



Social Engineering – Deceiving the weakest link in a Security Chain

WS 2004/2005

Version 1.3

Supervisor: Univ.-Prof. DI DDr. Gerald Quirchmayr

Author: Andreas Reichard (0126103)

Index

1.	Introduction	03
2.	The value of information	05
2.1	Knowledge means power	
3.	What is Social Engineering?	07
3.1	Axel Foley – A Social Engineer?	
3.2	Gathering information	08
3.2.1	Public sources	
3.2.2	Sympathy and credibility	09
4.	Motivation and Motives	11
4.1	Motivation for Social Engineering	
4.2	Motives of Social Engineers	12
5.	Characteristics of a Social Engineer	13
5.1	Personal skills	
5.1.1	Voice	14
5.1.2	Appearance	
5.1.3	Soft skills	15
5.2	Technical expertise	16
6.	Methods of Social Engineering	18
6.1	Asking for help	
6.1.1	The insider – A colleague asking for help	19
6.1.2	An Outsider	20
6.2	Offering help	23
6.3	Name-dropping	24
6.4	The use of authority, threats	26
6.5	Reverse Social Engineering	27
6.6	”Just asking for it”	28
6.7	Dangerous offerings over E-mail	
6.7.1	Persuasive E-mails	29
6.7.2	E-mails from a trusted source	30
6.7.3	Forged E-mails	
6.8	Phony Websites	31
6.8.1	How to get onto a phony Website	32
6.8.2	Dangers coming from phony Websites	33
7.	Victims of Social Engineering	36
7.1	Typical characteristics of persons vulnerable to Social Engineering	
7.2	Attractive positions for and attacker	
8.	Who might be a Social Engineer?	40
8.1	Persons	
8.2	How to identify a Social Engineer	41
9.	Defences against Social Engineering	44
9.1	Technical measures	
9.2	Education & Training	46
9.2.1	Awareness training design	47
9.2.2	The lack of interest on Security matters	48
9.2.3	Consistence of the awareness training	49
9.3	Organisational & Managerial measures	53
9.3.1	Security policies	
10.	Conclusion	59
11.	Sources	60

1. Introduction

As time passes, we hear and read more about Hacker activities and their effects on economical, political, but also private sectors of our daily life.

In order to prevent such attacks in the future, the people responsible are forced to tighten existing Security measures. By checking a network infrastructure for vulnerabilities and eliminating these by reconfiguration or the acquirement of better technologies and better Know-How, many people, network administrators (offering a technical approach to the problem), as well as managers (with an organisational point of view), tend to believe that they have done everything they can to prevent successful hacking attempts in the future.

This assumption is actually quite far away from the truth.

Although technical improvement of Security measures is, no doubt, a necessity, it covers just those parts of a Security Chain which can be controlled by technological means, which themselves are controlled by an administrator. Those parts which cannot be controlled this way, like the administrator himself (or generally the people who work with the systems), remain unprotected against *psychological* attacks directed against them.

This paper gives an introduction to the topic of "Social Engineering", which is a manner of attacking people using certain psychological means which will be explained throughout this paper. Supported by practical between theoretical explanations, it presents the theory of Social Engineering as well as practical measures for protection against it.

Here is a short overview of the content discussed within each Chapter of this paper.

Chapter 2, "*The value of information*", explains the general value of every kind of information. Understanding it is essential for a furthermore understanding of the methods used within a Social Engineering attack.

Chapter 3, "*What is 'Social Engineering'?*", defines the term of "Social Engineering" and explains how we come to use it.

Chapter 4, "*Motivation and Motives*", covers the motivation for Social Engineering and what motives a Social Engineer might have in his attempt to attack a company or a person by a manner such as this.

Chapter 5, "*Characteristics of a Social Engineer*", discusses the characteristics of a Social Engineer. The chapter is divided into two sections.

The first is about personal characteristics of a person which might make him or her (although not specifically mentioned like here, everything throughout this paper of course applies to both sexes. Social Engineering is really not a question of sex, although the methods used to apply it can be) a successful Social Engineer.

The second shows how technical expertise aids in achieving the goals of an attacker who uses Social Engineering as part of his attack.

Chapter 6, "*Methods of Social Engineering*", some of the typical methods used within a Social Engineering attack. It shows, among other things, how the characteristics discussed in Chapter 4 are put into practical use by a sophisticated Social Engineer. This process begins with the retrieval of information from unsuspecting victims and continues by putting this information to use through technical expertise.

Chapter 7, "*Victims of Social Engineering*", looks for similarities in the characteristic behaviour of victims of a Social Engineering attack. It shows that there exist profiles which can make someone a particular attractive victim for a Social Engineering attack – or not.

Additionally, this chapter introduces positions within a company, which might be attractive to a Social Engineer and therefore in danger of an attack. Referring to the characteristics discussed before, it explains, why this might be so.

Chapter 8, "*Who might be a Social Engineer?*", identifies people, who might be in a good position or might have a motivation to make a Social Engineering attack and how to identify such an attack if it takes place.

Chapter 9, "*Defences against Social Engineering*", explains the technical and, more important, organisational and managerial kinds of defences that can be raised against Social Engineering attacks.

In **Chapter 10**, "*Conclusion*", you'll find a personal conclusion from the studies of the material and the preceding chapters.

2. The value of information

Generally we often assume that information that *we* do not consider important from our point of view *is* really not important at all. Therefore we tend to believe that this so-called "unimportant" information may be shared with other persons, especially if they give us a good reason why they might need it.

Since (as naive as this sounds) we generally like to help others and do not believe that there could come any harm out of it, we handle this information in a relatively careless way. But even the seemingly most unimportant information may prove highly valuable to a person who knows how to put it to use – for example a Social Engineer.

Fact is, there is no such thing as "unimportant" information nor a need to tell anyone about it, unless this person has a very good reason to know and can provide us with proof for that need.

Every kind of information is valuable because it may be used for exploits in ways that will be discussed later. If we think of an information as being unimportant, that is just a *personal judgement*, which may apply to us personally, but not to others and surely not to a whole company.

2.1 Knowledge means power

The better an enemy is known to a defender, the better stand his chances of holding off an attack directed against him. This simple knowledge is as old as mankind itself.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

(Sun Tzu, "The art of war")

With the knowledge about weaknesses in his enemy's defence, an attacker can look for ways to take advantage of these. Therefore, being a potential victim, it is in the defender's interest to keep knowledge about these weaknesses safe and unknown (at least as long as countermeasures have been successfully implemented), not only to persons with possible intentions of exploiting them, but to everyone else as well (since it is unpredictable how this information might spread behind one's back).

Knowing that the chance of achieving his goal increases with getting as many of these valuable information pieces as possible, an attacker will be looking for ways to obtain such information, even taking into account high efforts to do so.

One kind of persons, who do such things, are Social Engineers.

Knowing that people generally tend to trust others (at least unless given a reason to change that behaviour, for example bad experience or a Security policy advising them to do so), Social Engineers use specific communication and

manipulation techniques to talk seemingly unimportant information out of people who would never think of what could be achieved with that information if one just knows how.

But not only Social Engineers, other people as well have learned that supposed "unimportant" information may help them on their way to achieve their goals. Big corporations base whole marketing strategies upon the gathering of such information because there are still lots of persons who do not think it may be wrong to tell everybody who wants to know about it. Police officers, private detectives and others sometimes use these techniques as well.

Of course this shall not mean that we are not allowed to share any kind of information with other people in order to protect ourselves, those we care about and others. This is not only unthinkable, since the sharing of knowledge is based deep within human society (there exist even institutions based on this, for example the Open Source Community), but also unnecessary paranoid. But to think a little more about what we are telling other people, if they really have a need to know and if we can foresee some of the consequences this might have would be most wise in order to prevent exploits based on the information we publish.

3. What is "Social Engineering"?

Whenever a communication takes place between two persons, this communication can be exploited. What someone needs to be as to do so is being a good liar.

According to Ira Winkler, author of "Corporate Espionage", the Nazi regime used the term for the manipulation of an entire population. In the Soviet Union it was used as well, for the same reason. In the 1980's hackers chose the term "Social Engineering" for describing their methods of obtaining information from other people by non-technical means. This is actually the definition on which this paper is based.

Therefore, "Social Engineering" is a manner of influencing people into doing things that, under normal circumstances, they would not be doing and which, most of the time, lead to their harm, or other's. It is a manipulation technique which can be done over the phone, but also in direct contact to the victim.

3.1 Axel Foley - A Social Engineer?

Whoever has wondered about Axel Foley, the movie character played by Eddie Murphy in "Beverly Hills Cop", and how he manages to get into places where he is not supposed to be and get information he is not supposed to know about, may have noticed that, besides the fact that he is ever-talking (which gives the movie a humoristic touch), Foley seems to judge the people on impulse and tells them everything that comes into his mind which would make them believe that he has a right to do something when he actually does not. In other words, he is just lying and making up stories, but he is very good at it.

Although, because this is a movie, Foley's behaviour is clearly exorbitant, some of his doings clearly fall into what we call "Social Engineering". With a charming and sympathizing smile, self-confident and ever-talking, Foley just appears spontaneously and gives explanations why he has to go somewhere where normally people would not be allowed in. This is more or less, what a Social Engineer might do (if he chooses to appear somewhere in person).

But Social Engineering is more than just that. Actually, unlike Axel Foley, Social Engineers in preparation or execution of an attack try not to go anywhere in person because they fear that anyone could recognize them later or their attempt might be discovered.

Instead they gather information, first in taking advantage of every possible legal information source they can find. Which sources these are depends on the target. If it is for example a company, then one of the first things a Social Engineer would do is go to the company's Website and look out for information available to the public.

If it is a person, a Social Engineer might take a look into the phone book to find out a phone number and an address or do some researching on the Internet in order to find out something about that specific person. For this, excellent search tools and -engines exist nowadays, allowing with a minimum of time and information the extraction of valuable information about a target. One of them is

www.google.com, which, besides the ordinary functionality of a simple search-engine, has a number of specific commands to specify a search and get more and better results (this is known as "Google hacking").

So what Social Engineering, at the beginning, is about, is gathering information (that is exactly why it is so important to understand the value of information in general, which was discussed in Chapter 2). The more an attacker advances to his ultimate goal, the more illegal become his methods to obtain that information, as will be explained next.

3.2 Gathering information

The most important thing a Social Engineer needs for being able to influence people is *credibility*. This he obtains by gathering information that makes him appear like someone who has a right to know certain things which, for example, are normally meant to be known only to a handful of people. When the Social Engineer appears to be from the inside (thanks to the information he has gathered before and has been able to present to the people he deceives in a way to obtain credibility), people all too often do not hesitate to give him the desired information, not wondering if he really has a right or need to it.

The process of information-gathering with its coherency in the increase of information, credibility and illegality can be explained with the following diagram.

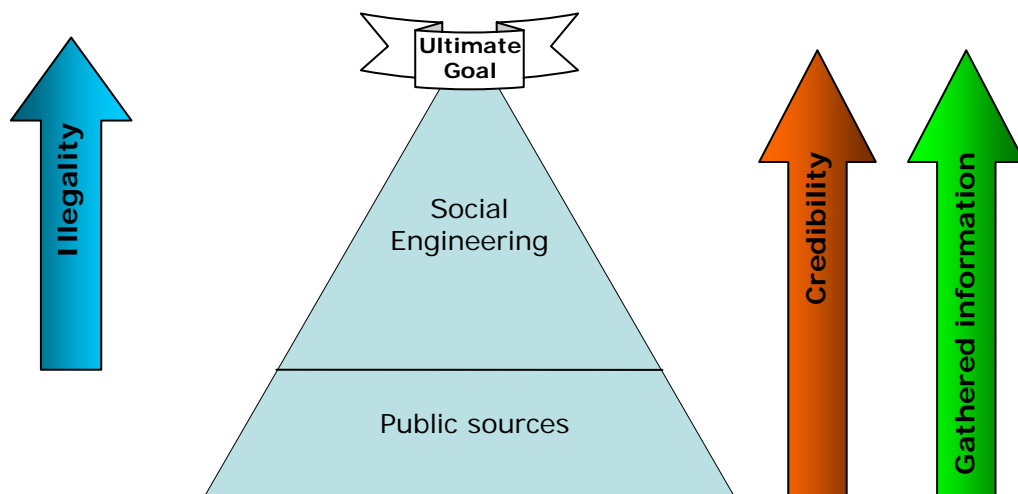


Fig. 3.2 The process of information-gathering

3.2.1 Public sources

At the beginning (the bottom of the pyramid), a Social Engineer tries to get information from every public source available. After all, why should he bother with obtaining information by illegal methods, when lots of it can be gathered by means which are perfectly legal, if one knows how and where to look for it?

There are many ways to gather information about something or someone by public sources. The advantage for the Social Engineer here is obvious, no one can arrest him just for doing some researching.

Public sources would be for example the Internet (for example via *www.google.com*), phone-hotlines, public phonebooks and collections of online researching-tools (such as "Net Detective").

There exist Internet companies who offer to provide social security numbers just by knowing a person's name and address – for \$5!

How easy it can be to get information about a person online is also explained by Carol Lane in her book "Naked in Cyberspace: How to find personal information online".

"In a few hours, sitting at my computer, beginning with no more than your name and address, I can find out what you do for a living, the names and ages of your spouse and children, what kind of car you drive, the value of your house and how much you pay taxes on it. I can uncover that forgotten drug bust in college."

Although this quote refers to the U.S. (in Europe the laws for protection of personal information are stricter), it makes quite clear that there exist possibilities of getting access to personal information of which a person would, under normal circumstances, never think of.

Lane's conclusion is:

"If Information exists anywhere, no matter how carefully guarded, it exists somewhere else, where virtually anyone can gain access to it."

How true this is can be seen by the fact that many companies encrypt their sensitive data traffic but often do not encrypt their backups of the very same data. So all an attacker theoretically has to do to get access to this data is not to attack the well-protected system handling the data, but the backup system.

3.2.2 Sympathy and credibility

The more information a Social Engineer gets, the more credible he becomes for the people he talks to. Yet, so far, no real Social Engineering has occurred, only public sources, which are legal to use, have been used to obtain information.

Illegality starts, when one begins to lie to other people in order to extract even more information from them, *there* using for example Social Engineering. With taking that step, one crosses the line of legality because from that point on others have to be deceived and given trust exploited, which is possible thanks to the credibility earned before. This, of course, is illegal.

To create sympathy, a Social Engineer appears to be a charismatic, likeable and attractive being. To create credibility next, he lets other people know about some of the information he has gathered so far (often speaking in a certain lingo, like being among a selected group of persons) in a way so they see him as a colleague, an insider, a person like themselves who may even be in the same

company, although, sometimes, especially in bigger companies where it is impossible to know everybody, they have not seen him before.

One popular approach of Social Engineers is to present themselves as "the new guy". Nobody suspects anything if he asks a lot of questions then, people will even be eager to help the new colleague in his first days within the company (remembering how *they* felt on their very first day; a Social Engineer will try to trigger that memory, so to increase a feeling of sympathy for him).

Social Engineers usually try first to build social bonds between them and their victims, for example by showing understanding for their victim's situation to later ask indirectly for the same, which creates a feeling of guilt and is exactly what the Social Engineer wanted to create in the first place. This is a very common method of Social Engineering, details on it, as well as some other methods of Social Engineering, will be explained in Chapter 6.

4. Motivation and Motives

Before going into further details we should distinct between *Motivation for Social Engineering* and *Motives of a Social Engineer*, which should not be mistaken as being the same. The following explains why a distinction does make sense.

4.1 Motivation for Social Engineering

The question we ask ourselves here is "Why would people make use of Social Engineering techniques?" The answer is simple. Social Engineering works like a tool for the one who knows how to handle it. For such a person, having a specific goal, arises the question of how to reach it. Might not Social Engineering be an attractive alternative to other, more straining methods? In many cases it is.

Imagine for example a person who needs to hack into the computer system of somebody else within a company. What is the first thing that pops into our minds when we think of this scenario? Probably a nerd, rubbing his hands together before typing lots of seemingly weird looking commands into the command shell of his computer before, finally, smiling with satisfaction, proclaiming that he has achieved to crack the user account and has access to whatever information he wanted to have.

What less people would think of would be a guy that thinks different, *before* starting to type any commands into his computer.

This guy might think "Hmm, maybe I *could* get into that computer if I'd spend all night looking for a Security hole somewhere in that other computer's operating system or any of its applications, but wouldn't it be much easier to just ask somebody the right questions in a very specific manner, so that nobody would suspect that in the end I probably end up with an account with full access to the system that is my target?"

Unimaginable? Not at all, that is one reason that makes Social Engineering so popular.

Not only does it offer a workaround for a task that, in many cases, would otherwise mean an enormous effort, but it may sometimes be the *only* possibility to get to some sensitive information at all (if this cannot be reached by technical or other means).

However, before asking ourselves "So, why do people still hack into computer systems if it really was *that* easy just to talk somebody out of the needed information for a legal login?", we must consider one thing:

Social Engineering requires a lot of preparations – and skills (more about this in the next chapter). Not the kinds of skills that one might read about in a book (although you can learn about it from books too), but more the kind that one has to experience for himself, out in the field, talking to people, interact. There is hardly another way to develop an own and credible style of Social Engineering, since it so much depends on what kind of a person you are and – more important – what other people think of you. So one really has to learn about this if he

wants to be a successful Social Engineer, it all comes with experience, training and testing.

So, in short, the motivation for Social Engineering is it being a completely different way of approaching the goal one might be looking for. Other, perhaps more common (mostly technical based) approaches might get us there as well, but often with much more effort.

A good example for this would be a Social Engineer with technical expertise who asks himself "Why should I run a brute force attack on a system to get hold of an account (although I could, but not without raising the suspicion of the responsible administrator who checks his logs on a regular basis) when a simple phone call can provide me with just the same, but without raising any suspicion, if I make it the right way?".

And, again, there are many situations where Social Engineering is the *only* way to get to some information because there simply is no technical way to achieve it. Because when we talk about Social Engineering, we talk about attacking those parts of a Security Chain, which are the weakest – the persons operating in it.

4.2 Motives of a Social Engineer

What brings persons to use Social Engineering on others? To answer that, we only have to take an honest look at ourselves. Is not the information we are not supposed to know about the one we most strive for?

It seems so, there were cases of Social Engineers who broke into corporations using Social Engineering, just for the thrill whether they would get away with it or not.

Imagine a lover who found out that his partner had been cheating on him. Might it not be interesting for him to read his or her E-mails?

Or the private detective who works on a case and is stuck there because he cannot get hold of some information he needs.

Without wanting to plunge deeper into the depths of human behaviour we sure can think of many other scenarios, some morally more disturbing than others, where Social Engineering might be a solution to the question of how to get to information that, by normal means, would be out of our reach. What they all have in common, is that in every one of them we can identify someone who is willing to spread false information about him or others just to get to some valuable information.

When does that happen, who would do such a thing? Very many people would and actually do that, out of revenge, personal or financial gain, thrill and challenge. Most of them by just lying with whatever comes into their minds, others approaching more considered, probably by the use of Social Engineering methods we will talk about in the following Chapters.

Which persons and in what positions might be a threat concerning this matter will be the topic of Chapter 8.

5. Characteristics of Social Engineers

The most important thing for a successful Social Engineer is what impression he makes on others, especially on those who can provide him with the information he wants to obtain, but also on those who just help him to "climb the ladder" until he gets there.

But information is worth nothing if one does not know how to use it. Therefore, although with this we are not talking about "Social Engineering" anymore, it would be useful for a Social Engineer to have some technical background as well, or to know and trust someone who has it, in order to put the knowledge gained through Social Engineering into practical use.

Since this part is not really about Social Engineering, it is kept quite short in this paper. For further studies on technical approaches, I recommend reading "Counter Hack" by Ed Skoudis, which is a good book for beginners on these matters. More sophisticated readers might prefer reading the "Hacking exposed" book series which offers a deeper insight. References to these books can be found in Chapter 11.

Returning to the topic of Social Engineering, we now go into the details of what a person must be like and what skills he must have to be a successful Social Engineer, in order to hopefully recognize one when confronted by him.

5.1 Personal skills

How to judge a person if one might trust him/her or not? Directly asking someone that question might reveal answers like "I must know him for quite some time", "I can tell that from the look in his eyes/the tone of his voice" etc.... but think about these arguments - are they really "hard" reasons to trust somebody? Some are, like if you have known someone for quite a while you might get to trust that person and be right about it because this person has proven over the years to have earned this trust. But others definitely are not. Why not? Because one might have learned about what he must *appear* to gain trust from others and just play a good act.

So the personal skills needed to successfully social engineer on other people are those that give people the impression that they can trust you.

It is necessary to differ here, between both sexes, male and female. Although many things apply for both of them, it is obvious that, considering a heterosexual victim, one might be more vulnerable to Social Engineering if the attacker comes from the other sex and knows how to put that to his advantage. Although there are few who would admit that, it is (with few exceptions, among them homosexuals) a fact, our sub consciousness is to blame for that.

People familiar with the concepts of NLP (which stands for "Neurolinguistic Programming") might note that many of them find their way into Social Engineering (for those who never had anything to do with NLP I recommend reading "Introducing NLP" by Joseph O'Connor and John Seymour).

5.1.1 Voice

Very often Social Engineering is done over the phone. This gives the attacker the possibility to remain relatively anonymous while the phone might play to his advantage on another matter – his/her voice. Social Engineers know about the effect a pleasant voice, especially over the phone, can have on their targets, so they sometimes work hard, do voice training, to improve theirs.

Male Social Engineers train themselves to speak in a deep, pleasant-sounding tone while females try to sound sensual and sexy in order to increase their attractiveness on their victim and gain their trust. This is, not only, but especially important when talking over the phone since their victim is unable to see them, so the only way to appear attractive to them is through their voice.

5.1.2 Appearance

If a Social Engineer chooses to appear in person to attack a victim (which is relatively uncommon as he puts himself into the danger of later recognition, but sometimes he has no other choice) he will surely try to add the fact that his victim can see him to the points of his advantage. How this is done depends completely on the specific situation.

Imagine for example an attack on the female receptionist of a large company. A Social Engineer might choose to appear as a business partner, dressed elegantly and acting this way as well. Being always friendly, kind and understanding (maybe even a little flirting) he is instantly likeable to the person he is attacking which puts him into a good position for proceeding with his attack. If his victim is rather shy and unsure, the Social Engineer will probably act a little bit like a father, making compliments about how the receptionist is doing her job so very well and therefore earning her sympathy. If she is stressed and complaining about it (which already is a sign for sympathy since it is clearly not part of her job to complain in front of business partners; it is more a private, personal part which is exactly what the Social Engineer is looking for), he will show understanding, probably making up a story of himself doing a similar job in the past and feeling exactly the same way about it. He might even go a step further and offer her a job with better conditions. Imagine being disgruntled with your job and someone who seems to be successful with his job appears in the company entrance hall, tells you how good you handle your job, shows understanding for the pressure you are under and suddenly makes you a job offer. Would such a person not be someone you would do a small favour if he asked you for it? Having considered the topic of this paper probably not, but many people would think otherwise. That is exactly why Social Engineering is done successfully many times.

But the same attack could be carried out completely different. The Social Engineer might have chosen to appear like a plumber, claiming that someone had told him last week to come here and take a look at a specific restroom where the toilets are out of order. When the receptionist calls that "someone" she might probably be notified that this person has taken his first day of vacation and will not be back for a week (which the Social Engineer had found out earlier, that is

why he had come at this specific day). The correct way to handle this situation would be to let the plumber wait until the situation is sorted out.

However, imagine that the plumber is complaining that he has to go to another appointment and the restroom, which he claims is near the conference room (and therefore should not be out of service since a conference is about to take place there in half an hour – the Social Engineer has found this out as well) has therefore to be repaired quickly. The receptionist might have been in a similar situation once and knows how unpleasant these formalities sometimes can be "... so, for God's sake, why not let him in. After all, he's just doing his job and already has had a busy day with all that confusion about the vacation of his contact within the company. And the restroom needs to be repaired, after all there is this conference...".

So without further delay, just by appearing like someone who has a right to be at a certain place, a Social Engineer has gained access to a restricted area where, by other means, it would have been hard to impossible to get in.

5.1.3 Soft Skills

Social Engineers are generally very good actors and liars. They extract certain information from and about their victims and change their own behaviour in a way that, combined with the information they have gathered so far, will get them a step closer to their ultimate goal (this is sometimes called "cold reading").

To be able to do that, they rely on their ability to appear like- or at least trustable to other people. We already mentioned that they try to accomplish this by using their voice and appearance, but the most important thing has yet not been mentioned – Soft Skills.

First we need to define what Soft Skills are. One definition for Soft Skills is "the knowledge about how to handle persons and decisions". You should, however, note that within this paper we examine Soft Skills only in the context of Social Engineering. Actually it is a much broader field which covers many more aspects than the ones we are about to analyze.

The basic principle for the development of Soft Skills is attentiveness. By this we mean the ability to identify other people's sentiments and use that knowledge to adapt our own behaviour, the way we do and say certain things (here NLP comes into play). So it is less about IQ (intelligence quotient), but more about EQ (emotional quotient) that gives a person Soft Skills.

Now it should be easy to understand why those are so essential to Social Engineers. They try to perfect the art of reading as much as possible about a person just from observing that person or interacting with it. Being able to act on impulse as well as being very flexible, they may then act in a way that makes them like- or trustable (although this is not always the case, as we will see in the next chapter there exist other methods of Social Engineering which do not rely on sympathy at all).

Social Engineers need a great deal of self-confidence to start and keep up their act. While performing, they always walk on a tightrope (which for some of them is the real goal in doing what they do, they are looking for the thrill of how far

they can go until they have to retreat without their act getting discovered) since they constantly have to observe their counterpart and react very quickly on whatever it does, never losing the ultimate goal out of sight but being ready for whatever may come along spontaneously.

This might look a little bit like a game that Social Engineers are playing with their victims, this assumption is actually not so far away from the truth. But, of course, no Social Engineer just jumps into such a situation unprepared. The need for being prepared for every kind of occasion that might come up spontaneously does not mean that Social Engineers have no need for the other preparations *before* they get to work. A Social Engineer usually plans his attacks very detailed, making backup plans if something does not proceed the way he originally wanted it to (which happens quite often since human behaviour *is* quite unpredictable). This is done mostly by information gathering, as described in chapter 3.2.

Putting this information to use, the Social Engineer uses his Soft Skills as well as other things (voice, appearance) to get closer to his goal, step by step, just as if he was climbing a ladder.

A good Social Engineer is then, for example, able to make someone skip existing Security measures (like waiting until someone can confirm that the plumber from the example above has indeed been hired for a job) because of certain circumstances (which may have been created by himself or an accomplice).

We will go into the details of specific methods of Social Engineering in Chapter 6.

5.2 Technical Expertise

We have already mentioned the value of information at the beginning of this paper. But information is only valuable to a person who knows how to put it to use. In the context of an attack this use might, by all means, be technical. Note, that this has nothing specifically to do with Social Engineering, which describes just the manner of information gathering over the deception of people.

However, it is mentioned here because many Social Engineers also have enough technical Know-How themselves to put the gathered information to use or at least know people who are willing to do it for them. This combination of a possible psychological as well as technical attack scheme makes these Social Engineers even more dangerous.

The following example will explain this. Imagine a successful Social Engineer who has finally gotten what he wanted, the login information of an account on a computer system with remote access to it. Logged in, he will then be able to extract the information he was originally looking for. But what would he do without having knowledge about how to handle the operating system installed on that computer? With the account information he could login, alright, but what then? What if the information he is looking for is not even on that specific machine, but on another within the network which to which he first has to be connected to?

Therefore, at least a minimum knowledge about the system a Social Engineer wants to access to is essential, without it the probably hard-gathered information is worthless to him. The more of it he has, the more dangerous he becomes, as he has not only some of the knowledge of what some people call a "Hacker" (be aware that there is a distinction between the term "Hacker", that being someone with the expertise to do harm, but only seeking knowledge, and "Cracker", which is someone who uses this expertise with the intention of actually doing harm) but also a much broader field of possibilities for getting the information he wants, thanks to his Social Engineering abilities, including each and every person who is connected to it.

The devastating effects of the combination of Social Engineering skills as well as technical expertise can be seen when looking at the case of the probably most famous Hacker, Kevin Mitnick (whose book about Social Engineering was taken as a source for this paper, see Chapter 11), who not only had extraordinary Know-How about computer systems, but also mastered the art of Social Engineering up to the point where he was said to be able to extract nearly every piece of information from everyone.

It is said that he once said that the reasons why he had been able to break into so many systems were not so much his technical abilities, but more his ability to Social Engineer on people.

6. Methods of Social Engineering

Social Engineering depends on human behaviour and therefore is a very dynamic field. However, experience has shown that there are some typical methods of Social Engineering attacks which repeatedly occur in variations. Knowing about them can make it possible to prevent attacks in the future or at least lessen the damage caused by them because it enables the creation of Security policies which tell how to deal with such attacks.

Important to know, concerning all of the following methods, is, as already mentioned, that Social Engineers try to know as much as possible about the person they attack, before they actually do so, in order to predict how it reacts when put into a specific situation (for example if it has to make a possibly critical decision whether to grant someone access to a restricted resource, or not).

Some Social Engineers even go so far as to create a database with information about their victims, there storing information like if they are new or experienced company members, cooperative or distrustful when confronted with more delicate Security matters, well informed or ignorant and also even personal information such as hobbies, the names of relatives, ages, favourite sports, vacation spots etc.

One of Kevin Mitnick's partners known by the pseudonym of "Roscoe" is said to have done so in order to memorize all the information he got about the people he and his fellow Crackers later Social Engineered on.

The following subchapters describe some methods of Social Engineering. Countermeasures against these attacks are described in Chapter 9.

6.1 Asking for help

Asking for help is a very common approach of Social Engineers.

Most people like to help others when they get the feeling that those are in desperate need for aid. It is an instinct within people's hearts that makes them believe that they can generally trust anyone to be honest to them when calling for help.

This makes it very easy for a Social Engineer to use this instinct to his advantage. All he has to do is create a scenario credible enough for the people to lower their shields of suspicion and offer to help or agree to do so when asked for it.

When attacking with this method, there exist two species of persons a Social Engineer wants people to believe he belongs to. The first is an outsider, the other one an insider, a colleague of the victim (and the attacker will press on this during the attack!). It is not hard to guess that the role of an insider is usually preferred by Social Engineers, although there are some situations in which the role of the outsider suits him better.

Depending on the complicity of the attack plan, a Social Engineer is often forced to not only take over identities, but to change them as well, in order to proceed

with his attack. In such cases he collects enough information about the first victim of his "chain of identities" to make it credible to others that he *is* actually that victim (this depends, of course, totally on the scenario; under certain circumstances such an approach would have little to no chance of success, for example within a small company where all the people know each other so well that they are able to recognize a voice on the phone that is not familiar). To do that, he needs not only enough information about the person he is "becoming", but also to adopt the manner of speaking of that person (lingo).

This means, for example, that a Social Engineer attacking a company with an Intranet-system named "Intrasys" will not ask another employee "Can you check this for me on the Intranet?" but rather "Can you check this for me on Intrasys?" Mentioning the name of the system makes it more credible for others that he is really who he claims to be, someone from the inside. Who else would know the name of the Intranet-System (although no one bothers to hide this name...)?

Once the attacker is "accepted" as an insider, he goes on by collecting enough information about someone else (probably the same person who came to trust him in the first place) to take over his identity in order to proceed with the attack, and so on.

6.1.1 The Insider – A colleague calling for help

In big corporations it is impossible that all employees know each other. People come and go, trainees, hired co-workers and visitors can make it very hard for someone to distinct between people he can trust and others whom better not, without offending anyone.

However, when someone enters your office with the words "Hi, you must be Joe, right? I'm John, the new guy from Network Security. I just wanted to come by and say hello to everybody" - would you really ask him first for his Security badge before revealing any information, which he asks you for, right before he told you how his first day here has been and how nice colleagues he has? Many people would not, because they do not know that a Social Engineer always tries to hide the really important questions inside a normal-seeming, small-talk conversation as well as because they fear offending the other.

Nevertheless, they would have, in a friendly way of course, any reason to ask for identification, before revealing any sensitive information to him, there is nothing offensive about that.

But a Social Engineer tries not to take any chances (although, in a normal scenario, he has to do so, many times), so he will only take an approach like the one described above if no other suits him better. A friendly new colleague might seem ok for his fake identity, but a colleague who is in desperate need of something might put the victim under some pressure, which could improve the chances of success of the attack. Especially if the Social Engineer combines his attack with other methods such as "name-dropping" or the use of authority and threats (both methods are specified in the following subchapters).

So why not change his identity into something more useful when attacking his victim? Not just the "friendly guy", but also the "stressed colleague" who needs

help in order to get his job done which was given to him under troubling circumstances. Friendly he may be, nevertheless, but saying things like "Hi, you must be Joe, right? George told me where to find you, I'm John, the new guy from Network Security. Listen, sorry about the hurry, but they just pulled me over to George's department because of some problems they have with User-Authentication. They need me to get this done here in the next 30 minutes, because there's going to be a meeting with the CEO ending in 45 minutes, the systems have to be up and running 'till then. Normally they would have asked James to fix that, but it's his day off and he's unreachable. George told me you know the root password for the Server, so I need it right now to get this thing working again before that meeting's at an end."

(Note: The "root" account is the administrator's account on computer systems using "Unix" or "Linux" (which is actually based on Unix) as operating system. Whoever has access to this account has complete power over the computer system, which is very often what an attacker is looking for when attacking such a system.)

Who wants the blame if the systems are not up and running when needed, especially in front of the CEO? No one, of course, so better help that friendly, poor (because so much stressed) colleague to get his work done quickly, instead of asking formal questions. After all, he said he came from George, also knows James, so it should be ok...

Taking a closer look, the method here contains more than just asking for help, it uses also "name-dropping" (mentioning the names of well-known persons called "George" and "James") and the use of the authority (in this case that of the CEO). Many people put into the above situation spontaneously think "if the systems are not running at the appropriate time, this will raise questions about who is to blame for that – that better not be me, especially not if the CEO is sitting next to my boss!".

Social Engineers know this very well, so they try to create a scenario in which their victim will behave in a manner predictable for the Social Engineer, in this case based on fear and companionship with a fellow co-worker.

6.1.2 An Outsider

Although some Social Engineers have enough knowledge (for example about a company, maybe because they have worked there before) to sound credible to insiders from the very beginning of their attack, many times they do not. In such a case it is logical that the first link in a chain of identity-takeovers is the identity of an Outsider, in order to get enough information about an Insider to take over an inside identity later.

This could be for example a repairman, an external co-worker, a business partner, etc. A Social Engineer just has to know how to play his act to sound credible and then proceed in the chain of identity takeovers.

It can have various reasons why a Social Engineer approaches a victim posing as an Outsider. These are, among others:

1. He was not able to gather enough information in order to sound credible enough to be taken as an Insider.
2. He wants to keep more distance because of fear of recognition (in case that the attack is to be discovered).
3. In the scenario it is currently not necessary to pose as an Insider

Ad 1.)

The Social Engineer has to face the fact that he is not able to collect enough information to pose as an Insider and expect to appear credible. So he does not even try it, but takes his chances in posing as an Outsider.

Ad 2.)

This is one reason why Social Engineering is often done over the phone. The Social Engineer knows that if his attack is to be discovered, tracks would probably lead back to him. So he decides not to take that risk and better physically stays away from his victim, taking into account that this could make it harder for him to get to the information he wants.

Ad 3.)

Sometimes there is no need for an attacker to pose as an Insider. The information he wants can also be known to an Outsider, sometimes the chances stand even better then. For example it is more likely for an outside repairman of a telephone company to ask about a dialup modem line which can be used to dial into the company network from the outside, than for an inside clerk, who definitely has no need to know such a thing.

Whatever reasons an attacker has, the goal remains the same: Appearing credible to the victim. If not under circumstances which fall under point 3, this is generally harder than if he would pose as an Insider.

However, there are some typical approaches of Social Engineers when posing as an Outsider.

The researcher:

Very often Social Engineers claim to be researching on some kind of topic related to the institution they are attacking. This gives them the chance to ask very specific questions without raising too much suspicion. After all, it is expected that a scientific researcher takes his work seriously, with all the details necessary to finish it.

Social Engineers choosing this kind of attack can claim to be a student writing a book or paper or researching for a lecture. They can often expect cooperation from their victims, since many of them have been in the same situation at one time or another and were grateful then, if given the information needed to complete their task.

Note that the Social Engineer sometimes tries to create a scenario similar to one that is known to his victim, in order to create understanding for his situation. We tend to trust things that are known to us, which is exactly what this kind of approach is about.

The Social Engineer would then ask some questions whose answers are mostly without any real value to him. But among those he also asks, quite inconspicuous, some questions where the answers are really what he is after. Other questions and small-talk are just to create a diversion from the really important questions because among them these are unlikely to be noticed.

The employee from another company:

Also a very common tactic of Social Engineers is to appear to be from another company, making some kind of service for a victim company and therefore being in need of some information.

Of course this may mean that another Social Engineering attack has to be made first on that other company in order to gather enough information about it to sound credible to the victim company.

In such a case a Social Engineer often tries to appear like "just a poor, stressed employee who tries to get his job done". Creating this scenario gives anyone who asks questions about Security matters the feeling that he is making life even harder for a man that so far has had a bad day anyway and is just trying to do his job (remember the plumber case we talked about before). The additional use of methods like name-dropping, threats or the use of authority can aid a Social Engineer in getting along here.

Popular jobs faked by Social Engineers are that of an employee of a telephone, network- or computer company, member of a cleaning crew and other jobs of companies whose services are needed in the majority of corporations today.

The business partner:

In some occasions Social Engineers have been known to fake being a business partner of the victim company. Within that role they put employees of the victim company under the pressure to act in a manner not offensive to them, as this would be bad for business.

After all, no one wants to be the one screwing the partnership with another company because one of its managers felt treated in an inappropriate manner.

Take the example of a perfectly dressed up and friendly person entering the entrance hall of a victim company. Telling the receptionist that he has an appointment with one of the top managers in the company (and knowing very well that this very manager is unreachable at the moment, that he found out by Social Engineering on another person), he waits patiently until the receptionist tells him what he already knows, that the manager is on vacation.

Cursing his secretary for having made a mistake he then complains about the lost amount of time and asks if he could somewhere connect his Laptop to the Internet, just to quickly send away some E-mails and reorganise his time schedule.

Since he looks and acts so professional, for the receptionist there is no doubt that he is what he claims to be, a business partner who was about to have an appointment with one of the company's top managers. However, that claim can

hardly be proven since the very manager he wants to meet is on vacation and said to be on his boat, more or less unreachable.

Understanding the annoying situation for the likeable (and maybe, if the receptionist is female, also attractive and charming) businessman, the receptionist shows him the way to where he can connect his laptop to the Internet. The risk of an external laptop connected to the company network in order to access the Internet would not come to the receptionist's mind, but the "businessman", actually a Social Engineer, just waited for his chance to scan the company network for possible weaknesses and maybe, if given the chance, install some malicious software on it, to later connect himself to the same network from the outside (this kind of software is called a "backdoor").

6.2 Offering help

A very tricky kind of attack is to secretly cause a problem (or make it look like there exists one) and later offer a solution to it. The people affected by the problem will be glad to have someone able and willing to solve it for them. Therefore they tend to ask not so many questions about the rights of this person to access the data of the application where the problem has occurred, if only they will be able to continue with their work. Plus, they will be eager to help the attacker out of gratitude on some other thing that he probably requests from them.

An attack of this kind actually can consist of two attacks, depending on if the problem the attacker is talking about really exists or is one that he has made up. In the first case, the attacker has to cause the problem in order to offer a solution afterwards. As causing a problem is an attack itself, the attacker might use one of the already described methods to do so.

Later (not depending on the fact if there really exists a problem or not, for in the eyes of the victim such is the case) he calls the victim who is affected by the problem and acts like it is known to him and it is his job to see that the people affected by it can continue with their work as soon as possible. Since time is usually short, affected people will be grateful and not ask many questions about what exactly they have to do to help solving the problem as long as the one who tells them what to do seems to be someone who can help them solve it (for example someone from Network Security who claims that the problem was caused by the recent installation of a new Security patch; in any way someone they can trust). Therefore such a person can easily tell someone to download and install software from an unknown (maybe even one inside the network infrastructure or one that was made to look like that) source calling it a "bug fix" where in reality the victim will be installing a backdoor or other malicious software instead.

The following example shows this:

When an attacker has already succeeded in his first attack causing the original problem (only if this is really necessary, of course, in this example that is the case), he could for example let the victim's workstation's network interface be unknown to the network's DHCP-Server. This means that the DHCP-Server will

not assign an IP-Address to this workstation because it does not recognize its MAC-Address (which is a unique identifier by which network interfaces are identified by DHCP-Servers), meaning that the workstation will not be able to connect to the company network.

Later the attacker calls the victim to offer a solution to this problem. If he calls in the morning, when the attacker expects the victim to have just arrived in his office (which is something that can be found out with just one phone call), he can say something like "We've been having some troubles after a Security update over here and have been working all night to solve them. Still, we're not quite finished and they've told us that you should be among the first to be able to log onto the network again, that's why I call you."

Confirming the existence of the problem (because he really could not connect to the network right before the attacker called), the victim gives the attacker, as requested, his MAC-Address, which he can read from a sticker attached to his workstation. With this information the attacker reactivates the victim's account, for what the victim normally is most grateful.

After that the attacker could say something like "You should now be able to log onto the network again. But we've not solved all of our problems here yet, because of that it may happen that you loose your connection again. To prevent this, we've written a small script which you should execute before you carry on with your work. So if you can spare just a few more minutes, I can talk you through it. Normally we would do all this automatically over the network without bothering you, but as I said, we're not so far yet and just would like to get you back working without any further troubles."

For the victim it looks like the attacker does some extra work just to get his computer running securely again. Since the attacker is doing him some favour with this and has already had a hard night of work, the victim will be glad that he can continue with his work and do anything the attacker says.

Never would he think of that friendly guy that he is actually talking to a Social Engineer who has somehow compromised the DHCP-Server (probably by first attacking another person) of the network infrastructure? Unlikely.

When the attacker tells him how to execute the script, this actually installs a Trojan Horse, which is a malicious software that makes it possible for the attacker to take over the victim's workstation via remote access.

Again we see that the typical scheme: The victim is under pressure (he has to continue with his work as soon as possible, the attacker knows this and has picked him partly for exact that reason) and the attacker has to ensure that the victim believes him to be who he claims to be (we have already seen how he manages to do that).

Because of the pressure he is under, the victim is glad to have someone with a quick solution for his problem at hand, so he asks not too many questions about what is really going on as long as he can continue with his work afterwards.

6.3 Name-dropping

In order to succeed with their attack it is essential for Social Engineers to know who they have to talk to, to get anywhere and the general "chain of command" within the institution they plan to attack.

As we have already seen in the previous two methods of Social Engineering, an attacker likes to put his victim under pressure to assure that he cooperates without thinking too much about Security aspects. This pressure can be achieved in various ways, one of them is called "Name-dropping".

Remember the example in 6.1.1, where the guy from George's department said he had to get some systems up and running again before a meeting with the CEO and the victim's boss ended (of course, depending on the importance of it, such an event should, at least to a certain point of truth, really take place and not be some invention since then it would be too easy for someone to recognize this as an attack and take countermeasures). Hearing that certainly put the victim under pressure because he did not want to be the black sheep whose fault it was that something did not work as it should have. So he chose better to cooperate with the attacker, who knew pretty well about the pressure he puts the victim under, after all he knew how to create it.

Name-dropping should not be mistaken with something like "... and if you do not do as I say, I'll tell Mr. VIP". That would fall under the use of authority and threats (which will be the topic of the next subchapter), name-dropping is more subtle than that. As the name implies, it is more about "dropping" important names within a conversation to make the victim *realize for himself* the consequences of non-cooperation with the attacker's request. Therefore, so far there is no need for a Social Engineer to make any direct threats, although this does not mean that he does not do so later, if he deems it necessary to make the victim pliable.

The name-dropping example of the above could for example be "... and I also talked to Mr. VIP about this, he said it was a brilliant idea and should be among the top priorities for the next week". There is no threat in that, just a small hint that Mr. VIP (who could be the victim's boss or some other person with authority) thinks very positive about the attacker's idea... and who wants to argue with Mr. VIP about something that he considers a top priority? Certainly not the victim who maybe is a newbie anyway (and therefore the perfect victim for a Social Engineer, see Chapter 7) and not willing to get into any kind of trouble in his first days within the company.

Additionally, people have the tendency to comply to requests when doing so appears to be in line with what others (not even necessarily people with an authority) think or do. Social Engineers know that, so they will be eager to give a victim that exact feeling, that doing something is ok to do just because someone else the victim trusts has done it as well or has agreed to it.

Name-dropping also works if the general success of an operation depends on one person (let us again call him Mr. VIP) and this person is used to put a victim under pressure. Imagine for example that some important documents are requested by the attacker who claims to be somebody else within the group working on a specific task. As usual, the deadlines press on the people, so when the attacker requests the documents, saying that he has to review them before they to go to Mr. VIP, the victim has to imagine what happens if he does not cooperate – the working process gets stuck, just because of him. The whole group may not be able to finish this week's tasks in time, people will have to work overtime, maybe even during the nights and so on.

Although within a good project management the possibility of such a case should be eliminated, there can always be found situations like this, where everything depends on one person and that he gets the information as quickly as possible (especially when time presses).

So, again, the victim asks himself – “Do I want to be the one who is called responsible if we cannot finish within time and have to work overtime? Just because of some formalities? Certainly not. I am sure everything is fine with this request, after all that guy knows what he is talking about and he is also a colleague of Mr. VIP...”.

The Social Engineer knows how to seemingly create a scenario of pressure and take over the role of someone probably in the need to talk to the victim about it (in this case a colleague of Mr. VIP).

6.4 The use of authority, threats

If name-dropping does not have the desired effect on a victim, a Social Engineer might increase pressure by directly reminding the victim of the authority of the person he names or even claims to be himself, and of the consequences of non-cooperation with his request. With the example from the previous chapter it should not be difficult to imagine that.

The use of authority and threats are just more direct ways of name-dropping, one could call it the “hardliner’s way”. A Social Engineer will usually try to leave this to the last because there are not many things for him left to do if even this fails. It includes reminding the victim of the consequences of non-cooperation with the attackers request, for himself and for others, as we have already seen before, but in a more direct way of saying.

Imagine the same situation as before, where an attacker wants a victim to send over some documents for a review for Mr. VIP and the victim rejects that request because of Security concerns.

The attacker’s reply to that could be “Ok, if you say so, that’s fine with me. If Mr. VIP asks tomorrow, why the documents are not on his desk, I’ll just tell him that I could not get them ready in time because you would not send them to me.” – There is no need to say more because with that the victim already got the message and, knowing the status of Mr. VIP, realizes the consequences of his non-cooperation (for himself, or worse, the whole department). If he still goes through with not handing over the information, than the attacker has to live with that and look out for other ways to obtain the documents – or give up. But all too many people (especially those picked out as victims by a Social Engineer, see Chapter 7 for characteristics of such people) will, when put under such a pressure, cooperate, afraid of the consequences and of looking bad in the eyes of their colleagues, not thinking of the consequences if valuable information gets into the wrong hands (here again, we are at the point of making people realize the value of the information they handle).

6.5 Reverse Social Engineering

Reverse Social Engineering is very similar to what we have already seen in subchapter 6.2, the topic of "Offering help".

What is different, however, is, that the victim is not contacted by the attacker in the first place, but the other way round, which creates more credibility for the role the attacker is playing. This may be because the attacker creates a problem and sets himself up as the person who should be called in a situation like this.

Or the attacker takes on the answering call to a request call that has originally been made by someone else, a legitimate colleague, for example by redirecting it to his own phone.

The general idea behind this method is that the victim talks to a Social Engineer believing all the time that he is talking to the right person he is supposed to inform about the kind of problem he has, without having been contacted first by the attacker.

The Social Engineer will then answer this call like he knows exactly what to do and instructs the victim into doing something, again for example like installing some malicious software or something alike. With the right lingo and knowledge about what he is talking about, it should not be difficult for a good Social Engineer to appear trustable to his victim.

Looking for an example we can take a look at an incident which has occurred in Austria in autumn 2004. A group of Social Engineers placed forged ATM machines in front of original ones so that some people inserted their ATM cards into the forged ones. The machines, however, did nothing then, not even return the inserted cards, which made people call a helpline that was available there. The person answering these calls spoke like a banker and offered those people help with their problem, asking them for their account number and the ATM pin number.

Those people never knew that this person was actually not a banker, but a Social Engineer who had quite an easy task talking people out of their ATM pin numbers. Not until they discovered that their bank accounts have been emptied and the case showed up in the media, too late for many of them.

But why did people do that, give away their ATM pin numbers over the phone? The answer is simple: Because the Social Engineers made their act look quite professional, from the forged ATM machines to the professional sounding, helpful banker on the fake helpline who was actually nothing more than a Social Engineer talking people out of sensitive information. They made people believe the scenario created for them, as do all successful Social Engineers.

In another case a Social Engineer posted flyers on a company's bulletin board with a "new number for help desk". Within a short time period he had collected an impressive number of passwords because employees called the number regularly to receive help, not knowing that they were actually talking to a Social Engineer, not the real help desk.

6.6 “Just asking for it”

Not many people would think of a Social Engineer just directly asking for the information he wants to know, getting right to the point – and getting away with it!

How is that possible? Of course a Social Engineer must present a good reason to request the information he requests, therefore, as always, he has to present a scenario credible enough for his victim to trust him to be someone who has a right to access that information.

Again we get to the point how an attacker gains so much trust from his victim. Look back to chapter 5, where we have talked about this. Setting up a credible scenario, putting himself into it as a poor (maybe overworked and stressed) guy and using the right lingo can be all that is necessary to ask a lot of questions, among them the few that are really what the whole attack is about.

However, this sounds easier as it might be. For such a direct method of Social Engineering an attacker must have much knowledge about what he is talking about as well as the proper lingo and much self-confidence, as he has to talk to his victim in a manner as if there was nothing in the world as normal as him just asking some questions within the scenario he has built.

Since such expert's knowledge can be hard to learn (if you have never had to do anything with it before), there are not many Social Engineers who dare to attack so directly unless they have, for example, worked before in that specific area and therefore do not have to worry about sounding like professionals to others who expect them to do so if they are to buy the act. Others, who do not have this expertise readily on-hand, will focus first on preparing their attack carefully before actually launching it.

6.7 Dangerous offerings over E-mail

Every day when we check our E-mails we find some in our Inbox with more or less resistible offerings including healthcare, money savings, access to pornographic or hacker content Websites.

Many people see these messages as the junk they really are, reminding themselves that “there is no such thing as a free meal”.

But there are also many where these messages and their offerings can catch the eye, even getting someone so far as to click on one of the links within those messages or open an attachment. This happens especially if the offering is something scarce (“get it before it's too late!”) or if an amount of people will be competing for it (“the first 500 to register will receive a free gift!”).

Links or Websites in such E-mails often lead to the download of an application, game, document or something similar. What these have in common, is that they contain malicious code (that is why they are called “Malware”) which, after downloading it, is then executed on the victim's computer, infecting it with a virus, installing a Trojan horse, a dialler or something similar.

The same goes for attachments which come via E-mail and have to be executed by the recipient.

Technically, these matters fall into the area of Network Security. Why it is mentioned here nevertheless, is because the methods used to attract people into downloading and executing Malware on their systems fall into the area of Social Engineering. What we have here is something that pretends to have a trusted source and offers us a good or a service in a manner that in reality plays us for a fool concerning the risks of such an application – which is a typical aspect of Social Engineering.

6.7.1 Persuasive E-mails

From the media people tend to know about Malware, names like “Love letter”, “Anna Kournikova” and others still ring a bell for many of us.

But what makes so many people believe, nevertheless, that the application they just got over E-mail or downloaded from a Website could not be one of those they have heard about, causing so much damage? Because the authors of such E-mails are clever and know how many people think about certain things.

Many of these dangerous E-mails have subjects that make them appear like replies to other E-mails, for example

“Re: Here is the sexy photo of me you asked for”

“Re: Free gift”

“Re: I got what you wanted, though it cost me much”

etc.

The receiver remembers that he has never written an E-mail to which such a reply would apply. But that doesn’t stop him from thinking that someone has sent this to him by mistake. He got it, so why not take a look at it, since the subject sounds so interesting...

Other E-mails have subjects which try to attract without appearing like a reply:

“Check out this cool hacker tool”

“Finally I got access to the XXX-portal, check it out”

“Free cable TV – It’s so easy!”

or simply *“I love you”* (which was the subject of one of the first E-mail Worms, the famous “Love letter”)

What the authors of these E-mails know, is that a persuasive offer makes people underestimate the risk of opening an attachment or downloading and executing software (if they are even aware of it).

So, from a Social Engineering point of view, the author of such E-mails successfully predicts how people will react on the subject of the E-mails he sends them.

6.7.2 E-mails from a trusted source

If an E-mail appears to come from a more or less trusted source, people are even more tempted to trust its content and open an attachment.

But sometimes even an offer coming via E-mail from a relatively trusted source, such as a personal friend or a known institution, can carry Malware as an attachment, for example a "Worm".

A Worm is a Virus which spreads by itself from an infected system, often naming as source the owner of this very system and therefore appearing to others as if coming from a (more or less) trusted source. After all, who would suspect a good friend of sending Malware to one of his friends, especially within a small program designed to wish "Merry Christmas"?

The friend never did that on purpose or even with his knowledge, but that is not known to the receiver. When opening the E-mail and the attachment, the receiver infects his own system as well, forwarding the Worm to all the people within the address-book of his E-mail client (because of its implementation within current Versions of Microsoft Windows, Microsoft's Outlook Express is often the target for malicious software of that kind) and infecting them as well, spreading the Worm.

For many people it is enough to know that they received an E-mail from a friend to trust its content. That this E-mail may have just been *forwarded* by this friend does not come into their minds (although they could easily see that when looking more closely at the E-mail, but many people do not think that far). Again we see the critical pattern of going along with what others deem right. We have already discussed this in Chapter 6.3.

The fact remains, that it is really totally unimportant that a *friend* sent such an E-mail, that could have been done by any unknown person in the Internet as well.

That friend might not have noticed that the E-mail carries malicious content and just passed it on to other people, therefore it would be wise not to trust too much into the Security precautions of other people, but better tighten ones own.

6.7.3 Forged E-mails

Besides Worms there are other possibilities to forge E-mails and make them look if they come from a trusted source.

Steal account information:

The first possibility to create a forged E-mail is to steal the account information of the account where one wants the E-mail to come from. After a legitimate login it is possible to send E-mails from that account as if being its rightful owner. These E-mails are, from the legitimate owner's point of few, forged, but in reality they are as legitimate as if they would have been sent by himself because they *really* come from his account.

Many Webmail-accounts show the time and date of the last login after a successful login, as well as any number of failed logins. Being attentive to these information can tell a rightful owner if his account is being misused by someone else.

If an account thief does, however, *not* use Webmail, but an E-mail client like Outlook, Thunderbird etc., it is, from the user's point of view, impossible to know if his account is being misused. Only the E-mail provider could tell that by checking Server logs.

Server-side scripts:

With some knowledge about setting up a Webserver and a server-side programming language (like PHP or Perl) it is possible to write a small script through which it is possible to send E-mails and set recipient, outgoing E-mail address and other parameters to any value desired.

There are some Websites which offer such a service for free on the Internet. All one has to do is enter the parameters into form fields, generating an E-mail which is sent to the recipient with the parameters that have been introduced before.

By this it is possible to send E-mails with an outgoing E-mail address such as "whoami@nomansland.com".

However, giving such an E-mail a closer look (at the E-mail header) can reveal where it has really come from (the header contains, among other things, information about the Mail server that the E-mail was sent from).

6.8 Phony Websites

Similar to E-mails telling their receivers to download Malware are phony Websites. Links to those Websites often come with E-mails as well, but can also be found within other Websites.

These fake Websites try to look like the original Website of the trustful source they pretend to be, their content might be dangerous to anyone who accesses them.

What makes these Websites look so authentic is that their creators often copy images and the design of the original Website. Sometimes these Websites even show the image signalling a secure, encrypted connection (commonly used Web browsers use the symbol of a closed lock for this).



Fig. 6.8a: Symbols signalling a secure connection in Firefox and Internet Explorer Web browsers

The symbol of the closed lock can be implemented into a phony Website simply by putting it as an Image into the down right corner, fooling users who do not know that the functionality of an encrypted connection is part of the Web browser program, not the Website displayed by it.



Fig. 6.8b: Symbol for a secure connection put onto a Website as an Image (Firefox Web browser)

These people believe then that they are surfing securely on the original Website when in fact they do not because what they see it nothing more than an image on a Website with no functionality behind it. This is very dangerous when the data handled are numbers of credit cards, bank accounts and the like.

6.8.1 How to get onto a phony Website

People who do not have much experience in surfing the Web can be fooled into visiting a phony Website without wanting to do so. This can happen by following a fake URL (unified resource locator, this is the direction to which a link goes to).

Taking a look at the URL of Paypal, an organisation for Electronic Payment over the Internet, we can see that the original URL is

`http://www.paypal.com`

A fake URL for this URL could be

`http://www.paypal.com`

When one sees the fake, clickable within an E-mail or on another Website, would he/she notice that the last "l" of "Paypal" has been replaced with a "1" instead, leading to a complete different Website? Hardly.

A not-so-clever approach that would work nevertheless on many people, would be the following URL:

`http://paypal.tripod.com`

Everyone who has surfed around on the web for some time will identify this URL as a fake since Tripod is a more or less well-known free Web space provider. "Paypal" in this case is nothing more than a name for that particular Web space account, it could also be "peters_place" for that matter. But you can be sure that there are still many people who do not know this and would actually believe that this URL really leads to the official Website of Paypal.

Tricks like these are often used on the Internet to catch attention for particular Websites, which would otherwise not be visited that often. Their creators make

use of the well-known name of another institution and the possible confusions with the domain name of the Website of this institution. This may be a foul trick, but it works pretty well, as experience has shown.

There are, however, more sophisticated ways to lead someone onto a Phony Website. Some versions of the Internet Explorer Webbrowser had a bug which allowed someone to manipulate the display of the string that shows the user on which Website he is currently surfing.

The browser was not capable to display a URL properly if it had the following form:

```
http://www.myurl.com%01@badguys.com/stealpassword.asp
```

When the URL contained the character @ with a non-displayable character right before it, the Internet Explorer displayed that part of the URL that came before that character, but linked to the part after the @ (in this case obviously a Web site with the intent to do harm to its visitors).

By placing enough characters for a tab into the URL

```
http://www.myurl.com%01%09%09%09%09%09@badguys.com/stealpassword.asp
```

it was even possible to hide a Web site from the Windows Taskbar.

Using these techniques (which are nowadays known as "Phising"), attackers were able to mislead people onto Phony Websites, and stealing their information, until Microsoft released patches that fixed these bugs. Still, Phishing and its popularity has become a serious problem, most notably for banks and their costumers.

Be aware that not all URL-based confusions are however intended. Sometimes a Website whose domain name is easily confused with another proclaims this fact to visitors, telling them that they may have landed there by accident and that the official Website of the institution has a different URL. Most of these "honest" Websites contain even a link to the original Website, so that somebody who accidentally accessed this Website can quickly continue to the original Website. But since this is more of a *service* to the people surfing the Internet, we try to concentrate more on the *intent* to mislead people to phony Websites, as that happens within the context of Social Engineering.

Now, after having an idea of how one could get onto such a phony Website, we need to examine how those can pose a threat to a person surfing on it.

6.8.2 Dangers coming from phony Websites

The reason why phony Websites are dangerous is exactly the same reason why a Social Engineer can be dangerous to us. Both use the same approach to extract sensitive information from us.

When a Social Engineer attacks a victim, he presents himself as someone who can be trusted concerning passing on confidential information. He looks, talks and acts in a way that lets his victim believe that he is really what he seems to be, someone to trust.

A phony Website does just the same. Created to look and act like the original Website, its goal is to give a victim enough assurance so that he has no concerns about typing in confidential information into forms if the Websites prompts him to do so.

Let us take a look at the following text of an E-mail:

msg: dear eBay User,

It has become very noticeable that another party has been corrupting your eBay account and has violated our User Agreement policy listed:

4. Bidding and Buying

You are obligated to complete the transaction with the seller if you purchase an item through one of our fixed price formats or are the highest bidder as described below. If your are the highest bidder at the end of an auction (meeting the applicable minimum bid or reserve requirements) and your bid is accepted by the seller, you are obligated to complete the transaction with the seller, or the transaction is prohibited by law or by this Agreement.

You receive this notice from eBay because it has come to our attention that your current eBay account has caused interruptions with other eBay members. Therefore eBay requires immediate verification for your account. Please verify your account or the account may become disabled.
Click Here To Verify Your Account – http://error_ebay.tripod.com

Designated trademarks and brands are the property of their respective owners. eBay and the eBay logo are trademarks of eBay Inc.

Fig. 6.8.2 A fake E-mail containing a link to a phony Website

This is a fake, but many eBay-users would actually fall for this and visit the link which would take them to a phony Website of the online auction company eBay. How to identify it as a fake?

1. The choosing of words is partially clumsy, no professional editor would have let this E-mail get passed to costumers the way you can see it above.
2. A company like eBay would never send out E-mails like these for the verification of user accounts.
3. The domain of the link leads not to eBay, but to Tripod, which is, as already mentioned in 6.8.1, a free Web space provider. "error_ebay" is nothing more than a name for that Web space.

What could have happened to people taking this E-mail seriously? They would have followed the link, entered the phony Website and typed in their account

information into some form field, when asked to do so. With the click of a button they would have gotten a message like "Verification successful, thank you very much for your cooperation" and probably would never have thought about the incident anymore (since everything would seem to be in order), unaware that they just sent their account information to a group of criminals.

7. Victims of Social Engineering

People react differently to Social Engineering methods. Some make better victims for Social Engineers, others not. The following chapter shows the characteristics of people that make them vulnerable for Social Engineering and explains, why that is so.

7.1 Typical characteristics of persons vulnerable to Social Engineering

Social Engineers make people do things that they would normally, under the given circumstances, not do. What they have to do when they attack somebody, is to affect their victim's behaviour in a manner suitable for their purpose.

Some people make it easier for Social Engineers to affect their behaviour, than others. This depends on the following characteristics of a victim's personality:

- Self-esteem
- The ability of logical thinking, even when put under pressure
- The rate of contentedness within the current situation (for example the job situation)
- An advisable rate of distrust for unknown people
- General naivety when it comes to unknown people

Social Engineers are normally excellent judges of character. This enables them to see very quick within seemingly harmless small talk or just by observing someone if this person will be "hard to crack" (meaning in this context how easily the Social Engineer can affect the victim's behaviour for his purpose) by Social Engineering, or not. Based on this judgement they choose their methods of attack, some more adequate for a specific victim than others (which leaves it very clear that a general statement about the most effective method of Social Engineering cannot be made, since this depends completely on the person at which the attack is directed at and on the context as a whole).

Social Engineers will generally look for people whom they can easily put under pressure, since then many people tend to act more or less in panic, forgetting precautions or not giving them enough importance to follow them, although they should definitely do so (not just under the circumstances, but in general).

7.2 Attractive positions for an attacker

After discussing the characteristics of potential victims of Social Engineering we can now identify some positions within companies which are particularly attractive for Social Engineering attacks.

Receptionist:

Being the first person anyone who enters the facility of a company talks to, the person in this position is of particular interest to a Social Engineer. It is a receptionist's job to know much about a company and the people who work there, he/she has also many possibilities for requesting information which might be of interest to a Social Engineer.

Additionally, a receptionist seldom knows very much about technical or Security matters or the value of information in general, but is nevertheless part of the company, so to direct the first attack at the receptionist is very often one of the first steps of a Social Engineering attack.

Department of human resources:

The department for human resources has all the information a Social Engineer might want concerning employees within a company. It therefore has great value to him as an information source, which makes it not unlikely that this department might get attacked sometime by the use of Social Engineering methods.

The employee information handled there includes:

- Current status (available, on vacation, ill, currently busy on an outside job etc.)
- Which department an employee belongs to
- Names of colleagues
- Position within the department
- Superior (this is particularly important for a Social Engineer to create pressure)
- Labour condition
- Contract & salary information
- Colleagues and Co-Workers
- ...

Think back to the example in Chapter 6.1.1. The attacker might never before have heard of any "George" in the department he claimed to be in, but after an attack at someone from human resources he might have gotten that information and could have used it as we have seen in the example, to gain the trust of a victim who would react upon hearing the familiar name.

Managers:

Managers often have great authority over other employees who control technical and organisational mechanisms within a company. Additionally, since their work field is more organisational, managers often lack enough technical background to see all the dangers of certain actions which may be part of an attack.

Both, but especially the authority over others makes it very attractive for a Social Engineer to direct an attack against a manager of a company. Taking over his role can prove very valuable since normally there are not many people within

a company who would question a manager's decisions if put under enough pressure.

"Newbies":

Employees just recently employed within a company (often called "Newbies") often face some problems in the first days with getting along in their new and unaccustomed surroundings. Because of that they are probably the most endangered group of employees in danger of being attacked by a Social Engineer.

Being new within a company, Newbies often try to do their job as best as they can and leaving no doubt about that. Being insecure, the last thing they want is raising just the slightest possibility of irritation of any kind. They are the last persons who would question the decision of someone with authority over them, after all who are *they* to question Mr. VIP (so they think)?

The effects of authority, threats, pressure etc. work best on Newbies. Social Engineers know that, therefore they favour directing their attacks at them.

Temps, freelancers:

Temporary employees (called "Temps") and freelancers within a company often have access to confidential resources in order to do their temporary jobs. But since they are not full parts of the company, they often lack knowledge about various organisational and Security aspects. This makes them vulnerable for Social Engineering attacks.

However, there is one big disadvantage for a Social Engineer trying to take over the role of a Temp or a freelancer. These people come and go and since they are not "full" employees, they generally do not get as much trust from other employees as do "real" colleagues, which makes it harder for Social Engineers to get access to resources which are not within an immediate reach of the person whose role they have taken over, if that person is a Temp or a freelancer.

Help desk:

Help desk employees are responsible for opening and disabling user accounts, sending and resetting the passwords for these accounts, installing software (employees should not be allowed to do that under normal circumstances, for Security reasons) and troubleshooting on these matters. Because of that they are extremely attractive to Social Engineers for directing an attack against them.

By deceiving a help desk employee an attacker might be able to get an existing user account closed in order to later call the account's owner and offer help (which is a typical Social Engineering method, as explained in Chapter 6.2).

Network Administration:

These are employees of the department responsible for a functioning network infrastructure. They can reconfigure Servers, routing tables, handle remote access requests etc.

This makes them attractive for a Social Engineer, for example if he is planning to cause a problem somewhere within the company to later offer help on the matter (as seen in Chapter 6.2).

Often the network administration department also handles Security issues. In this case a network administrator may have had training on the Social Engineering issue, but a company should take no chances on that and see to it that *every* employee, regardless of his position within a company, gets the proper education on this to be able to recognize an attack (see Chapter 9.2 for more details).

8. Who might be a Social Engineer?

Identifying a Social Engineer can be an extremely difficult task. However, there exist certain people who, besides the people who could be Hackers or Crackers, theoretically, would have a good chance of starting a Social Engineering attack on a company or person because of their past job experiences.

This does of course not mean that these persons automatically should be suspected of being Social Engineers, but it cannot hurt to know that they probably could be.

8.1 Persons

Former police detectives and police officers:

Police detectives and officers are trained to have characteristics which could make them potential Social Engineers. Many techniques in crime investigations also make use of Social Engineering, those people need to see behind the scenes in order to fulfil their duties.

Former private detectives:

Private detectives are often hired to find out exactly that kind of information also Social Engineers are looking for. Many of them are former police detectives, police officers or people who have otherwise gathered experience on the matter of finding out information that is not supposed to be found out using common methods.

Private detectives often walk on the edge of legality with their methods of obtaining information. That is, because these methods seldom are very different from those we have already seen above, used by Social Engineers.

Former employees:

Former employees are one of the most dangerous groups for companies concerning the matter of Social Engineering. Since they know the company, the people and the lingo, they know practically everything necessary to Social Engineer successfully on other people within the company.

Sometimes, when the end of their employment has only been recently and the company is big, they can make employees believe that they are still part of it (if the word has not spread that they do not work there any more) or even access resources which are still available to them although they are no longer part of the company.

As if that would not be enough, they often also have the necessary (technical) Know-How to put the information gathered by Social Engineering methods directly to use.

Insiders, disgruntled employees:

Disgruntled employees can be as dangerous as former employees, but they are even worse because they are still legally on the inside of the company. Therefore they can access much more resources than outsiders, but are still trusted among their colleagues because of their status.

They could exploit information resources for personal gain or sabotage computer systems for revenge. Sometimes they work as so called "moles", stealing company secrets and selling them to competitors or to start their own business.

Insider attacks are therefore considered the most dangerous of all, looking at Security in general. The damage caused by these is far greater than that caused by Hacker activities coming from the outside (which nevertheless appear more often in the media; Security incidents in general are tried to be kept secret as not to lose the trust of the public).

The problem with treacherous insiders is that everyone could be one. There has even been a case where a cleaning crew has been bribed by a competitive firm to copy blueprints of a technical device.

The most successful Russian spies during the cold war were cleaning ladies, "dumpster diving" through the garbage of American institutions, collecting useful information.

(Note: "Dumpster diving" means rummaging through other people's garbage, especially thrown-away papers, in hope to find some valuable information that has not been destroyed as it should have been. See Chapter 9.3.1 for details on this.).

Visitors:

Visitors in a company have to be treated in a careful way. In cases where groups of reporters have been invited to the facility of a company in some cases in the past one person among them was actually no reporter, but an industrial spy.

Therefore many companies do not allow any video or photo cameras during such visits, but also keep a very good look at their visitors which are never allowed to wander on their own through the company's facility. Some companies (such as NOKIA) even have visitors sign an agreement of nondisclosure before those are allowed to enter a facility. Although the visitors are allowed to ask questions during the visits, they all too often hear things like "Sorry, this information is confidential."

Knowing what a good Social Engineer is capable of, measures like these do not seem paranoid at all, but more a necessity.

8.2 How to identify a Social Engineer

It can be extremely hard to identify a Social Engineer for what he is. This is not only because Social Engineers may be as qualified in their art, as they have to be

to remain undetected, but also it is a very delicate matter to suspect someone of being a Social Engineer. Too quickly people are offended, even if they are questioned just because of standard Security procedures existent within a company.

Social Engineers know this very well and it is very important for them to give others the feeling that it would be rude if they are questioned, even on an absolutely questionable subject (that is why they like others to be in their dept before asking them for something).

Here are some points which could make it easier to identify someone trying to Social Engineer:

1. Social Engineers like to put their victims under pressure. This pressure can be created using various methods.
Sometimes Social Engineers act very kind and friendly to create a feeling of necessary gratitude within their victims, so that they can expect something from them in return for their kindness.

The pressure can also come by name-dropping (see Chapter 6.3) or from the use of authority or even by threats (as seen in Chapter 6.4).

2. Social Engineers like to do small talk and ask many questions. This is nothing but a camouflage because within these questions which give their victims the feeling that they know what they are talking about (it is a method to assure that the role taken over by a Social Engineer is believable to the victim), Social Engineers like to place a few critical ones, as if they were as harmless as all the others. The answers to these questions is what a Social Engineer has been looking for all along, so a victim should always consider exactly *what* has been asked, independent of what has been said or asked before or will be asked later and should not fear to question any request for information or an action to be taken.

Social Engineers try to make their victims forget about such concerns by chatting with them and appearing like friendly, likeable and completely unsuspecting persons.

3. When asking questions, Social Engineers like to give others the feeling that there is nothing unusual about them asking those questions, in order to appear as if they have a right to ask them and receive answers in return.
If others reject to that, Social Engineers use name-dropping, authority or threats to make victims pliable.

4. Social Engineers always create scenarios in which it is seemingly necessary to step down from standard procedures, especially concerning Security matters. They are very imaginative in that and should never be underestimated, for that is one thing they count on when they think about their attack strategy.

5. Social Engineers try to appear trustable to others. They do this by including information into a conversation which may be relatively irrelevant (not necessarily, but often, they often got those by Social

Engineering on someone else), but marks them as being people from the inside because others would not know about these.

Therefore it is essential not to be fooled just because someone knows for example the name of some other person within the company relevant on this matter or speaks with the proper lingo. Only "hard facts" have to count when the matter of accessing a critical resource is brought up during a conversation, with very little to none room for exceptions. Of course this depends on the context of the situation (for example it is nonsense to reject giving out a Security code if this is essential to save human lives when a fire broke out), but one has to know that Social Engineers, as said before, know how to create or simulate situations in which such exceptions *can* be found.

9. Defences against Social Engineering

Although it may be difficult to identify it when someone tries to social engineer, there are some precautions in order to defend companies and people against Social Engineering.

9.1 Technical measures

Social Engineering is a manner of attacking people *psychologically*. Nevertheless there are some technical precautions which can help defending people against such attacks.

It is important to understand that the following measures are directed against *Social Engineering* and as such only are *part* of a complete Security infrastructure.

Electronic employee directory:

Within big companies it is difficult to have an up-to-date overview over all the people who work in it. Usually only the department for human resources has an electronic directory for that reason, in which all the information concerning employees is stored.

However, some of the information should be made available to all the employees within a company, best through an online directory (embedded within an Intranet system) with the ability to search for names. This directory should contain employee profiles, not only with names, but also with photographs, phone- and mobile numbers, E-mail addresses and with the status of the employee within his department, so to verify if someone is really who he claims to be.

Also Temps, freelancers and such should be stored within such a directory (marked as being not "full" employees), as they are particular attractive victims for Social Engineering.

Regular updates of this directory are essential so that no profile remains there longer than necessary (this is especially important for the profiles of Temps). If a profile remained there even just a few days after an employee has left the company, this could be exploited by a Social Engineer because, using this profile, he could appear to many as an insider who in reality has already left the company.

Of course such a directory is extremely valuable to a Social Engineer, since it contains lots of information about potential victims. Precautions need to be made to prevent that from happening, best through training so that no one accesses the directory on request of a Social Engineer.

Digitally signed E-mails:

As seen in Chapter 6.8.2, some attackers try to make E-mails appear like they come from a trusted source. In order to prevent this, it is wise to use digital signatures, their easy-to-use functionality embedded within installed E-mail clients. Using digital signatures, receivers can verify that the E-mail they just received is really from a trusted source.

In order to fake such a signature an attacker would have to steal the private key of that source, which is harder to accomplish (although not impossible, as a good Social Engineer would look for ways to get his hands onto another person's public key).

Caller ID's:

Social Engineering very often is done over the phone. An attacker tries to take over the role of somebody else, claiming on the phone that he is actually that very person.

This can be prevented through the usage of caller ID's within the telephone system of a company. If installed, the name and number of the person who calls is shown on a display, so when this person calls he/she can be identified. It is nearly impossible for someone to call and claim something else than what is on the display (at least when the call is coming from within the company's telephone system). With help of the online employee directory, it is then possible to verify if a caller is really who he claims to be.

Of course this is no solution for legal calls that come from the outside, for example from a mobile phone. In this case only the number is shown on the display, letting the person picking up the call verify the caller by this meaning. This is not as secure as verifying a call from the inside (since the name does not show up on the display), but the mobile number can be verified quickly using the online employee directory (where it has to be listed), which should be sufficient.

However, calls from or to a mobile phone should be handled with extreme care. Sometimes Social Engineers like to pose as employees outside of the facility and therefore in need to be called back on their mobile phone. Before doing so, the number of that mobile phone should always be verified first. If this cannot be done, then even more caution is necessary dealing with the person on the other end of the line. It could be a Social Engineer.

When called from a number that cannot be verified, it is usually a good idea to call the person back on a number that *can* be verified because it is listed within the employee directory. Although it is theoretically possible to alter the telephone switch of a company to forward a call to an external, unlisted number, this requires not only access to that switch, but also technical Know-How as how to reprogram it. This is therefore unlikely.

Password rules:

People should use strong passwords which should not be easy to guess for an attacker. However, still many people use their mother's, daughter's or pet's

name as a password, which of course can be fatal because such information can easily be found out by a Social Engineer.

Besides the proper education concerning the use of strong passwords (see Chapter 9.2) the software responsible for the handling of passwords (for example the operating system) should contain rules about how a password has to look like and reject easy-to-guess passwords once typed in by an employee during the process of password changing (which should regularly take place to enhance Security).

Furthermore, every time a password is changed, a reminder should pop up, reminding the employee to never, under any circumstances, give away their password to someone else.

Employees should also not be able to choose the same password or one they have used at some time before, again.

Secure entrance to sensitive areas:

Company areas in which sensitive information is handled should have special secured entrance doors through which only one person at once can pass. Additionally this person must identify itself first, either to a Security guard or by use of a smartcard.

This is necessary, as Social Engineers have tried in the past to appear as employees from a transport company with a big and heavy box they carried in their hands. They asked an employee who just came by if he could hold open the (Security) door and helping them carry the box inside. By this manner they got inside the sensitive area without having to identify themselves. This technique is called "piggybacking".

For that reason it is good to not only check identities electronically, but also have a Security guard standing by who would notice such an attempt and would interfere. If a company cannot afford this, it should at least install a camera observing everyone who passes through a Security door.

E-mail filters:

The Mail server of a company can be configured in a way that E-mails with suspicious attachments (for example executable files) are not delivered. This way the responsibility of probably fatal decision-making is assigned from the receiver to the Mail server which is immune to Social Engineering (but not its operator!).

9.2 Education & Training

The far most important part in the defence against Social Engineering is the education of people concerning these matters. Many people have never heard of Social Engineering. These people need to develop an understanding for what Social Engineering is about, that the threat coming from it is real, why every kind

of information is valuable and how to protect themselves from psychological attacks of these kinds.

9.2.1 Awareness training design

The best way to teach people how to properly react when confronted with a Social Engineering attack is through training. This should take place regularly (at least once in a year), additionally every new employee, Temp or freelancer should attend to a special training before he starts working. This does not exclude secretaries, Security guards, cleaning personnel – everyone within a company should have to pass through that training.

Here we already face the first problem: How to train people on something every year without boring them with always the same material? It is on the designer of the training program to see that this does not happen.

This is a challenging task, if it fails, people will lose interest in the subject, ignore the rules because they see no necessity for them, meaning that Social Engineers will be able to exploit the holes in the Security net created by this.

Distinct training programs should exist for the following groups:

- Managers
- IT personnel
- Computer users
- Nontechnical personnel
- Administrative assistants
- Receptionists
- Security Guards
- Cleaning crew members

When an employee changes his position within a company (for example because of a promotion), it is required that he gets trained again, tailored to his new responsibilities.

A training designer has to see that the trainees have enough possibilities to think about the things they have learned throughout the training. This means that especially during the first time of the training the priority lies more on getting people to remember a reasonable number of basic, but essential messages instead of stuffing them together in one room for 10 hours, leaving them numb with too much information afterwards. Later, when going into more details, the sessions should be longer.

A training designer should also consider the methods of education. People tend to shrink away from “pure” classroom sessions, so the training should not just consist of lectures, but also discussions, instruction videos, computer-based training, online courses and printed materials for later studies.

A company must not necessarily develop such a program design all by itself, there are a number of companies specialized on that kind of training.

These companies often offer testing of the Security awareness of an institution as well. By launching a penetration test on it and later analyzing what probably has

gone wrong, they can show how this could have been prevented and help with improving Security awareness within that institution. There exist even certificates on such training programs, this can give employees extra motivation.

9.2.2 The lack of interest in Security matters

One problem with such training is to make people realize that there is actually a necessity for it. This is sadly one of the biggest problems of Security in general. Many people think of Security as being something they are not interested in because most of the time it just stands in their way when it comes to completing their daily duties and it makes their life uncomfortable.

As uncomfortable as it may be sometimes, but nevertheless - Security is necessary, people have to realize that. Of course life could be much easier if we could just trust anybody, but this is an utopia, so people have to learn that not only computers may be attacked, but they themselves as well and in ways that are hardly imaginable without having been confronted with the subject of Social Engineering by proper education. They have to know about the methods used by Social Engineers in order to identify an attack when it is directed against them.

When hearing about examples of Social Engineering, many people think "Such a thing could never happen to me, who would fall for these cheap tricks anyway?". Thinking like that is actually very naive, Social Engineers know as well as Security experts what people generally tend to think about Security. This plays to their advantage, which is exactly why people have to change their way of thinking about these matters.

This can be achieved by awareness training. Once people understand what Social Engineering is about and see the danger they are in while they just go along with their jobs, they will accept training as part of protecting what they are all working for. They will acknowledge that within a company it falls into *everyone's* responsibility to do so (be it a top manager or a member of the cleaning crew). The Security conscience has to be within each individual, not just a specified department (which is a common mistake made by people, thinking that *they* have no real responsibility because it is the Security Department's job to look after these things – the Security Department can hardly defend individuals against Social Engineering, only the individuals themselves can). The importance of Security throughout the company and the consequences of its failure have to be known to the trainees in order for them to understand why it is important to comply with it, rather than treating Security as an obstacle that has to be circumvented.

Getting to that point is the result of a process of understanding what is at stake. It is a challenge for the coach of the training to reach that point as quickly as possible, for all following training sessions after that will be rewarded with better attention by the trainees.

However, just understanding the necessity is not enough. The awareness training should also interest and encourage people to think *further*, for themselves, about this issue, for the field of Social Engineering is dynamic, where static rules alone, even if followed, cannot offer sufficient protection. The more they do that, the smaller will be the chances of success for a Social Engineering attack.

9.2.3 Consistence of the awareness training

Security policy:

Training is based on the Security policy of the company (as will be explained in chapter 9.3.1). These guidelines have to be among the first things trainees have to understand, in order to follow them. The problem with these static guidelines is that it is difficult to predict all situations in which people may be constrained to revert to them. Throughout the awareness training people have to develop their own awareness, based on the principles of the Security policy, in order to be ready for the dynamic situations they might find themselves in someday.

What has to be protected?

Among the first things a trainee must understand is *what* it is he has to protect. In other words – he has to understand the value of information (as described in Chapter 2).

Who is the enemy and how does he attack?

After understanding what they have to protect, it is important for them to know who the enemy, a Social Engineer, is and how he will appear to them (friendly, likeable, trustable etc., see Chapter 5), hoping to deceive them into trusting him and revealing information to him.

Next they need to know how they will probably be attacked. People have to realize their own human nature with all its weaknesses and that Social Engineers know about these as well, probably even better than people do themselves because they have studied them. They need to know about Social Engineering methods (see Chapter 6) and that there is simply no 100% safety from them, for no one, not even experts on that matter. Why? Because we are all human.

Role-playing discussions can help to show this.

Verifications:

Social Engineers try to let their victims believe that they are someone who is authorized to access sensitive information or to give the victim instructions into taking certain actions (revealing some information, typing commands into a computer etc.).

Trainees have to know that whatever happens, they always have to ask themselves 3 questions:

1. Is the person making the request really who he claims to be?
2. Is the person currently employed within or does it share a need-to-know relationship with the company?

3. Is that person authorized to access the information requested or call for a requested action?

Only after the positive verification of these questions should access to data be considered. If there is even the slightest doubt concerning those 3 questions, trainees should *always* either call their department supervisor or the Security Department, where specialists on these matters can deal with the matter accordingly.

Any kind of information, may it be verbal, a document, an E-mail, a file or a disk containing data has to pass these verifications or must otherwise not be transmitted.

It is important not to make any exceptions here, even if a top-manager, "Mr. VIP" himself is the one making a request. Many people would fear questioning someone with an authority such as this, but one should never forget that a Social Engineer knows exactly about this fear and will try to exploit it to his advantage if given a chance.

If the people with authority have understood the value of these Security precautions, there should really be no need for fear of appearing rude if questioning someone with authority before granting access to sensitive information. On the contrary, these people will probably be glad to see first-hand that the training in which the company has spent a lot of money actually works.

Ongoing awareness:

Although training sessions should be repeated on a regular basis, this is not enough. People tend to lose the feeling for something when not confronted with it over a longer time period. Since the protection against Social Engineering is of such a great importance, this cannot be allowed.

Here, again, a good design for ongoing awareness training is essential. On one hand people have to be reminded of essential Security issues, on the other hand these reminders must neither be annoying nor give them the feeling of being tutored. What must remain is the feeling that the Security measures taken by the company are necessary and have to be followed (with the possibility for making suggestions to the responsible department on how to improve them).

Here are some examples of what could help to insure ongoing awareness among employees:

- Including Security relevant articles and material in the company newsletter as well as the Intranet (including cartoons etc. so that people are attracted to read them)
- Making a competition for the "Security Employee of the month" for people with new ideas for improving company Security or people who found possible weaknesses within currently implemented Security measures. Proposals can be made to the Security Department.

- Providing extra information on Security issues for interested employees and reminding all employees of the possibility to obtain this information by E-mail and posters hanging in employee areas.
- Using Security-related screensavers.
- Placing phony stickers on the telephones, saying something like "Is your caller really who he claims to be?"
- Configuring E-mail clients so that by default they send encrypted E-mails; a warning should appear in case an unencrypted E-mail is to be sent, informing the user about the risks.
- Including Security awareness as a standard item on employee performance reports and annual department and company reviews
- Offer gimmicks such as free fortune cookies that contain a small Security reminder instead of a fortune.

While designing the ongoing awareness program, a designer has to keep one thing in mind and pass it on to the people that are trained: The threat is constant. So must be the awareness of the employees.

Reward program:

It is a fact that the chance of winning a reward makes people work harder on a subject. Awareness training designers can make use of that, since Security matters are no exception.

We already mentioned putting up a competition for "Security employee of the month". Additionally it should be made public if a person successfully detected or prevented a Social Engineering attack.

On the other hand, employees must also be aware of the consequences of failing to abide to the Security policies. Though making mistakes marks us as being human, repeated violations of Security procedures must not be tolerated within a company as they pose an unacceptable threat to all the persons involved.

Strong passwords:

This is one of the most important issues of Security in general. Training must include education on the choosing of a strong, hard-to-guess (even for a computer) password.

There are a few basic rules:

1. Passwords should not be anything related to the password's owner (like the pet's name, which is a very popular password), so that it may not be guessed.
2. Passwords should have a minimum length of 8 characters
3. Passwords should not be words that can be found in any dictionary (there exist dictionary-attacks where programs try to crack passwords by going through dictionary files)

4. Passwords should not just consist of letters, but also of numbers and special characters (at least one of each).
Some people argue that it is difficult to memorize anything else than "mary1" or "maryXXXX" where the last 4 X stand for the year of one's birthday. But there are tricks to get a secure password containing numbers that still can be remembered easily.

Some letters look similar to numbers, so, in a password, they can be replaced by them.

- 1 looks like l
- 0 looks like O
- \$ and 5 look like S
- 8 looks like B
- 3 looks like a mirrored E

Then there are words that sound like a number or a single character, so we can use that instead of the word.

- 4 sounds like "for"
- 2 sounds like "to" or "too"
- b sounds like "be"
- u sounds like "you"

Using these tricks it is not hard to find a relatively secure password which can still be memorized.

Examples: j0hn1ik3\$app135 -> can be memorized as "john likes apples"
ub2\$w33t4m3 -> can be memorized as "you be too sweet for me"

Of course this still does not offer protection against a brute-force attack, but dictionary attacks should have a hard time cracking a password that follows these simple rules.

5. However, even the best password is not secure if we do not keep it for ourselves. We have already seen that setting up a phony Website is one manner to obtain a password from an unsuspecting victim. Therefore, one should never use the same password within a company as used on a Website in the Internet, for this Website could have been a phony Website set up by a Social Engineer to retrieve a password, hoping that it might be the same that is used within the company. And since many people only have a couple of passwords and change only among those, a Social Engineer betting on this might just get lucky.
6. Passwords should not be reused within the same eight-month period. If an attacker discovers that an employee is using the same passwords over and over again (probably even in a cycle), it will be easy for him to get access to all the password-protected resources these passwords grant access to.

7. Writing down a password should be strictly prohibited, especially within the company building itself, the risk that someone discovers the note is too big. If a password *has* to be written down, the note should be destroyed as soon as possible or stored in a safe place (some administrator passwords are stored in envelopes within safes).
8. Devices like routers have default passwords which must be changed before using it (this is very often forgotten by the responsible administrator). On the Internet there exist lists of default passwords for various devices, so not changing a default password for a device makes it very easy for any hacker to gain access, either by knowing the default password of a specific device or running a dictionary-attack against it, where the dictionary contains of default passwords.

9.3 Organisational & Managerial measures

The company's management has to decide on the creation of Security policies and training programs. Should those be developed within the company's Security department or should this task be outsourced?

Developing the policies and training programs within the company has the advantage that the responsible persons, being the developers, have the best knowledge about them. Additionally a company may not want to outsource this particular delicate issue to another company in fear that a Social Engineering attack might come from there one day, by a person who then knows the policies inside out.

On the other hand, a company that is specialized on these matters (developing Security policies and awareness training programs) has great Know-How and experience, so, if affordable, it should probably be charged with this matter.

Either way, the management has to name responsible persons for the creation of policies and the ongoing awareness program. How many depends on the size of the company, but there should be at least two persons within the Security Department who have had special training on the matter of Social Engineering. This is necessary, not only for keeping up the training programs, but also to have someone to call immediately in case of a possible Social Engineering attack. Depending on if the company has authorized another company to care of its Security policies and training programs, there may be other persons as well, acting as advisors in times of trouble.

9.3.1 Security policies

Security policies are static guidelines on which all Security trainings within a company are based on. Every employee attending to such training must have understood these policies and must sign an agreement to affirm that he has done so and will not violate them. Additionally employees must be aware of the consequences if they fail that agreement.

The following shall help to get an idea of what policies concerning with the matter of Social Engineering should contain. It is, however, not strictly focused just on preventing Social Engineering attacks, but also deal with associated, more general Security issues.

However, these recommendations should definitely *not* be taken as a guide for setting up a *complete* Security policy since its focus is clearly on the topic of this paper, the defence against Social Engineering attacks. A complete guide would contain much more about technical and organisational aspects within policies, but this would go beyond the scope of this paper.

Risk assessment:

Before starting with the creation of Security guidelines, three things should be determined first:

1. What information needs to be protected (although we already know that generally *all* information should at least be handled with appropriate care) and with what priority?
2. What specific threats exist against these assets?
3. What amount of damage would it cause to the company if these potential threats were to materialize?

The trade-off between Security and availability:

Security measures generally exist in a trade-off between security and availability. The ultimate goal is to have relatively good Security precautions which do not hinder company processes too much within their execution.

Improving Security precautions would enhance security, but on the other side this would not be worth the obstruction of some business processes within the company.

Decreasing Security precautions would enhance the execution of business processes, but not in an amount that would make it a good trade-off compared to the higher risks for the whole company.

Support, right from the top:

Security policies have to be strongly supported by the management of a company. This must be known throughout the company as the management acts as a role-model for employees.

Starting right from the top, all people within a company have to demonstrate that they have understood the importance of following the policies and how that is essential for the success of the whole company. This will encourage other employees to follow the policies as well.

One must only imagine the consequences for a company in which not even senior managers hold on to the policies – everyone else will ask themselves “Well, if *they* do not see any sense in it, why should I?” - with a devastating effect for the Security of the company.

Readability:

The author of the Security policies must see to it that these are kept free of technical jargon so that they can be readily understood by nontechnical employees. It is also important that every document makes its importance clear and why it therefore must be followed. Otherwise some employees may regard it as a waste of time.

Policies and security procedures:

Policies and Security procedures should be recorded on different documents since policies tend not to be changed as often as the Security procedures based upon them.

Decrease human decision-making:

The author of a policy against Social Engineering should be aware of technical-based possibilities to decrease human decision-making and leave it to machines, where this makes sense.

An example would be the choosing of a strong password which is a feature embedded within most operating systems and just has to be configured appropriately. Another would be the configuration of a Mail server that rejects E-mails with suspicious content.

Update process:

As business changes, new Security technologies are developed and new threats come up, it becomes clear that Security policies cannot be carved into stone. Therefore it is necessary to regularly review them and present updates embedded in a business process.

People have to be informed about updates over the Intranet, an updated version of the policies should additionally be made available in printed form in each department.

Testing:

Penetration tests and vulnerability assessments using Social Engineering methods should be conducted periodical to expose any weaknesses within Security awareness or infrastructure and find countermeasures, should any be discovered.

However, decision-making employees should be put on notice before such tests actually take place in order to avoid unwanted stress or panic reactions.

Data classification:

By now the importance about the knowledge of the value of information among employees should be fully comprehensible. However, we need to go a step further to protect that information by using data classification.

Data that should be protected has to be classified into various levels of sensitivity to classify its appropriate level of protection. Each level has its own policy concerning access to data classified with it.

One may ask if this is really necessary and if it would not be enough just to educate people on the value of information. The answer is no. Knowing that every bit of information is valuable may be good, but the question about which level of sensitivity a specific part of information has, should not be left in the hands of individuals with probably very different opinions on what is important information and what is not. Clear classifications make it easier to protect information from finding its way into the wrong hands because some individuals have different, *personal* views concerning the sensitivity of it.

The classification categories shown in the following table should satisfy the needs for data classification within a medium-to-large company.

Category	Description	Examples
<i>Confidential</i>	<p>Information within this category is of the most sensitive nature. Confidential information is intended for use only within the company. Only a selected number of persons with the absolute need to know should have knowledge about it.</p> <p>If such information falls into the wrong hands, this can have serious impact on the company, its shareholders, business partners and costumers.</p> <p><u>Distribution:</u> In person, outside the company by a reputable delivery service (UPS, FedEx), within an encrypted E-mail, by phone or fax (only if can be assured that the designated person can receive it immediately)</p>	<ul style="list-style-type: none">- Trade secrets, proprietary source code, technical or product specifications that could be of interest to competitors- Marketing and financial information not available for the public- Any other information vital to the operation of the company (such as future business strategies)

<i>Private</i>	<p>Information within this category is of private nature and should only be distributed within the company, but with great care and only to people who really have a need for it.</p> <p>It could have serious impact on the company's employees if this information fell into the wrong hands (especially those of a Social Engineer), even within a company.</p> <p><u>Distribution:</u> Same as confidential information, but E-mail does not necessarily have to be encrypted.</p>	<ul style="list-style-type: none"> - Employee medical history - Health benefits - Bank account information - Salary history - Any other personal-identifying information that is not publicly available
<i>Internal/Sensitive</i>	<p>Information within this category can freely be distributed within the company. Unauthorized disclosure of internal information is not expected to cause serious harm to the company.</p> <p>Beware, however, of Social Engineers, since they can use <i>any</i> kind of information in attempts to deceive other people into providing them with more sensitive information.</p> <p>Before handing out internal information to third party members (for example employees of vendor companies) a confidentiality agreement has to be signed.</p> <p><u>Distribution:</u> Same as confidential information, but E-mail does not necessarily have to be encrypted unless the information goes to a destination outside of the company.</p>	<ul style="list-style-type: none"> - Corporate organizational charts - Network dialup numbers - Internal system names - Remote access procedures - Other information about daily business activities that should not be released to outsiders
<i>Public</i>	<p>Information that is specifically designed to go to the public. It can be distributed freely to anyone.</p>	<ul style="list-style-type: none"> - Press releases - Customer-support contact information - Product brochures

Any company information not falling into one of these categories should be treated as *Internal/Sensitive*.

Security badges:

Every person working within a company has to visibly wear a Security badge with his name, department and photograph on it.

Badges for different groups of persons should have different colours so that even from far away a person can be identified as to what group he belongs.

Persons who do not wear a badge or who do not wear it visibly should be questioned immediately. This should not be considered rude, but the correct procedure for such a situation.

Garbage:

Social Engineers sometimes use a method named "dumpster diving" to get hold of information. By this we mean that an attacker rummages through a company's garbage, hoping to find some sensitive information that a careless employee has thrown away without thinking what this information could do in the wrong hands. This is perfectly legal if it takes place on public ground.

Very often this hope is rewarded, so documents, disk media containing information have to be destroyed beyond reconstruction when they are not needed anymore.

Paper documents have to be shredded (each department should have a paper shredder for that reason), disk media should be collected within a secure, non-public area and later be transported for their ultimate destruction.

Review of access rights upon change of position or responsibility:

Each kind of position has its own responsibilities and access rights. When those are changed, access rights have to change as well. Generally the "rule of least privilege" has to apply.

Therefore no more rights are granted to a certain position than those that are absolutely necessary for doing the job. If additional rights are needed, those have to be requested, applying to a policy for such requests.

This also includes the deactivation of user accounts of employees that do not work any longer for the company. This must happen as soon as an employee has finished his work or else someone (probably even the ex-employee himself) might be able to exploit this account and get access to sensitive information through it.

10. Conclusion

The reason why Social Engineering is so successful is because there are still many people who would not believe what a good Social Engineer is capable of.

Social Engineering is a method of attacking a company that has to be taken seriously because this kind of attack is not directed against machines as are "regular" Hacker attacks, but on the employees who operate with them. In all-too-human behaviour, which a Social Engineer can predict more or less, observing his victim while talking to it as if nothing particular was happening, these people tend to underestimate the danger coming from a person just asking some seemingly unsuspecting questions during a small conversation.

They would never suspect this very person of being capable to actually use something they considered absolutely harmless information to launch a serious attack against their company.

The job of a Security Administrator is a hard one within many companies. Still too less people know about the importance of Security and see it just as being something uncomfortable which usually has to be circumvented to get along with the everyday business. This is a problem of Security in general, but with Social Engineering, which is a relevant part of the whole Security issue, it is even worse. Not only do many people not yet understand what they have to be protected against when confronted with this subject, many of them underestimate the threat and wonder about the people falling for the "cheap tricks" of Social Engineers.

But these "cheap tricksters" are cunning. By fooling others, telling lies, appearing harmless and friendly, but creating pressure through dropping some names within a conversation they managed more than once in the past to get access to resources to which they would have never been allowed in, using other approaches. This should make many people wonder if Social Engineers should not be taken as the serious threat that they really are.

What society lacks on this matter is education. Properly designed and implemented training can change the way people think about Security and Social Engineering, which is a very important, but not technical sub-area of Security. It should be accordingly acknowledged.

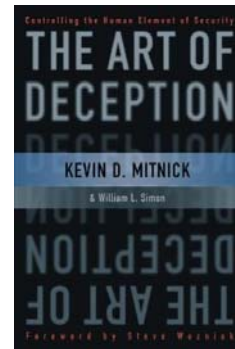
Because if we wish to defend ourselves against an enemy, we have to learn about and acknowledge *all* the methods brought up by him to do us harm.

Especially if one of them is so successfully practiced as Social Engineering.

11. Sources

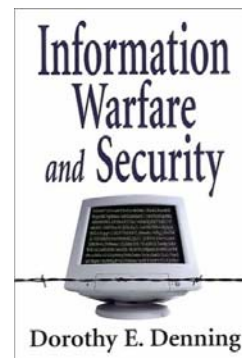
Kevin D. Mitnick,
William L. Simon

The Art of Deception
(ISBN 0-7645-4280-X)



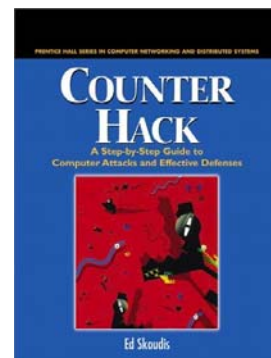
Dorothy E. Denning

Information Warfare and Security
(ISBN 0-201-43303-6)



Ed Skoudis

Counter Hack
(ISBN 0130332739)



Stuart McClure, Joel
Scambray, George Kurtz

*Hacking Exposed
Network Security Secrets
and Solutions*
(ISBN 0072260815)

