**Chapter 5: Mind Tricks: Psychological principles used in social engineering.**

In Hollywood movies and television shows con men and law enforcement are portrayed with almost mystical talents. They have the ability to get away with anything;

they seem to be able to just look into the eyes of a person and tell if they are lying or telling the truth. It is not uncommon to see situations like this: the cop looks into the eyes of his suspect and can automatically tell whether he is lying or telling the truth, or with just the power of suggestion the con man’s targets are handing over their life’s savings. Movies might have you believing that manipulation tactics and getting people to do anything you want is plausible or even easy. Are these scenarios really fiction? Is it possible to gain such abilities that are saved for fantasy in the movies? This chapter could be a book unto itself, but I will condense this information

down to principles that will truly change the way you interact with people. Some of the topics in this chapter are based on research done by the brightest minds in their respective fi elds. Th e techniques discussed in these topics were tested and put through the paces in social engineering environments. For example, the topic of microexpressions is based on the research of the world-renowned psychologist and researcher, Dr. Paul Ekman, who used his genius to develop techniques into reading facial expressions that can literally change the way law enforcement, governments,

doctors, and everyday people interact with others. Some of the principles of Richard Brandler and John Grinder, the originators of neurolinguistic programming, changed people’s understanding about thought patterns and the power of words. Th ese topics are subjects for much debate, and this chapter attempts to demystify this subject and explain how you can use them in social engineering.

Some of the best interrogators on the planet developed training and frameworks

to help law enforcement learn how to eff ectively interrogate suspects. Th ese

principles have such deep psychological roots that learning the methods used can

literally unlock the doors to the minds of your targets. Using cues that people give in their speech, gestures, eyes, and faces can make you appear to be a mind reader. Th is chapter examines these skills and explains them in detail so they can be utilized by a professional social engineer.

*Rapport* is often a word used by sales trainers and salespeople, but it is a very

important aspect of gaining trust and displaying confi dence. Knowing how to

instantly develop rapport with people is a skill that truly enhances the skill set of a

social engineer, and this chapter shows you how. This chapter fi nishes with my own personal research on how you can use these skills to hack the human mind. A *buff er overfl ow* is a program usually written by a hacker to execute code, of malicious intent normally, through the normal use of a host program. When executed the program does what the hacker wants. What if it were possible to run “commands” on the human mind that would cause the target to do what you ask, give over information you seek, and, in essence, prove that the human mind is able to be manipulated? This powerful information, of course, can be used for very malicious intentions. My goal in releasing this information to the public in this way is to pull back the

curtain from what the “bad guys” are doing by exposing their methods, thinking,

and principles, then analyzing each one and showing what you can learn from it.

Exposing these techniques makes identifying, defending, and mitigating against

these attacks easier for everyone.

This chapter is truly a mind-altering collection of data and principles. Following,

studying, and researching the methods will not just enhance any security endeavorsbut these principles can also alter the way you communicate and interact with others.

By no means, though, is this chapter a complete collection that covers all aspects

of each of these skills. I provide links and tips to where you can fi nd more information and programs to help you enhance these skills. Th is chapter sets a foundation as well as acts like a guide, pointing you in a direction so you can learn to enhance each skill over time.

Learning social engineering skills is not a quick process, so don’t be impatient.

Th e methods of learning some of these skills can take years to perfect and a lot of

practice to even become profi cient. Of course, you may possess a skill for a certain

aspect but if you do not, don’t become impatient with trying to learn it. Keep on

trying harder and practicing and you will get it.

Before you get into the meat of this chapter, the following section sets the stage

for why and how these principles will work. You must understand the modes of

thinking that exist. After you understand more clearly how people take in and

process information you can begin to understand the emotional, psychological, and

physical representations of that process.

**Modes of Thinking**

To alter someone’s way of thinking you must understand the *way* people think and

in what *modes* they think. Th is seems a logical fi rst step to even attempting this

aspect of social engineering.

You might think you need to be a psychologist or a neurologist to understand the

many aspects of how a person can think. Although that can help, it is not necessary.

With a little research and some practical application you can delve into the inner

workings of the human mind.

In August of 2001 the FBI put out a law enforcement bulletin (www.socialengineer.

org/wiki/archives/ModesOfThinking/MOT\_FBI\_3of5.htm) that made

a few very profound statements on the modes in which people think:

*Simply confirming your nonverbal behavior to the client, using*

*language from the client’s preferred representational system and*

*matching speech volume, tone, and area of speech often overcomes*

*client reluctance to communicate.*

Th is simple statement has a lot of depth in it. Basically it is saying that if you can

fi rst fi gure out the target’s dominant mode of thinking and then confi rm it in subtle

ways, you can unlock the doors of the target’s mind and help him actually feel at

ease when telling you even intimate details. Logically you may ask then, “How do I

fi gure out a target’s dominant mode of thinking?”

Even asking people what their mode of thinking is will not off er a clear answer,

because many people do not know what mode of thinking they often reside in. Due

to that, as a social engineer you must have some tools to help you determine this

mode and then quickly switch gears to match that mode. A clear and easy path

exists to this answer but you need to know the basics fi rst.

The Senses

For centuries philosophers have argued the value of perception. Some go so far as

to say that reality is not “real” but just what our senses build into our perceptions.

Personally, I do not subscribe to that idea, but I believe that the world is brought

to our brain by our senses. People interpret those senses for their perception of

reality. In the traditional classifi cation we have fi ve senses: sight, hearing, touch,

smell, and taste.

People tend to favor one of these senses and that is the one that is dominant. It

is also the way people tend to remember things. As one exercise to determine your

dominant sense, close your eyes and picture yourself waking up this morning—what

is the very fi rst thing you remember?

Was the *feeling* of the warm sun on your face? Or maybe you remember the *sound*

of the voice of your spouse or children calling you? Do you remember clearly the

*smell* of coff ee downstairs? Or quite possibly the bad *taste* in your mouth, reminding

you that you need to brush your teeth?

Of course, this science is not exact and realizing what your dominant sense is

may take a few tries to fi gure out. I once talked to a couple about this concept and

it was interesting to watch their expressions. Th e wife fi rst remembered waking

up and seeing the clock and then worrying that she was running late, whereas the

husband fi rst remembered rolling over and not feeling his wife next to him. After

some more questions it became evident that the husband was a *kinesthetic*, or his

dominant sense was his feeling, whereas his wife was very visual.

Of course, walking up to your target and saying, “Close your eyes and tell me

the fi rst thing you remember this morning,” doesn’t seem reasonable. Unless, of

course, your pretext is the family shrink, you might meet with some opposition

on this route.

How can you determine without going through an embarrassing interrogation

about their morning rituals what a target’s dominant sense is?

The Three Main Modes of Thinking

Although we have fi ve senses, the modes of thinking are associated with only three

of them:

» Sight, or a visual thinker

» Hearing, or an auditory thinker

» Feeling, or a kinesthetic thinker

Each sense has a range within which it works, or a *sub-modality*. Is something too

loud or too soft? Too bright or too dark? Too hot or too cold? Examples of these are

as follows: staring at the sun is too bright, jet engines are too loud, and –30 degrees

Fahrenheit is too cold. Ivan Pavlov ran an experiment where he rang a bell every

time he fed a dog. In the end the dog would hear the sound of the bell, then salivate.

What most people don’t know is that he was more interested in the physical and

emotional aspects of sub-modalities. Th e interesting point is that the louder the bell

rang the more the dog salivated. Th e range change of the sub-modality produced

a direct physical change. Pavlov’s research and all of his lectures are discussed in

much detail at www.ivanpavlov.com.

Even though people are very diff erent from dogs, Pavlov’s research is very important

in understanding how a person thinks. Many of us can think in all three modes,

but we dominate in one—one “rings” the loudest. Even within our dominant mode,

we might have varying degrees of depth for that dominant sense.

Following I will discuss some of the details of each of these modes in more

depth.

*Auditory*

*Auditory thinkers* remember the sounds of an event. Th ey remember that the alarm

was too loud or the woman whispered too low. Th ey recall the sweetness of the child’s

voice or the scary bark of the dog. Auditory people learn better from what they hear

and can retain far more from being told things than being shown things.

Because an auditory thinker remembers the way something sounded, or because

the sounds themselves help recall memories, he may use phrases such as:

» “Loud and clear…”

» “Something tells me…”

» “Th at sounds okay to me.”

And the range of this dominant sense can be within these sub-modalities:

» Volume (loud or soft)

» Tone (base or treble)

» Pitch (high or low)

» Tempo (fast or slow)

» Distance (near or far)

It is imperative to choose your words carefully with auditory thinkers. Th e words

they hear will make or break the deal. I have seen whole encounters go from great

to a disaster with one wrong word spoken to an auditory thinker.

*Kinesthetic*

*Kinesthetic thinkers* are concerned with feelings. Th ey remember how an event made

them feel—the warmth of the room, the beautiful breeze on their skin, how the

movie made them jump out of their seat with fear. Often kinesthetic thinkers feel

things with their hands to get the sense of the objects. Merely telling them something

is soft isn’t as real as letting them touch it. But helping recall a soft item they

touched before can recall emotions and feelings that are very real to a kinesthetic

thinker.

Th e term “kinesthetic” relates to tactile, visceral, and sense-of-self sensations of

the body—basically, where a person’s body is in space and the self-awareness of how

something made him feel. A kinesthetic thinker uses phrases such as:

» “I can grasp that idea.”

» “How does that grab you?”

» “I’ll get in touch with you.”

» “I just wanted to touch base.”

» “How does this feel?”

And the range for this type can have the following sub-modalities:

» Intensity (strong or weak)

» Area (large or small)

» Texture (rough or smooth)

» Temperature (hot or cold)

» Weight (heavy or light)

Helping a kinesthetic thinker recall a feeling or emotion tied to something can

make those emotions reappear as real as the fi rst time they occurred. Kinesthetic

thinkers are probably the most diffi cult for non-kinesthetic thinkers to deal with

because they do not react to sights and sounds and social engineers have to get in

touch with their feelings to communicate with this type of thinker.

Understanding these basic principles can go a long way toward being able to

quickly discern the type of person you are talking to. Again, without asking the

target to picture his morning rituals how can you discern the dominant sense? Even

more so, why is this so important?

*Discerning the Dominant Sense*

Th e key to determining someone’s dominant sense is to try to introduce yourself,

start a small conversation, and pay close attention to what is being said. As you

walk up to the target and lean in to say good morning, maybe she barely looks at

you. She might be rude, or she just may not be a visual. Visuals need to look at the

person speaking to communicate properly, so this behavior would seem to lend

to the fact she is not visual. Now ask a simple question such as, “Don’t you just love

the feel of a beautiful day like today?” and notice her response, particularly whether

she seems to light up or not.

Maybe you wear a large, shiny silver ring. As you talk you gesture; maybe you

see that the ring catches her eye. Does she reach out, interested, and need to hold

the ring or get close to observe it? Kinesthetics are very touchy-feely when it comes

to these things. I know a woman who is a strong kinesthetic and when she sees

something she thinks is soft or high quality she *must* touch it. She will say, “Wow,

that sweater looks so soft!” From that statement one might assume she is a visual,

but what happens next is what solidifi es it. She then walks up to the person and

touches the sweater and feels it. Th is shows her dominant sense is kinesthetic. Th e

same woman must touch everything in the grocery store when she shops, whether

she needs it or not. By touching the objects, she makes a connection and that connection

makes it real to her. Often she cannot remember things very well that she

did not come into physical contact with.

Asking questions that contain some of the key dominant words, observing a

target’s reactions, and *listening* can reveal what dominant sense he or she uses.

Listening for key words such as *see, look, bright, dark* can lead you to treat a target

like a visual. As mentioned earlier this is not an exact science. Th ere isn’t a general

rule that states if a person says, “I can see what you are saying…” then he is always

a visual. Each clue should lead you down the path toward verifying your hunch

with more questions or statements. One word of caution: talking to someone in

a diff erent mode than they think in can be irritating to some. Using questions to

determine a person’s mode of thinking can be off -putting. Use questions sparingly

and rely more on observation.

*Why Understanding the Mode Is Important*

I once worked with a guy, Tony, who could sell a cup of water to a drowning man.

Tony was a big believer in seeking out and then using a person’s dominant sense in

sales. He had a few methods that he used that you may learn from. When he fi rst

engaged the target he had a very shiny silver-and-gold pen he would hold in his

hand. He would gesture a lot and notice whether the person followed the pen with

her eyes; if she did slightly Tony would continually make the gestures bigger to see

whether her eyes followed. If that didn’t seem to work in the fi rst few seconds he

would click the pen open and closed. It wasn’t a loud noise, but loud enough to disrupt

a thought and draw someone’s attention if she were an auditory. If he thought

that was working he would click it with every important thought, causing the target

to have a psychological reaction to the sound and what was being said. If that didn’t

seem to work he would reach out over the table and tap her wrist or forearm, or if he

was close enough touch her shoulder. He didn’t touch excessively, but enough to see

whether she would shy away or seemed overly happy or disturbed by the touch.

With these subtle methods he could quickly discern what the person’s dominant

sense most likely was. Th is whole act would take under 60 seconds. After he found

the information he was looking for, he would then start to move his conversation to

that dominant sense, even taking on the traits of that sense in the words he spoke

and way he acted and reacted to the conversation. One thing about Tony is that he

outsold any person I have ever met. People would often say about him, “It is like he

knew exactly what I needed.”

Tony would talk to the person and treat the person the way they wanted to be

talked to. If the person was a visual thinker, Tony would use phrases like “Can you

see what I am saying?” or “How does this look to you?” He would use illustrations

that involved “seeing” things or visualizing scenarios. He would put people in their

comfort zone.

People feel at ease when they are in their comfort zone. Th e more you can do as

a social engineer to put people in their comfort zone, the better chance you have

at success. People gravitate towards those with whom they are comfortable; it is

human nature. For example, if someone makes you feel “warm and fuzzy,” or seems

to understand what you are saying, or seems to see where you are coming from, you

easily open up to, trust, and let that person in your circle.

I want to reiterate this point: fi nding and using someone’s dominant sense is

not an exact science. A social engineer should use it as a tool in the arsenal and

not rely on it as something magical or scientifi c. Certain psychological aspects of

human nature are based on proven science and can be relied upon. As a matter

of fact, some of these aspects are so impressive that they can make you seem like a

mind reader. Some of them have been a topic of serious debate and some accepted

by psychologists, law enforcement, and social engineers for years. Th e next section

of this chapter discusses these, starting with microexpressions.

**Microexpressions**

You are probably familiar with the idea of reading facial expressions. When someone

is happy, sad, angry, or whatever, when someone feels it you can look at his or

her face and see that emotion. What if someone tries to fake that expression, like a fake smile? We have all done it, walking through the market and bumping into someone we just don’t like that much—we put on a “smile” and say, “Hey John, nice

to see you. Say hi to Sally.”

We may act very pleasant and cordial, but inside we are feeling nothing but

irritation. Th e expressions that we show for longer periods of time on our face are

called *macroexpressions* and are generally easier for people to see the emotion that

is being conveyed. Similar to microexpressions, macroexpressions are controlled

by our emotions, but are not involuntary and often can be faked.

A certain few pioneers into the study of human behavior have spent decades

researching something, coined *microexpressions*, to understand how humans relay

emotions.

Microexpressions are expressions that are not easily controllable and occur in

reaction to emotions. An emotion triggers certain muscular reactions in a face

and those reactions cause certain expressions to appear. Many times these expressions

last for as short as one-twenty-fi fth of a second. Because they are involuntary

muscular movements due to an emotional response, they are nearly impossible to

control.

Th is defi nition is not a new understanding either; Charles Darwin wrote a book

in 1872 called, *Th e Expression of the Emotions in Man and Animals.* In this book

Darwin noted the universal nature of facial expressions and how muscles were used

in facial expressions.

In the early 1960s two researchers, Haggard and Isaacs, fi rst discovered what today

is called microexpressions. In 1966, Haggard and Isaacs outlined how they discovered

these “micromomentary” expressions in their publication titled, *Micromomentary*

*Facial Expressions as Indicators of Ego Mechanisms in Psychotherapy*.

Also in the 1960s, William Condon, a pioneer who studied hours of tapes frame by

frame, discovered that humans had “micro-movements.” He also heavily researched

neurolinguistic programming (more on that later) and body language.

Probably one of the most infl uential researchers in the fi eld of microexpressions

is Dr. Paul Ekman. Dr. Ekman pioneered microexpressions into the science it is today.

Dr. Ekman has been studying microexpressions for more than 40 years, receiving

the Research Scientist Award as well as being labeled one of *Time Magazine’s* most

infl uential people on earth in 2009.

Dr. Ekman researched facial expressions with psychologist Silvan Tomkins. His

research revealed that, contrary to popular belief, emotions are not culturally determined,

but are universal across cultures and biological.

Working with Dr. Maureen O’Sullivan he developed a project called the Wizards

Project*.* He began to pioneer the use of microexpressions in lie detection. He used a base of 15,000 people from all walks of life and all cultures and found out of that

large number that only 50 had the ability to spot a deception without training.

**Chapter 6: Influence: The power of persuasion**

The epigraph sums up this entire chapter. You might be wondering why I didn’t

include this within Chapter 5’s discussion of psychological principles of social

engineering. Psychology is a science and a set of rules exists in it that, if followed,

will yield a result. Social engineering psychology is scientific and calculated.

Infl uence and persuasion are much like art that is backed up by science. Persuasion

and infl uence involve emotions and beliefs. As discussed in some of the earlier chapters,

you have to know how and what people are thinking.

Infl uence and the art of persuasion is the process of getting someone else to *want*

to do, react, think, or believe in the way *you* want them to.

If you need to, reread the preceding sentence. It is probably one of the most powerful

sentences in this whole book. It means that using the principles discussed herein,

you will be able to move someone to think, act, and maybe even believe the way *you*

*want him to because he wants to.* Social engineers use the art of persuasion every day

and, unfortunately, malicious scammers and social engineers use it, too.

Some people have devoted their life to researching, studying, and perfecting

the art of infl uence. Th ose such as Dr. Ellen Langer, Robert Cialdini, and Kevin

Hogan have contributed a very large repository of knowledge in this fi eld. Mix this

knowledge with the research and teachings of NLP (neurolinguistic programming)

masters such as Bandler, Grinder, and more recently Jamie Smart, and what you

have is a recipe to become a true artist.

True infl uence is elegant and smooth and most of the time undetectable to those

being infl uenced. When you learn the methods you will start to notice them in commercials,

on billboards, and when used by salespeople. You will start to get irritated

at the shoddy attempts of marketing people and if you are like me, you will begin

to rant and rave at terrible commercials and billboards while driving (which does

not make my wife very happy).

Before getting into how social engineers will use in infl uence and persuasion,

the chapter begins with a short tour of some of the key elements of persuasion

and infl uence that I have compiled and used. Th is chapter will discuss things like

reciprocation, manipulation, and the power of setting goals, just to name a few of

these key elements.

Infl uence and persuasion can be broken down into fi ve important aspects, as

discussed in the following sections.

**The Five Fundamentals of Influence**

**and Persuasion**

Th e fi ve fundamentals of persuasion are crucial in obtaining any type of successful

infl uence upon a target:

» Setting clear goals

» Building rapport

» Being observant of your surroundings

» Being fl exible

» Getting in touch with yourself

Th e whole goal of social engineering is to infl uence the target to take an action that

may or may not be in their best interest. Yet they will not only take the action, but *want*

to take the action and maybe even thank you for it at the end. Th is type of infl uence is

powerful and can make a social engineer who possesses these skills legendary.

World-renowned NLP trainer Jamie Smart once said, “Th e map is not the territory.”

I love that quote because it blends perfectly with these fi ve fundamentals. None of them

are the whole sum on their own, but individually they are like points on a map that

show you the whole territory of what you want to accomplish. Th e following section

delves deep into the fi rst fundamental: why setting clear goals is very important.

Have a Clear Goal in Mind

Not only should you have a clear goal in mind, you should even go so far as to write

it down. Ask yourself, “What do I want out of this engagement or interaction?”

As I discussed in Chapter 5, especially in relation to NLP, a human’s internal

systems are aff ected by his thoughts and goals. If you focus on something, you

may be more likely to become it or get it. Th is doesn’t mean that if you focus on the

thought of getting one million dollars, you will get it. In fact, it is unlikely. However,

if you had a goal of making one million dollars and focused on the steps needed to

make that money, your goals, education, and actions would increase the likelihood

of you achieving that goal. Th e same is true with persuasion. What is your goal? Is

it to change someone’s beliefs? To get him to take an action? Suppose a dear friend

is doing something terribly unhealthy and you want to try and persuade her to

stop. What is the goal? Maybe the end goal is to persuade her to stop, but maybe

little goals exist along the way. Outlining all of these goals can make the path to

infl uencing that person clearer.

After setting the goal, you must ask yourself, “How will I know when I have

gotten it?” I once listened to a training program off ered by Jamie Smart, one of

the world leaders on NLP, and he asked each person in the classroom these two

questions:

» What do you want?

» How will you know when you have it?

At this point, I paused the CD for the fi rst question and answered for myself out

loud what I wanted from this course. Th en I pressed Play again and when he asked

that second question, “How will you know you have gotten it?” I paused the CD again

and was lost. It was clear to me that I didn’t have a roadmap. I knew what I wanted

out of that course, but I didn’t know how to gauge when I had gotten it.

Knowing what you want out of your engagements is an important aspect of

infl uence and persuasion tactics. When you approach a target knowing what your

goals are and what the indicators are that you are getting what you want, then you

can clearly identify the path you need to take. Clearly defi ned goals can make or

break the success of the infl uence tactics used by a social engineer as well as make

the next step much easier to master.

Rapport, Rapport, Rapport

Chapter 5 has a whole section on rapport building. Read it, study it, and perfect

your rapport-building skills.

Developing rapport means that you get the attention of the person you are targeting

and his unconscious mind, and you build trust within that unconscious portion.

Mastering the skill of building rapport can change the way you deal with people,

and when it comes to social engineering, it can change your whole methodology.

To build rapport, start where the person you want to infl uence is mentally—try

to understand their frame of mind. Are they suspicious? Are they upset, sad, or

worried? Whatever emotional state you perceive them to be in, start from there. Do

not focus on your goals as much as focusing on understanding the person. Th is is

a very vital point. Th is means a social engineer must understand his target enough

that they can imagine where they are consciously. What are the target’s thoughts

and state of mind?

For example, imagine you want to infl uence your dear friend to want to quit

smoking or doing drugs or something else. Notice you don’t want to convince her

to quit, but convince her to *want* to quit. Your goal cannot be about *you*, right? It

must focus on the target. You can’t start your conversation with what her addiction

is doing to *you* and how much *you* hate the smell, and so on. Th e argument has to

be what is in it for *her*. You cannot start the conversation with a verbal attack about

what the person has done to you with their habit, but you need to understand where

that person’s frame of mind is, accept it, and come into alignment with it.

Social engineering is much the same: you can’t start where *you* are mentally.

Th is is going to be struggle for many people. Do you know why she smokes? Do

you understand the psychological, physical, or mental reasons why? Until you can

really get into her shoes, you cannot build a strong rapport and your eff orts at

infl uence will fail.

In addition, you cannot always base the idea of building rapport on logic. I once

was in the hospital with a dear friend who was dying from throat cancer. He had

smoked for more than 40 years and one day he found out he had cancer. It spread

fast, bringing him to the hospital to live out his last days. His children would come

to visit and every now and then they would leave the room. I thought they were

overcome with emotion. One time after they excused themselves I went out to

comfort them and they were outside the hospital smoking! I was dumbfounded. I

don’t smoke and have no desire to, and although I can understand how strong an

addiction can be, I couldn’t understand how after seeing the pain their father was

in, how they could raise a cigarette to their lips.

Logic would not win in this case. Telling my friend’s children why smoking is bad

and how it will kill them would do no good—this information was useless because it

was combative and only made me feel good in saying it, but did not align with their

present frame of mind. Until you understand the person you cannot successfully

build a good enough rapport to influence him or her.

Be in Tune with Yourself and Your Surroundings

Being aware of yourself and your surroundings, or *sensory acuity*, is the ability to

notice the signs in the person you are targeting and yourself that will tell you that

you are moving in the right direction or not.

Many of the principles discussed in the previous chapter apply to persuasion.

Reading body language and facial signs can tell you much about your infl uence on

the person.

To really master the dual art of infl uence and persuasion, you have to become a

master watcher and master listener. Chris Westbury, a cognitive neuropsychologist

at the University of Alberta, Canada, estimates that human brains process

information at 20 million billion calculations per second. Th ose calculations are

represented by facial expressions, microexpressions, gestures, posture, voice tones,

eye blinks, breathing rate, speech patterns, nonverbal utterances, and many more

types of distinguishing patterns. Mastering infl uence means to be aware of those

subtle things in yourself and others.

I found, for myself, the ability to be observant proved to be easier for me after

receiving some training from Dr. Ekman in microexpressions. I found afterward that

not only did I become much more aware of what was going on with those around me,

but also myself. When I felt a certain expression on my face, I was able to analyze

it and see how it might be portrayed to others. Th is recognition of myself and my

surroundings was one of the most enlightening experiences of my life.

NLP experts promote minimizing your internal dialog when trying to infl uence

others. If you approach the target thinking about the next stage of the attack, the

end goal, or comebacks for potential conversation stoppers, that internal dialog can

cause you to miss a lot of what is going on around you. Being observant takes a lot

of work but the payoff is well worth it.

Don’t Act Insane—Be Flexible

What do I mean by not acting insane and being fl exible? One defi nition of insanity

that’s been fl oating around for years is “doing the same thing over and over and expecting

diff erent results.” Being willing and able to fl ex is one of the keys to persuasion.

You can think of this fl exibility in terms of physical things. If you were tasked to

persuade or bend something, would you rather it be a branch from a willow tree or

a steel rod? Most people would say the willow branch because it is fl exible, easier

to bend, and makes the task accomplishable. Trying to persuade others while being

unyielding and infl exible doesn’t work, and neither does persuasion if you are not

fl exible.

Many times, an audit will not go as planned. A good social engineer will be

able to roll with the punches and adjust their goals and methods as needed. Th is

does not go against the idea of planning ahead; instead, it bespeaks the point of not

being so rigid that when things do not go as planned you can move and adapt so

the goal is not lost.

Th e way a person would view an insane person is the way a target would view

the infl exible social engineer. Th e social engineer would look unreasonable and you

would most likely never reach endgame.

Get in Touch with Yourself

By getting in touch with yourself, I am not suggesting some Zen meditation avenue,

just that you understand your emotions. Emotions control practically everything you

do, as well as everything your target does. Knowing your emotions and being in touch

with yourself can help you lay the groundwork for being an eff ective social engineer.

Going back to the earlier example of you and your smoking friend—approaching

your friend if you have a deep-seated hatred for those who smoke aff ects your

approach. It can make you act, express, say, or do something that will close the door

to persuasion. You may never compromise on certain things, and being aware of

those things and your emotions about them can help you to develop a clear path

toward infl uencing a target.

Th ese fi ve fundamentals are key to understanding infl uence and persuasion. Being

able to create an environment where a target wants to do what you are requesting is

the goal of persuasion, and these fi ve fundamentals will help you create that environment.

Th e next section examines how social engineers use these fundamentals.

**Influence Tactics**

As mentioned, social engineers must practice the skill of persuasion until it becomes

part of their everyday habits. Th is doesn’t mean that they must infl uence everyone

in everything they do, but being able to turn this skill on and off at will is a powerful

trait of a good social engineer.

Infl uence and persuasion have many aspects you can use and many that fi t easily

into an audit. Other aspects might not fi t too easily, but hold a very powerful position

in the world of infl uence. Th e following sections cover eight diff erent techniques of

infl uence that are used often by media, politicians, government, con men, scammers,

and of course, social engineers.

Each section provides an analysis of each technique to see how it is used in other

areas of infl uence besides social engineering, as well as takes a closer look at how

it can apply to a social engineer.

Reciprocation

*Reciprocity* is the inherent expectation that when others treat you well you respond

in kind. A simple example is when you are walking into a building—if someone holds

a door open for you, he expects you to say thank you and then make sure that next

door stays open for him as he comes in.

Th e rule of reciprocity is important because often the returned favor is done

unconsciously. Knowing this means that you now have a step up on how you can

use it as a social engineer.

*Give Something Away*

Th e thing you give away can’t be some simple piece of junk. Th e thing given must

have value—to the recipient. Giving away a beautiful hardcover novel written in a

language the recipient does not read or collect is useless.

Th e item can be a service, a physical item, some valuable information, assistance,

or anything else that the receiver will deem as a value (even something as simple

as holding the door or picking up something dropped). Some sales organizations

promote this method but then fall short by off ering something that has no value.

Imagine you are at a trade show and at each table is a giveaway. If you walk up to a

table and notice a pile of cheap-looking pens you might just walk by. Th e next table

has an interesting puzzle-like game. You are intrigued so you pick it up; after you

spend a few minutes playing with it a salesperson approaches and says, “You want

a hint?” After showing you a small hint he asks whether you have a minute so he

can show you a service you might really love.

How can you say no? You get an intriguing game and a free hint, and now all he

wants is a minute of your time? It’s a perfect setup.

*Create Indebted Feelings*

The more value the gift has to the recipient and the more unexpected it is, the

greater the sense of indebtedness.

Not allowing the gift to be used in an obvious manipulation tactic is important.

Don’t say or act like, “I gave you this great gift now you owe me.” Even thinking it

can take away any feelings of indebtedness. Th e “gift” should be totally free and of

great value to the recipient.

Th e Humane Society of the United States, for instance, gives away personalized

mailing labels as a free gift. No strings are attached and many people use them for

holiday cards or personal letters. Th ey are attractive and good quality. You sign up

for them, and many months later you will get a call asking for a donation to support

your local Humane Society. Th e recipient’s sense of obligation is usually too great

to not contribute even a little.

By way of another example, *Fortune Magazine* off ers college professors free issues

of its magazine to try out in their classes with no strings attached at all.

*Ask for What You Want*

On one occasion as I was entering a building, I saw a man who looked very much

to be the “boss” get out of his car parked in the spot marked “For CFO Only,” and

he was on his cell phone. He was not a happy guy, and I overheard him telling

someone that he was upset because he had to go inside and let some people go. I

assumed from his tone that he was on with his wife or girlfriend and he didn’t like

the job he was about to do.

I walked past him and went to the front desk and as I walked up I saw that the

girl behind the desk was playing Minesweeper. As I approached the counter she gave

me the standard, “How can I help you?” She had a look on her face that said she was

bored and not in the mood. I said, “Look, I am here for a meeting, but your boss is

about to walk in and he is in a bad mood…” I then trailed off and just stood there

with a folder in my hand. A few seconds later the boss stormed in the front door and

I said loudly, “Th ank you so much for your assistance.”

She looked over and said to me, “Excuse me, sir,” then said to her boss, “Good

morning, Mr. Smith, I have your messages,” and then handed him a small pile of

paper as he walked by.

When he disappeared to his offi ce she thanked me profusely. I just saved her and

she knew it. Th e information I gave her was invaluable, and my next words would

be imperative: “I need your help. I wanted to see the HR manager just for a brief

meeting. Can you get me into her offi ce real quick?”

She walked me back to the manager’s offi ce and introduced me as “her friend” that

stopped in. Within minutes my plan was launched, and all thanks to reciprocity.

As a social engineer, look for little opportunities to give out information that

will make you valuable to the recipient and more importantly, make the recipient

indebted to you.

Be aware of your surroundings and what little things you can do to make your

targets indebted to you. Remember it doesn’t have to be something amazing, just

something that they value. A good point to keep in mind is to not “stalk” the target.

Standing and staring at him or her waiting for an opportunity to do or say something

can be off -putting. Th ese principles should be natural.

Naturalness means you start doing these principles in everyday life. Hold doors

for people, be very polite, and look for opportunities to do good things for others.

Th ese actions will become second nature and you will have fewer struggles doing

them in an audit.

Reciprocity is a powerful infl uence tactic, and the next two principles discussed

are closely tied into it.

Concession

A *concession*, or the act of conceding, is defi ned as “an acknowledgment or admission,”

or “the act of yielding.” Concessions are used often within the social engineering

context as a play on the reciprocation instinct of humans. Humans seem to have

a built-in function that makes them want to “do unto others as they do unto” you. A social engineer can use the “something for something” idea or the “I’ll scratch

your back if you scratch mine” principle.

Scarcity

People often fi nd objects and opportunities more attractive if they are rare, scarce,

or hard to obtain. Th is is why you will see newspapers and radio ads fi lled with “Last Day,” “Limited Time Only,” “Only 3-Day Sale,” and “Going Out of Business

Forever” messages that entice people to come from all over to get a share of the

soon-to-be-never-seen-again product.

Th e use of scarcity in the sales context is best known with the catch phrase *“Act*

*now! Supplies are limited!”* Other techniques are the common *“Th e fi rst X callers*

*get a free widget,”* or having an intentional short supply of a popular product. In

recent times, this practice was most popularly alleged with the Nintendo Wii. Jason

Dobson, a writer for Gamasutra, said, “But I think [Nintendo] intentionally dried

up supply because they made their numbers for the year. Th e new year starts April

1, and I think we’re going to see supply fl owing”.

Where I live, a car dealership ran an ad on a Th ursday stating it had to get rid

of X number of cars due to new stock arriving. Th e prices were so low and some of

the cars—wait for it—were no longer being produced, and that weekend was the last

weekend ever that you could come in for a piece of auto-selling history.

Th e sales went through the roof that weekend, so the sale was over right? Nope,

that ad ran every Th ursday for more than three months. I often wondered how people

just didn’t catch on to it, but the dealership sold a lot of cars using this method.

Social events can often appear to be more exclusive if scarcity is introduced. Th e

perceived social benefi t of attending these events often goes up in these circumstances.

In advertising, this point is driven home with ads for music events that

point out how the last concert was quickly sold out.

Many popular restaurants have been known to close off sections of the restaurant

to appear busier than they really are. Th e perception that they are extremely

popular can often trigger a heightened desire to eat at that establishment.

**Chapter 9: Prevention and Mitigation**

The preceding chapters show you all the methods and ways that social engineers

trick and scam targets into divulging valuable information. They also

describe many of the psychological principles that social engineers use to influence

and manipulate people.

Sometimes after I give a speech or security training, people will look very paranoid

and scared and say something like, “It just seems there is no hope to even

attempt security. How do I do it?”

Th at is a good question. I promote having a good disaster-recovery plan and

incident response plan because nowadays it seems that it is not a matter of “if” you

will get hacked, but “when.” You can take precautions to give you at least a fi ghting

chance at security.

Social engineering mitigation is not as easy as ensuring hardware security. With

traditional defensive security you can throw money into intrusion detection systems,

fi rewalls, antivirus programs, and other solutions to maintain perimeter security.

With social engineering no software systems exist that you can attach to your

employees or yourself to remain secure.

In this chapter I present the top six steps I tell my clients they can take to prevent

and mitigate social engineering attempts:

» Learning to identify social engineering attacks

» Creating a personal security awareness program

» Creating awareness of the value of the information that is being sought

by social engineers

» Keeping software updated

» Developing scripts

» Learning from social engineering audits

Th ese six points all boil down to creating a security awareness culture. Security

awareness is not about a 40-, 60-, or 90-minute program once every year. It is about

creating a culture or a set of standards that each person is committed to utilizing in

his or her entire life. It is not just about work or websites deemed to be “important,”

but it is the way one approaches being secure as a whole.

Th is chapter covers the aforementioned six points and how creating a security

awareness culture can be the best defense against a malicious social engineer.

**Learning to Identify Social**

**Engineering Attacks**

Th e fi rst stage in social engineering prevention and mitigation is to learn about

the attacks. You don’t have to dive so deep into these attacks that you know how to

recreate malicious PDFs or create the perfect con. But understanding what happens

when you click a malicious PDF and what signs to look for to determine whether

someone is trying to trick you can help protect you. You need to understand the

threats and how they apply to you.

Here’s an illustration: You value your home and the things in it, but especially

the people in your home. You do not wait to have your fi rst fi re to fi gure out how to

plan, prevent, and mitigate its danger. Instead you install smoke detectors and plan

out an escape route in case of a fi re. In addition, you might train your children with

the phrase to, “Stop, drop, and roll” if they are on fi re. You teach them how to feel

the door for heat and to stay low to avoid smoke inhalation. All of these methods

are ways to prevent or prepare for a fi re before you have a real fi re and have to deal

with the devastation it brings.

Th e same principle applies to protecting yourself and your company from social

engineering attacks. Do not wait for the attack to occur to learn about how devastating

they can be. Don’t think I’m self-serving, but I promote social engineering

audits to regularly test your employees’ ability to withstand these attacks, and following

up with training.

Teach yourself and your employees how to “stop, drop, and roll,” so to speak, when

it comes to these types of attacks. What are the latest news stories on how social

engineers are attacking companies? Knowing them can be a fi rst line of defense,

the same as knowing what a fi re can do to your home. Learn the diff erent methods

that modern social engineers and identity thieves use.

Another good step is reading this book. It is full of all the methods and principles

that social engineers use to manipulate their targets. Th is book is more than just

a compilation of stories and wonderful hacks; it off ers an analysis of the thinking

and tactics used by the malicious social engineer.

Also check out the videos on the www.social-engineer.org site, in the Resources

area, which demonstrate exploits in action. Th e average user does not need to watch

them with the intent of understanding how to perform these attacks himself, but

to understand how an SE performs the attack.

Basically, the more you know about how these attacks occur, the easier you can

identify them in the “wild.” Being aware of the body language, expressions, and

phrases used in an SE attempt will make your ears perk up when you hear or see

someone utilizing these methods.

You don’t need to spend tons of time learning about SE methods. However,

spending a few minutes now and then reading the news and reading stories on

www.social-engineer.org or other sites can help you see the methods being used

now against companies.

After you have a good basis of knowledge and an audit under your belt, the next

step, creating a security-minded culture, will seem simple to develop.

**Creating a Personal Security**

**Awareness Culture**

In July of 2010 I was part of a small team of security professionals that held one of

the fi rst organized and professional-level social engineering contests at Defcon 18.

Some of the best and brightest minds from around the globe come to Las Vegas,

Nevada, once a year to speak, teach, and learn.

My team and I decided it would be a great opportunity to hold a contest that

would showcase whether corporate America is vulnerable to this attack vector

(responding to a “contest”). We organized the contest by having interested people

sign up to take part in two stages of social engineering : information gathering and

active attacks.

To keep the contest legal and moral we did not want any person victimized, and

no Social Security numbers, credit cards, and no personal identifying information

would be gathered. Our goal was not to get any of these people fi red. In addition our

goal was not to embarrass any particular company, so we decided also no passwords

or other personal security–related information from the companies. Instead we

an internal cafeteria, to who handles its trash disposal, to what browser it uses, and

to what software it uses to open PDFs. Finally, we chose target companies from all

sectors of business in corporate America: gas companies, tech companies, manufacturers,

retail, and everything in between.

Each contestant was assigned one target company in secret, on which he had two

weeks to do passive information gathering. Th at meant contestants were not allowed

to contact the company, send it emails, or in any way try to social engineer information

out of it. Instead they had to use the web, Maltego, and other tools to gather as much

information as possible and enter all they found into a professional-looking report.

From the information gathered we wanted contestants to develop a couple of

plausible attack vectors that they thought would work in the real world. Th en contestants

had to come to Defcon in Las Vegas, sit in a soundproof booth, and make a

25-minute phone call to their target to implement their attack vector and see what

information they could obtain.

I could spend the next 20–30 pages telling you what happened at that contest and

what the outcome was, but one thing we found was this: Every contestant obtained

enough information out of the targets that the company would have failed a security

audit. Regardless of the experience level of the contestant and the pretext, the

contestants were successful in accomplishing their goals. For a full report about

the CTF and what occurred, visit www.social-engineer.org/resources/sectf/

Social-Engineer\_CTF\_Report.pdf.

Now on to what applies here—security awareness. Corporations that care about

security have programs where they train their employees how to be aware of potential

security risks via phone, Internet, or in person. What we found was that security

awareness in those companies was at failure stage. Why? How could it be that these

Fortune 500 companies that spend millions or more on security, training, education,

and services designed to protect their employees could be failing at security

awareness?

Th at is my point in the title to this section—security awareness is not personal

to employees. Often in my professional practice when I talk with employees about

their feelings about an attack they respond with something like, “It is not my data;

what do I care?” Th is attitude shows that the security awareness that these companies

were trying to instill never hit home; it was not important, eff ective, and most

importantly, not personal.

In reviewing much of the material and methods available for so-called security

awareness, what I have found is that it is boring, silly, and not geared to make the

participant interact or think. Short DVD presentations that cover a ton of things in

a shotgun approach that blasts the participant with a lot of tiny little facts are not

designed to sink in too deep.

What I challenge you to do as a company or even as an individual is to create a

program that engages, interacts, and dives deep into security awareness. Instead of

just telling your employees why having long and complex passwords is a good idea,

show them how quickly one can crack an easy password. When I am asked to help

perform security awareness training for a client, sometimes I ask an employee to

come up to my computer and type in a password that she feels is secure. I do this

before I release any information about passwords. Th en as I start my presentation

on that section I start a cracker against that password. Usually within a minute or

two the password is cracked and I reveal to the room the password that was secretly

typed into my computer. Th e immediate and drastic eff ect it has on each person has

an extreme impact. But after numerous demonstrations like that employees will

comment on how they now understand how serious having a good password is.

When I discuss the topic of malicious attachments in email, I do not have to show

employees how to craft a malicious PDF but I do show them what it looks like from

both the victim’s and the attacker’s computers when a malicious PDF is opened.

Th is helps them understand that a simple crash can lead to devastation.

Of course, this teaching method produces a lot of fear, and although that is not

the goal, it is not a terrible side product, because employees will remember it better.

But the goal is to make them think not just about what they do not only at work and

with their offi ce computers, but also their own bank accounts, home computers,

and how they treat security on a personal level.

I want each person who hears a security presentation or reads this book to review

how he interacts with the Internet as a whole and make serious changes to reusing

passwords, storing passwords or personal information in non-secure locations,

and to where they connect to the Internet. I cannot tell you how many times I have

seen a person sitting in the center of Starbucks on her free Wi-Fi checking a bank

account or making an online purchase. As much as I want to go up and yell at that

person and tell her how quickly her whole life can be turned upside down if the

wrong person is sitting on that same network with her, I don’t.

I want people who read this to also think of how they give out information over

the phone. Con men and scam artists use many avenues to steal from the elderly,

those having hard economic times, and everyone else. Th e phone still remains a very

powerful way to do this. Being aware of the vendors’, banks’, or suppliers’ policies

on what they will and will not ask for over the phone can help you avoid many of

the pitfalls. For example, many banks list in their policies that they will never call

and ask from a Social Security number or bank account number. Knowing this can

safeguard you for falling for a scam that can empty your life savings.

Calling security awareness a “program” indicates that it is something ongoing.

A program means you schedule time to continually educate yourself. After you

obtain all this useful information, then you can use it to develop a program that

will help you to stay secure.

**Being Aware of the Value of the**

**Information You Are Being Asked For**

Referring to the Defcon 18 social engineering contest again, in it we learned another

valuable lesson—when the information is perceived as having no or little value, then

little eff ort is placed on protecting it.

Th is is heavy-duty statement, but was proven true with how many targets willingly

handed over information on their cafeterias, waste removal, and so much more.

You must realize the value of the data that you have and be aware of a tactic a social

engineer might use to reduce the value of this information in your eyes.

Before giving out information to someone, determine whether the person who

is calling or interacting with you deserves it. Humans have this built-in desire to

want to help and to be helpful to those whom we perceive need it. It is a major

way a social engineer manipulates a target into handing over valuable information.

Analyzing the person with whom you are interacting and determining whether

she deserves the information she is asking for can save you the embarrassment and

damage of falling victim.

For example, in the social engineering contest at Defcon one contestant had a

pretext that he was a customer of a major antivirus company. He called in with a

serious problem—his computer couldn’t get online and he felt it was due to something

the antivirus was doing and wanted the technical support representation to

do one simple thing—browse to a website.

Malicious SEs often use this attack vector. By driving a victim to a website embedded

with malicious code or malicious fi les they can gain access to a target’s computer

and network. In the case of the contest, the website was not malicious at all, but it

was to show that if this were a malicious attack it would have been successful.

Th e fi rst attempt was laid out like this by the contestant: “I cannot browse to my

website and I think your product is blocking me. Can you check by going to this site

so I know for sure whether it is your software or not?” Th e technical support representative answered well by saying, “Sir, our product

would not block you from going to that site; it wouldn’t matter if I can go there or

not.” He declined the request.

Th e contestant did not give up there; after talking a bit more he again tried, “I

know you said your product would not block the site, but it worked until I installed

your software, so can you please check for me?”

Again he was declined his request: “Sir, I am sorry for that inconvenience but

again our product would not block you and my going to the site will not help you

fi x the problem.”

It seemed as if the request was going to be rejected for good when the contestant

tried one last-ditch eff ort and said, “Sir, it would make me feel better if you would

just try going to this site for me. Please, can you help me out?”

Th is simple request put our technical support rep over the edge and he opened

his browser and went right to the site. He had the right idea, he even had the right

security awareness answer, but in the end he wanted his “customer” to “feel better”

and honored his request. Th is could have led that company to a major pitfall if it

were a malicious attack.

Th e technical support representative knew that this information was not relevant

to that particular call. Like him, you must be determined to analyze whether the

information being asked for is deserved and relevant to the person with whom you

are interacting. Approaching this scenario from the other angle, what if the contestant

were a legitimate customer and the rep had declined to go to that website—what

is the worst that could have happened?

Th e customer might have been a little upset at being declined the request he

wanted but it still would not have changed the outcome. Th e product he had was

not the cause of his woes.

A social engineer often uses charm to start a conversation about the weather,

work, the product, anything at all, and uses it to reveal the information sought.

Th is is where a good security awareness policy comes into play—educating your

employees about what tactics might be used against them can save them from acting

out of fear.

In one audit the pretext I used was being the assistant to the CFO. Th e call

center employees had a fear of losing their jobs for rejecting the requests from

such a high-level management. Why? Th ey are not given the proper education to

know that rejecting that request would not cost them their jobs. At the same time

protocols should be in place for the employee to know when a request for information

is proper.

Th e perceived value of the information being asked for closely ties in with an

educated and aware person knowing that even minor tidbits of data can lead to a

massive breach. Knowing that the person on the other end of the phone doesn’t really

need to know what the name of the food preparation company for the cafeteria can

help an employee to answer appropriately. If you are an employer then help your

employees develop answers to these requests. In most cases a simple, “Sorry, I don’t

have that information; please contact our purchasing department if you want that.”

Or “I’m sorry I am not allowed to divulge that information but you can send an

email to info@company.com to request some of this info,” can go a long way toward

quashing many social engineering eff orts.

I mentioned earlier that creating an atmosphere that makes information seem

less valuable is also a tactic used by social engineers to get people to freely divulge

this “unimportant” information.

Using the contest example again, one contestant was asked to provide some

identifying information. His pretext was a company that was hired to do an internal

audit and when the target wanted to verify who he was he asked for something

off of the requisition form. Our contestant pretended to lean over to an imaginary

co-worker and said, “Jane, the gentlemen from Your-Target-Company wants the ID

number from the requisition, can you do me a favor and grab it from Bill’s desk?”

As “Jane” went to get the form the contestant engaged the target in idle chitchat.

“How’s the weather in Texas?” and “Have you ever been to Charlie’s Pub?” escalated

into things like, “Who handles the food for the cafeteria?” and “Want to see a cool

website we are working on here?”

All this happened while he was “waiting” for the ID number. Social engineers

use this tactic every day. Diversion and charm are key tools in many pretexts.

Information that is asked for during “chitchat” is perceived as having less value

because of the time in the conversation it is asked for. If the SE had asked that same

question when he was “verifying his audit fi ndings” it would have been met with a

diff erent attitude, but because he asked it during a friendly conversation so much

information was given freely.

Mitigation for this SE tactic is to ponder the value of the information that you

are planning on releasing despite of when in the conversation it is asked for. In the

earlier example, the target’s simply waiting for that ID number before continuing any

conversation would have been very appropriate and saved him from being duped.

Th is particular point is not always easy to implement because employees, especially

those facing the customer, must be able to release some information without fear of

attack. Simply being aware of the value of information cannot alone stop an attack.