

Look Mom, I'm a Thespian: How to Use Acting Skills as a Social Engineer

Chris Hadnagy

Social Engineering is a complex beast. It is not simply lying or telling someone a deceitful story to get them to give over their passwords. Social Engineering (SE) is defined, well at least by me, as any act that influences a person to take an action that may or may not be against their best interest. With that definition in mind there are many different principles that influence SE and the skills needed both physically and psychologically.

The concept behind this column is to provide the tools, techniques and direction to the readers that would like to either incorporate more SE into their current work or to become a full-time social engineer. I would like to take this month's article to talk about at least one of the psychological principles involved in SE that should be considered foundational and required. It makes a huge difference in your ability to be successful.

Discuss in Forums {mos_smf_discuss:Hadnagy}

Determination on the Follow Through

There is a great video called "Uta Hagen's Acting Class"; Uta Hagen is a world-class acting coach that has taught many of the big names in acting today. She compiled a couple of videos complete with exercises about how to get a person "in" the scene. I think this is a primary principle for social engineers as well.

When you are approaching a target, the pretext must not be an act, not something you are doing for this 3-4 minutes, but it is your life. It is who you are for that time. The pretext must be all encompassing.

How? How can a social engineer do that? I refer back to Uta's video. In that video she makes mention of this principle: "Words before actions and the action needs to back up the words." She then explains that, if the scene involves making you laugh and actor one tickles actor two and they laugh, then there is no reason for the words. This means that the dialog will be ignored.

As a social engineer we can utilize this psychological principle to our advantage. Our words that are spoken are very important as they will set the mood, tone, and emotional stage, but, if our actions are not congruent to those words, then we cause a disjoin and in effect turn the target off. Let me explain this through a simplistic example in a story format.

Recently I was tasked as part of some security work to see if I could gain access to a building through a secured door. I had a few options. 1) I could clone an RFID card of one of the employees and see if that worked. 2) I could try to tailgate through the door. 3) I could pose as a delivery person.

Now let me tell you some of the problems that existed here. First the employees were not just issued an RFID card, they are also given a pin number to go with the card. Once scanned they have 10 seconds to enter a unique code that if wrong locks them out. Secondly, the company stations a person at the door to check badges and make sure no tailgaters are let in. With these two factors I would have to act quickly and decisively to get past the door.

What I did is grab a box full of "supplies" and held in my hand a badge that looked very similar to the employees badges. As a stream of employees were coming back from lunch, I approached one and "bumped" into him. After apologizing I began to describe how busy I was in this project for the boss. We started a light conversation as we both walked towards the goal, the door. I let him enter first where he entered his code and RFID card then held the door for me. As we walked through knowing the guard would be looking for people like me, I waved my hand with the fake badge in it and quickly grabbed at the teetering box. The shock on my face was enough to make him feel empathy for me, and then I thanked "Jim" for holding the door for me and said, "See ya tomorrow at lunch."

The words were enough to make the security guard believe I belonged. I then without asking just walked in the direction that I felt my character would walk. Fortunately for me, I was not stopped and had access to the building now. My actions backed up my words and did not cause a disjoin, and I was granted access.

It is important that when we are trying to influence a person, we do not give their brains a reason to leave auto-pilot. Dr. Ellen Langer, a gifted and noted psychologist, was on my podcast and talked about how people do their jobs and live their lives on auto-pilot. In essence, they do their daily jobs in such a way that as long as there is no significant effort they can go along without being bothered. Understanding that means if we don't do anything to remove the target from their auto-pilot, we may be able to skate by unnoticed.

Reverse Psychology

In the same token, we may be able to reverse this principle and work it to our advantage. What I mean is similar to what Uta stated about our words coming before actions & actions support words. So what if we used our actions without words to build a scenario in the targets' mind all without having to talk?

Let's go back to our situation above, and see if there would have been another way to do that by reversing this principle. If I wanted to try and not have to use words, but I know that the security guard is expecting some words to back up my story, I could have simply acted as if I belong there. Everything is so natural that it exudes confidence as well as gives him the ability to know that I belong.

By acting the part, flashing the badge and walking with confidence, I build a nonverbal story that states, "I am an employee, and I not only deserve to be here, but you don't have to ask, just let me in."

Psychology vs. Social Engineering

This is just one of the many psychological principles of social engineering. It can benefit a social engineering professional to be aware of these principles, since not only do we attack but we must also defend. Knowing these principles can help us identify risks and educate our staff to learn to pick up on social engineering attempts. As we know from general security awareness programs, simply knowing is half the battle.

This doesn't mean I am recommending that we all become psychologists, but trying to understand the principles that motivate certain actions can greatly increase our ability to defend.

So what can you do? In addition to the resources we mentioned above, there are a number of great books you can read on certain aspects and principles of social engineering. I compiled these books with the help of the community at http://www.social-engineer.org/framework/Social_Engineering_Books. In addition, we will be teaching these principles at

the Social Engineering For Pentesters Courses we have scheduled. You can also take a course at a local college or remote college to cover some of these principles. Or for SE's sake, get out there and find a community theater and jump right in there.

Thanks for sending in some questions and comments on the new column. Keep it up and I look forward to seeing you out RSA and Seattle if you are signed up.

Until next month…

If you have comments or questions – please feel free to reach out to me at logan@social-engineer.org

Chris Hadnagy, aka loganWHD, has been involved with computers and technology for over 14 years. Presently his focus is on the "human" aspect of technology such as social engineering and physical security. Chris has spent time in providing training in many topics around the globe and also has had many articles published in local, national and international magazines and journals. He is also the lead developer of Social-Engineer.Org as well as the author of the best-selling book, Social Engineering: The Art of Human Hacking.

He has launched a line of professional social engineering training and pen testing services at Social-Engineer.Com. His goal is to help companies remain secure by educating them on the methods the "bad guys" use. Analyzing, studying, dissecting then performing the very same attacks used by malicious hackers on some of the most recent attacks (i.e. Sony, HB Gary, LockHeed Martin, etc), Chris is able to help companies stay educated and secure. Chris can be found online at <http://www.social-engineer.org/>, <http://www.social-engineer.com/> and twitter as @humanhacker.