are not really job postings. A common tactic for these entities to to make contact with a person (usually a job seeker) and gain specific information about the individual or previous employer(s). This information could include technologies used, configuration details, policies, network architectures, groups withing an organization, group sizes ("how big was the IR team you worked on"), the candidate's last 4 of their tax ID or social security number, the date and month of their birthday, and can often end with the attacker stating something to the effect of "without this information we can not submit you, we are required to fill out each box or the organization can not process your profile. "Fear is a very powerful manipulation tool that affects most people while greed is something that has a smaller target audience.

If you deposit this check in your bank account I will let you keep $134,967 dollars but you need to promise to wire the rest of the money back to me. This sentence is not that far from what people have seen in emails for quite some time. Although there are a number of social engineering tactics that are used in those scams greed absolutely has a role. Unlike fear, greed does not resonate with every user. I believe it resonates with greater that 85% of users whom believe their greed will have no, or near no, consequences but that is just an arbitrary guess. Greed does not have a great number of ways it can be used to manipulate people and it relies on trust. The person being manipulated must believe the greedy action he or she is taking will be rewarded without consequence. This can be manifested through the use of bribery, designed opportunistic acts, and designed skill superiority. Bribery is simple in theory but can become inordinately complex in practice. The essence of bribery is the attacker offers a benefit to a target and the target reciprocates with a desired action. Often times the attacker offers money but this could be replaced by a house, stocks, cars, bonds, vacations, season tickets, recognition, fame, employment, and so forth. Often times the bribery target's action will be the granting of access or information. Designed opportunistic acts are when an attacker designs a scenario where the target's greed will force the target to take a specific action. A simple example is placing/dropping money on the ground within view of a security guard. When the guard observes the money the guard will

approach retrieve it permitting an attacker to slip by unnoticed. Designed skill opportunity is a tactic in which the attacker places a friendly wager ("I'll bet you a beer") that the target can't best them at something ("you can't do that again on this device without messing up"). Greed is a tactic that has its uses but is limited much like lust.

Have you ever noticed that people become less intelligent when they are communicating with people they perceive to be highly attractive?Lust is a powerful tool that has been used to manipulate people since biblical times when a man claimed his wife was his sister so she could marry a king in order to preserve his own life. Manipulation using lust is fairly straightforward, find someone whom the target will consider very attractive then have that person interact with the target. When performed in-person the person whom is the object of the lust must be the actual attractive person. In the digital world only photos of the object of lust need be used as made popular with the term "catphishinng". In general, the goal of lust-based social engineering to gain access or to gain information. Don't be fooled just because someone is attractive, that person is as dangerous as everyone else because that person is just like everyone else. Lust can be used to transition into a far more powerful social engineering technique called love.

Love is one of the most powerful and destructive forces that has ever been bestowed upon mankind. It has cause many a good soul to start a feud or war, caused passionate murders, treason, and all manners of ill conceived plans, plots, and insidiousness. When it comes to love, there is hardly any force that will torture a person greater and which can cause a person to reject all sense of instilled morality, intelligence, and logic. Love can be used by attackers in only one way using two different avenues. The target is manipulated by the person whom is loved or someone impersonating the one whom is loved to achieve some end result. In the first scenario the attacker spends a great deal of time building a connection, instilling trust, and formulating what seems to be an authentic relationship. Slowly over time the attacker uses emotional influence to persuade the target to act in a certain manner. This social engineering tactic is a long-term strategy. In the second type of love social engineering the attacker impersonates the target's loved one and manipulates the target into performing some action. This scenario does not require the same timeline as the legitimate loved one has already built the emotional infrastructure required to conduct the attack; however, depending on the desired action this type of attack can still take considerable time to achieve success.

If you see someone struggling it is natural to want to assist because you are empathetic to their needs (or you don't want to look like a jerk). The desire to do good and to help others has a social rule attached, a "golden rule", that many have adopted as a type of life-style choice. There are many people who are empathetic due to religious convictions, a personal code of morality, and shared experience empathy exists as well. Religion has been a cultural mainstay since recorded history was begun and the majority of religions have teaching that refer to, or deal with, empathy or sympathy towards others. One way an attacker could use empathy to convince an attacker to perform an action is by way of religious activity. For instance, an attacker might know a target is part of a church prayer group and

thus submit a prayer request that directly relates to the target. The target being a good pious religious follower may perform some action or reach out to the attacker with the goal of providing help. For those in the community whom are not religious, most still have a moral code by which they consciously of unconsciously live. In such circumstances an attacker intentionally enter a situation that is disadvantageous (or appears to be disadvantageous) in order to create a condition by which the victim feels a need to render assistance. A common pattern in this form of social engineering attack is when an attacker feigns ignorance in skill or ability to gain information or when an attacker 'forgets' their access badge or is carrying to many items to use an access badge. Shared experience empathy is a little more difficult for attackers to perform because it does require a fair amount of intimate knowledge of the victim. In this scenario the attacker communicates with the victim, usually for 'advice', explaining the 'issue' which mirrors an issue the victim has had in the past. As the discussion progresses the 'issue' also progresses to the point where the victim is now revealing information about current projects, topics, or other information. The end result could also be the victim providing access to resources, whether they be personnel resources or access. Empathy is a troublesome social engineering tactic but it is nowhere as troublesome as anger.

Anger is the most basic emotion and has arguably been the one that has resulted in the most devastation throughout human history. If an attacker can anger someone the attacker can completely control that person. Anger really has only one attack vector, present someone with an argument that is so vile and repugnant that they feel obligated to respond and once they respond obliterate that response with factual arguments that undermine the victims very perception of the world. This may sound a bit "doom sayer" because it is specifically worded that way but is also an honest representation of an attackers goals. The actual attacks using anger-based social engineering may be quite subtle, nuanced, and cumulative. Cumulative in the sense the anger is built up over a period and is not a "flash in the pan". A common scenario for this type of attack is when an attacker starts a dialogue with a victim at which point they are in agreement about a topic which the victim is passionate. As time passes the attacker comes back to the victim with little bits of questions and small facts that undermine the victims efforts and beliefs. Overtime the victim becomes resentful and eventually performs some action. This is made more effective when the attacker is impersonating what is intended to the the target of the victim. For instance, an attacker may pretend to be a representative of a political party to which the human target is passionately associated. The attacker builds a friendly rapport with the target after-which the attacker starts to provide information to the target which is maligned with the target's personal beliefs and efforts. As all the information the attacker is providing to the victim is fact based and the attacker is still building a friendly rapport the target starts the fall. Once the target is at a breaking point the attacker totally rebukes the target and provides a detailed list of why the target is unworthy of being associated with the political party. At this point the target has a great deal of anger and resentment that will be (if the attack was successful) focused on the political party or possibly politics itself.

Jesus Christ was undoubtedly one of the best social engineers ever using fear, greed, love, empathy and even anger. Our definition of social engineering has been "The use of thought or mood altering human

borne stimuli to produce a desired outcome from a target human or group of humans". Simply put, social engineering is getting others to do stuff to get the result wanted. The content of this article has discussed how to create manipulations to which people will respond favorably. It has not be discussed delivery mechanisms such as email, voice calls, instant messaging, in-person contact, mail, etc. Social engineering delivery mechanisms will be covered in a later article. There are far more many ways to manipulate people than were covered in this article so it has been limited to fear, greed, lust, love, empathy, and anger.

Thank you for reading

-Andrew Kosakowski

www.Anthko.com