



FAKULTÄT FÜR **INFORMATIK**

# Trainings concept to prevent Social Engineering attacks in the context of Cyber Crime

MAGISTERARBEIT

zur Erlangung des akademischen Grades

**Magister**

im Rahmen des Studiums

**Informatikmanagement**

eingereicht von

**Ing. Ernst Hönig MSc BSc**

Matrikelnummer 0828394

an der

Fakultät für Informatik der Technischen Universität Wien

Betreuer: Ao. Univ.Prof. DI. Dr.Dr.Dr. Frank Rattay

Wien, 11.01.2010

\_\_\_\_\_  
(Unterschrift Verfasser/in)

\_\_\_\_\_  
(Unterschrift Betreuer/in)

## **Acknowledgment**

My honest gratitude is with my supervisor, Prof. Frank Rattay who gave me the chance to write this Master Thesis.

Further I thank Mr. Stephen Melnick, who was my proof reader.

I thank my wife and my two daughters who helped me in their own ways.

## **Eidesstattliche Erklärung**

Ernst Hoenig, 2512 Tribuswinkel

„Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.“

Wien, 11. Jänner 2010, \_\_\_\_\_

## **Kurzfassung**

Informations Technologie ist ein integraler Bestandteil in unserer Gesellschaft. Mit dem Aufkommen der neuen Technologie, im speziellen dem Internet, kommt auch eine neue Art von Kriminalität. Diese wird auch als „Cyber Crime“ bezeichnet. In einer bestimmten Art von Cyber Crime spielt das erfolgreiche Manipulieren, bzw. das "Social Engineering" eine wichtige Rolle.

Um nun solche Social Engineering Angriffe abzuwehren, enthält diese Magisterarbeit ein universelles Schulungskonzept. Dieses Schulungskonzept basiert auf drei Hauptsäulen: Der Analyse von psychologischen Faktoren, den Cyber Crime Aspekten und der Analyse der Didaktik.

Im Kapitel um die Cyber Crime Aspekte wird die Notwendigkeit eines solchen Schulungskonzeptes verdeutlicht, weiters werden aktuelle Statistiken präsentiert, welche die Dimension des Problems zeigen. Unter dem Kapitel der Analyse der psychologischen Faktoren werden sogenannte Duale Informationsprozess Modelle verwendet, um die geistigen Abläufe darzustellen, welche bei einer Manipulation beteiligt sind. Weiters werden in diesem Punkt konkrete Beispiele gebracht, die zeigen wie die verschiedenen Manipulationstechniken im Cyber Crime Kontext Verwendung finden. Im Teil der Analyse der Didaktik, wird die Sinnhaftigkeit des Instructional System Design (ISD), bzw. Analysis, Design, Development, Implementation and Evaluation (ADDIE) als Ansatz zur Schulungskonzeptentwicklung diskutiert.

Die Ergebnisse aller drei Analysen münden in das Schulungskonzept, welches drei Schlüsselemente zur Prävention von Social Engineering Angriffen vermitteln soll. Diese Schlüsselemente sind: Sensibilisierung für „Schlüsselreize“ die Manipulation ermöglichen, Höhere Motivation die Information sorgfältiger zu Verarbeiten, sowie eine Erhöhung der Fähigkeit zur Informationsverarbeitung.

Um dieses Schulungskonzept nun zu verbildlichen und um Beispiele für die Schlüsselemente zu geben, wird das Schulungskonzept bei einer fiktiven Firma angewendet. Diese Firma arbeitet im Bereich des Biomedical Engineering.

## **Abstract**

Information Technology has an integral part in our modern society. With the emerging of the new technology, especially the Internet, comes a new type of crime. This new type of crime is referred as Cyber Crime. In certain types of Cyber Crime, the successful manipulation, respectively “Social Engineering” of people plays an important role.

In order to prevent Social Engineering attacks this master theses contains an universal trainings concept. The trainings concept is based on three main pillars: The Analyses of the Psychological Factors, The Cyber Crime Aspects and The Analysis of the Didactics.

The Cyber Crime Aspects chapter reveals the need for such training concept and show the dimension of the issue in statistics. In the Analyses of the Psychological Factors part, dual processing information models are used to represent the mental processes involved in the manipulation. Furthermore it shows how the different manipulation techniques are used in the context of Cyber Crime. In the Analysis of the Didactics it is discussed how the Instructional System Design (ISD), respectively the Analysis, Design, Development, Implementation and Evaluation (ADDIE) training development approach fits to the requirements of the trainings concept.

The output of all three analytical steps are resulting in the trainings concept, that consists of three key elements to prevent Social Engineering attacks. These key elements are: awareness about “Simple Cues”, higher motivation to process information more carefully as well as a greater ability to process information.

In order to make the trainings concept more visual and to give examples for the key elements (training methods), the concept is applied on a fictive company. This company works in the field of Biomedical Engineering.

## **Glossary**

<b>ADDIE</b>	Analysis, Design, Development, Implementation and Evaluation are steps to develop a training
<b>AHTCC</b>	The Australian High Tech Crime Centre is a governmental organization that works in the field of Cyber Crime prevention
<b>Central route</b>	Central information processing route in the ELM model.
<b>Cross Site Scripting</b>	Cross-site scripting (XSS or CSS) is a Web based attack used to gain access to private information by delivering malicious code to end-users via trusted Web sites.
<b>Cyber Crime</b>	Crime in which IT is the enabler or the target.
<b>EAT</b>	Education, Awareness and Training is an IT Security Training methodology
<b>ELM</b>	Elaboration-Likelihood Model is a psychological model of information processing
<b>ENISA</b>	European Network and Information Security Agency is an non governmental organizations that works in the field of IT Security research.
<b>FTC</b>	Federal Trade Commission and in USA governmental organization that controls trade.
<b>HSM</b>	Heuristic-Symantec Model is a psychological model of information processing
<b>IC3</b>	Internet Crime Complaint Center is an non governmental organization the collects data about internet based crime.
<b>Identity Theft</b>	Identity Theft is theft of some others identity to commit illegal activities
<b>Information Gathering</b>	This is the first step in an Social Engineering attack and its purpose is to collect as much information as possible about the victim.
<b>Instructional Plan</b>	The Instruction plan is part of the training development process to group the lessons.
<b>ISD</b>	The Instructional System Design is a training development methodology
<b>LIST</b>	Legitimacy, Importance, Source and Timing can be abbreviated with the LIST
<b>Malware</b>	Also referred as malicious software a term that includes computer Viruses, Trojans and Spyware.

<b>NIST</b>	National Institute for Standards in Technology is an USA governmental organizations that works in the field of standards.
<b>Peripheral Route</b>	Peripheral information processing route in the ELM model.
<b>Phishing</b>	Phishing is a technique where Internet fraudsters send spam or pop-up messages to lure personal and financial information from unsuspecting victims.
<b>RAT</b>	Remote Access Trojan is a program that provides access to a PC from remote and without the knowledge of the legitimate user.
<b>Simple Cues</b>	Psychological term that relates to triggering events.
<b>Spam</b>	Spam is unsolicited e-mail.
<b>Spyware</b>	Any software that covertly gathers user information through the user's internet connection without his or her knowledge
<b>TEAM</b>	Training, education, awareness and motivation is an IT Security Training methodology
<b>Trojan</b>	Trojan or Trojan horse is a computer program that is apparently or actually useful and contains a backdoor or unexpected code.
<b>Virus</b>	A type of malicious software that can destroy the computer's hard drive, files, and programs in memory, and that replicates itself to other disks.

## **Table of Content**

<b>Acknowledgment .....</b>	<b>i</b>
<b>Eidesstattliche Erklärung .....</b>	<b>ii</b>
<b>Kurzfassung .....</b>	<b>iii</b>
<b>Abstract .....</b>	<b>iv</b>
<b>Glossary .....</b>	<b>v</b>
<b>1. Introduction: Scope of the Problem .....</b>	<b>1</b>
1.1. Cyber Crime Aspects .....	1
1.2. Conclusion .....	9
<b>2. Analysis of Psychological Aspects .....</b>	<b>10</b>
2.1. Introduction .....	10
2.2. Information Process .....	11
2.3. Peripheral Route – Simple Cues .....	15
2.3.1. Authority .....	16
2.3.2. Commitment and Consistency .....	19
2.3.3. Liking .....	20
2.3.4. Reciprocity .....	22
2.3.5. Scarcity .....	23
2.3.6. Social proof .....	24
2.3.7. Fear .....	25
<b>3. Analysis of Didactics .....</b>	<b>28</b>
3.1. Background .....	28
3.2. Instructional System Design .....	28
3.2.1. Analysis .....	30
3.2.2. Design .....	30
3.2.3. Development .....	31
3.2.4. Implementation .....	31
3.2.5. Evaluation .....	31
3.2.6. Information Security Awareness Programs .....	32
<b>4. Trainings concept .....</b>	<b>36</b>
4.1. Introduction .....	36
4.2. Concept .....	38
4.2.1. Trainings sample scenario .....	39
4.2.2. Pre-Training Phase .....	39
4.2.3. Trainings plan .....	41
4.2.4. Post-Training Phase - Evaluation .....	75
4.3. Summary .....	78



4.4. Ongoing Awareness.....	79
<b>5. Prevention Success Parameters.....</b>	<b>82</b>
<b>6. Conclusion .....</b>	<b>84</b>
<b>7. Appendix .....</b>	<b>85</b>
7.1. Information Awareness Poster examples .....	85
<b>8. Bibliography.....</b>	<b>87</b>
<b>9. Table of Figures .....</b>	<b>91</b>

## 1. Introduction: Scope of the Problem

Information Technology (IT) is an integral part of our society. IT is essential for economics, health care and public infrastructure. People are much more exposed to IT then it was in the past.

Given the fact, that the Internet allows people to act globally, with hardly any restrictions in terms of countries or local legislation and to be almost anonymous when doing so, the internet and its connected IT Systems are also a facilitator for a new kind of criminal activities. These criminal activities in combination IT are called Cyber Crime. The following chapter gives an overview on the different aspects and facets of Cyber Crime. It shows the criminal activities carried out with the successful manipulation of the people. Granger [2001] says the “Weakest Link” in the IT security chain are the people.

### 1.1. Cyber Crime Aspects

The Australian High Tech Crime Centre [AHTCC, 2009] defines basically two different modes of Cyber Crime. The first is where the target is the person and IT is the carrier or enabler for traditional criminal activities. In the second case crime is committed directly against computers and computer systems and the person is the originator.

The criminal activities are basically the same as in traditional crime [RUSCH, 1999]. But in comparison to non IT based crime it is much more global and difficult to tackle.

A good example of a traditional criminal activity that depends on the manipulation of people with the help of IT in order to commit the crime is the so called “Mule Recruitment”.

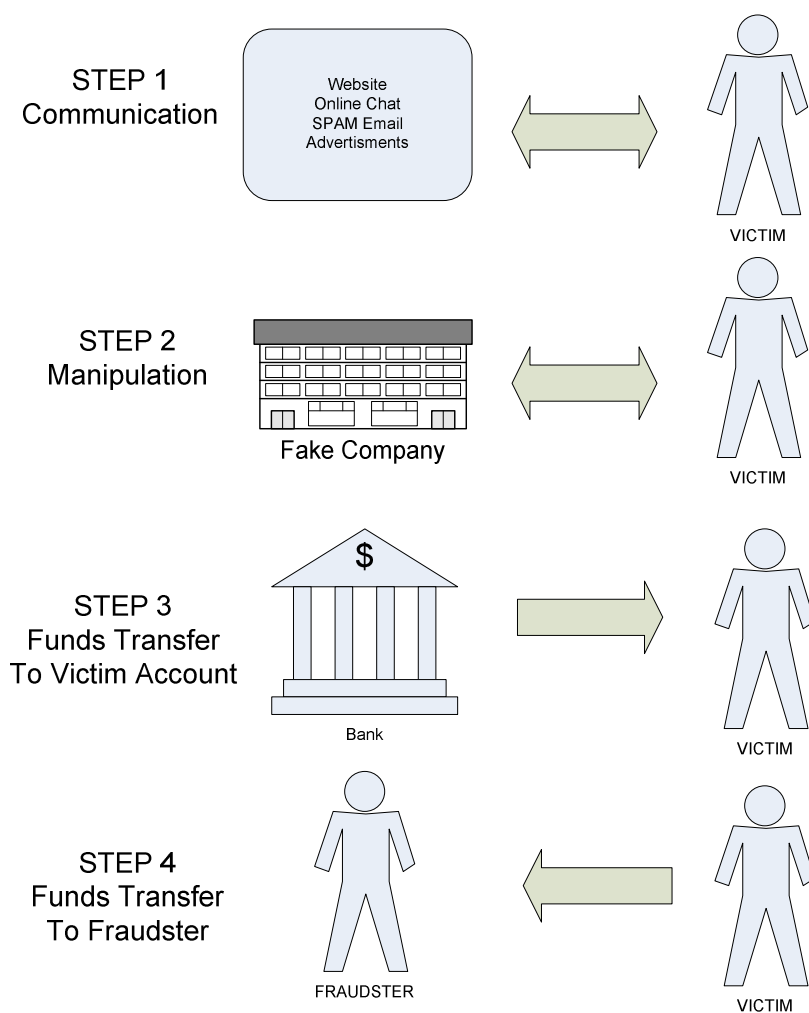
“Mule Recruitment’ is an attempt to get a person to receive stolen funds using his or her bank account, and then transfer those funds to criminals overseas.”

“The new methodology expands on existing money laundering scams; criminals advertise jobs on popular employment or job-seeking websites, online in chat rooms or through unsolicited employment emails.”

[AHTCC, 2009]

“Mule Recruitment” is just one example but it shows the involvement of the human factor and how manipulation techniques can be carried out via IT, in order that people are committing cyber crime.

The Figure 1.1 below displays the four consecutive steps of a “Mule Recruitment” crime.



**Figure 1.1.:** Process of “Mule Recruitment” [AHTCC, 2009]

The first step of the “Mule Recruitment” process can be summarized with the term of communication. The victim is approached by web sites, spam mails, chat rooms and all kind of advertisements. The methods of communication are not limited to the four mentioned. The goal in this step is always to get the victim to get in contact with the fraudster.

In the second step the fraudster tries to manipulate the victim to work for their company, but this company is a not real.

Once the victim is recruited and the bank account information is known to the fraudster, the money transfer is initiated. The funds could be stolen or black money from other criminal activities. In this third step the actual crime is committed.

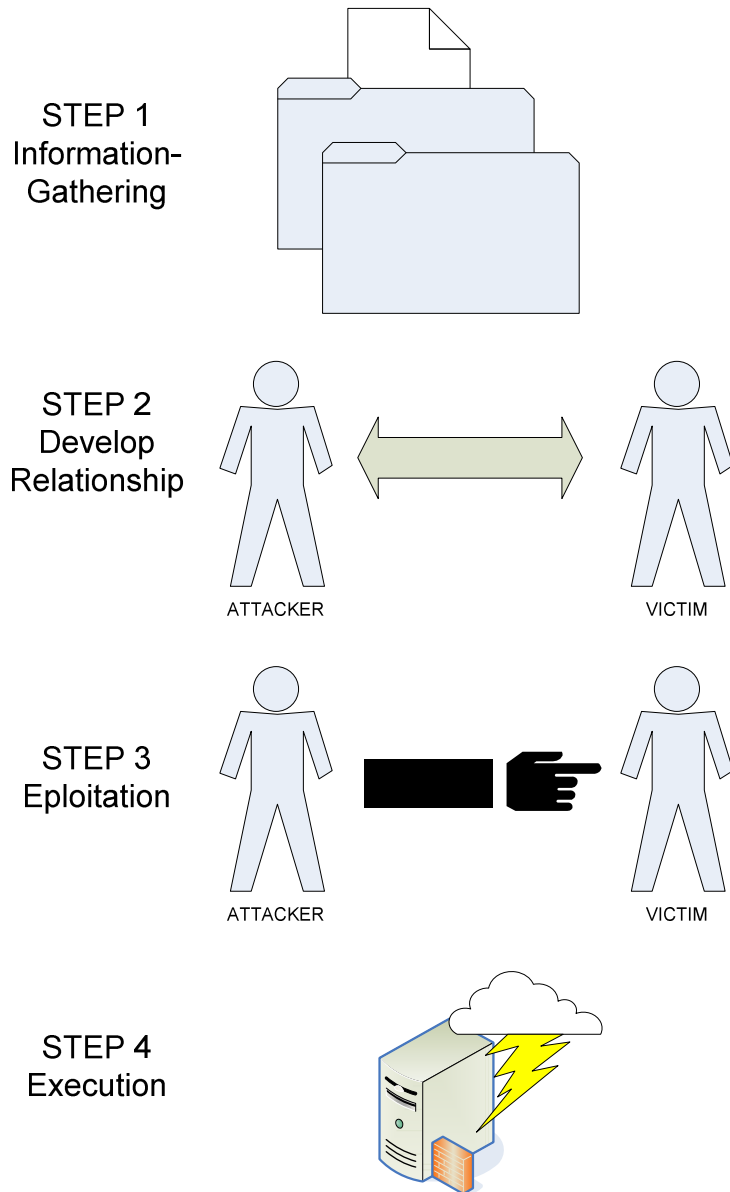
Once the victim has “laundered” the illegal funds, the fraudster asks the victim to transfer the money to an overseas bank account. This is done in most cases via wire transfer minus a commission charge for the victim.

The important success factors are the communication and the manipulation, both based on IT to attract and convince the victim.

An aspect of Cyber Crime that uses the person as enabler for crime against IT matches with the definition of Social Engineering.

“Social engineers use many different tactics to persuade and influence others in order to achieve their goal of gaining unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network.” [Granger, 2001]

Figure 1.2 explains how “Social Engineering” works and how the human factor comes into play.



**Figure 1.2.:** “Social Engineering” attack process [Malcom, 2007]

In the Social Engineering attack process, the first step is to gather as much information about the victim as possible. This quality and quantity of information is important for the success of the other steps. There are several sources of that can be used to gather information such as Search Engines or public web sites. Search engines can provide a lot of information about a network of a company. Search engines collecting information with programs called web bots. These web bots are feeding the database of the search engine. For an attacker who wants to carry use SE relevant information might be:

- Employee contact details and information
- Organizational Charts
- Email addresses
- Telephone numbers
- Physical locations
- Details of internal and external IT systems
- Documents that reside on public accessible servers

An other source of information gathering that used in the context of SE is the so called “dumpster diving” practice.

“Dumpster diving is an act of digging through the refuse, remains, or leftovers from an organization or operation in order to discover or infer information about the organization.” [Stewart et. Al., 2008]

The second step is called “Developing Relationship” and it consists of establishing a trust relation ship with the victim. Different psychological techniques are carried out to do so. These techniques are described in the chapter “Analysis of Psychological Aspects”.

Once the relationship of trust is established, the manipulation takes place. The target of the attack could be sensitive data or access rights or any other valuable information. This is actually the step in which the cyber crime is committed.

The last step “Execution” is carried out in the dependence of the kind of result from the manipulation. This could also lead into the new information gathering and a restart of the process.

The success of the Social Engineering attack is depending on the success of the manipulation of the individual.

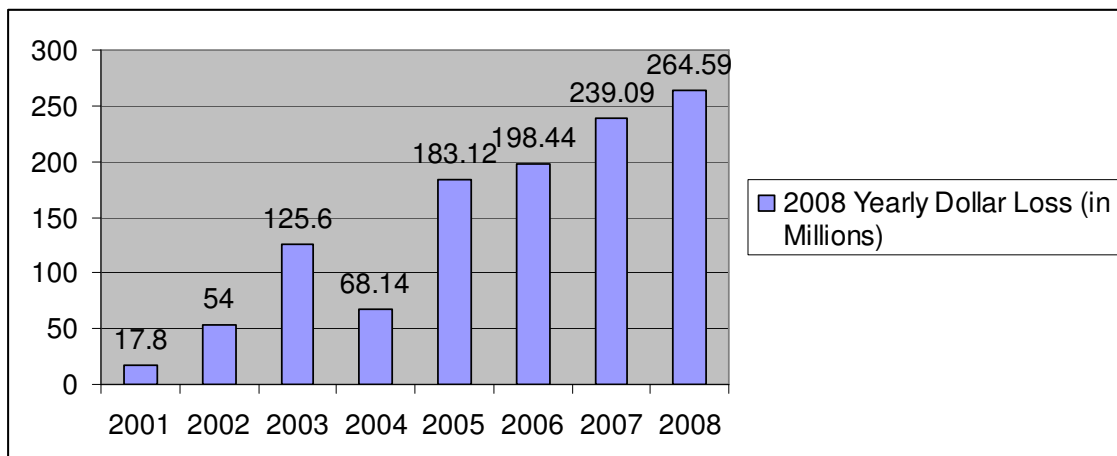
Note from the Author:

A lot has been written about Social Engineering but in the opinion of the Author the topic of this master thesis should be written from the Cyber Crime perspective where Social Engineering is just a part of.

The following statistics assisting to undermine the dimension of quantify the problem of Cyber Crime.

The Internet Crime Complaint Center (IC3)<sup>1</sup> a project awarded by the Bureau of Justice Assistance of the United States of America provides an easy to use reporting platform for victims of Cyber Crime. Furthermore the Internet Crime Complaint Center produces a yearly report, which reflects the Cyber Crime activities in the United States.

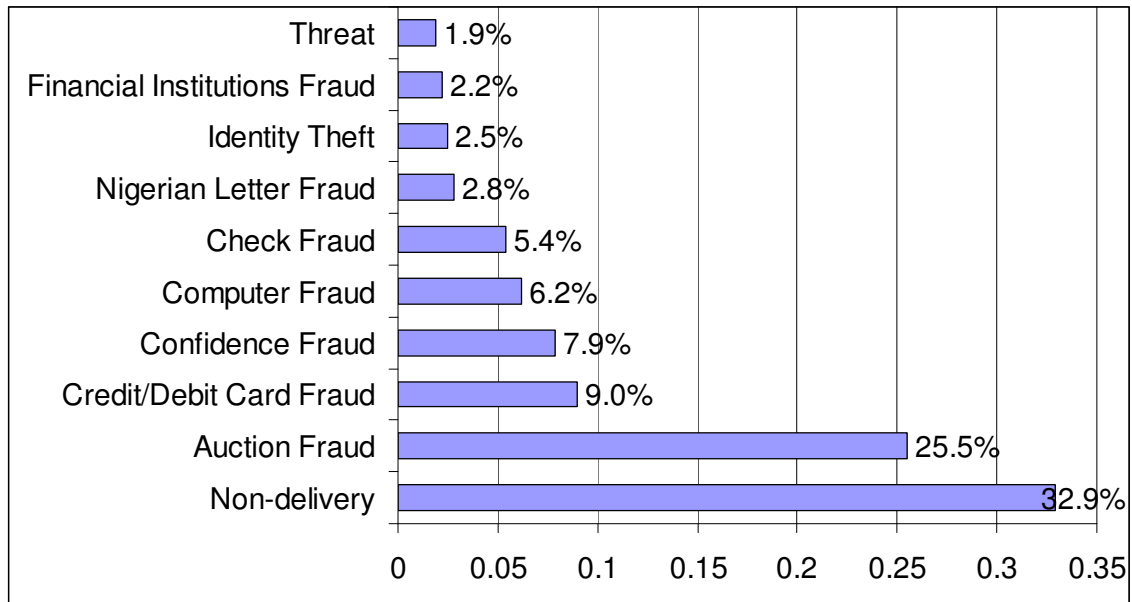
The Figure 1.3 shows the financial dimension of Cyber Crime. The loss of million dollars per year is increasing over the time. It is important to understand, that this report reflects Cyber Crime activities reported by people in the United States. Furthermore the report does not include any incidences reported from enterprises or companies.



**Figure 1.3.:** Financial Aspect of Cyber Crime [IC3, 2008]

The Figure 1.4 shows the different types of Cyber Crime in percentages, that have been reported and actually causing the financial loss.

<sup>1</sup> IC3, Internet Crime Complaint Centre – internet crime registration platform, <http://www.ic3.gov/> (accessed December 30, 2009)



**Figure 1.4.:** Cyber Crime types [IC3, 2008]

The fact is that most reported complains are “Non-delivery” and “Auction Fraud”. Going further into details and examining the top reported crime types, it shows clearly, that these crime types are very much linked with manipulation of people.

The IC3 classifies internet crime into fraud types. “Non-delivery” and “Auction Fraud” are both categorized as confidence fraud [IC3, 2008].

The definition of confidence fraud from the IC3 is:

“The reliance on another’s discretion and/or a breach in a relationship of trust resulting in financial loss. A knowing misrepresentation of the truth or concealment of a material fact to induce another to act to his or her detriment” [IC3, 2008]

In this crime a trust relation ship is exploited which involves the “human factor”. For example, the merchant had to appear trust worthy enough to pay in advance. There are similarities between such confidence crime and the “Social Engineering” attack from a hacker. Where as the hackers goal is normally not money, the successful manipulation of people is essential for both in order to be successful.



Note from the Author:

The nature of Cyber Crime activities, that include the human part are not always tangible in statistics. This makes it difficult to receive correct numbers.

The manipulation of people is very often used to commit another facet of Cyber Crime, the Identity Theft. Below the definition on Identity Theft and its emerging nature in combination with the internet.

“An emergent issue in society, identity theft is the series of tasks involving the theft of one’s personal information, such as your name, credit card number, or social security number which in turn is utilized for illegal activity. It is the fastest growing crime in America and it is estimated by the FTC<sup>2</sup>, that approximately 9 million individuals get their identities stolen each year. With more frequent online use, identity theft abuse is expected to grow and impact individuals of all ages.” [WEB3, 2009]

To give an example of the dimension of Identity Theft the following statement from the Identity Theft Daily web site<sup>3</sup> can bring some light into the shade.

“Federal prosecutors in Newark, N.J., allege that an international identity theft ring used social engineering and other techniques to steal more than \$2.5 million from home equity lines of credit.(...) ”

The defendants allegedly posed as the customers to trick bank, credit union and credit card company employees into revealing information and changing the mailing address on the accounts.” [ITD, 2009]

---

<sup>2</sup> Federal Trade Commission, US department of trade web site, <http://www.ftc.gov/> (accessed December 30, 2009)

<sup>3</sup> Identity Theft Daily, web site that provides information on Identity Theft cases for law enforcement and legal institutions ,[www.identitytheftdaily.com/](http://www.identitytheftdaily.com/) (accessed December 30, 2009)

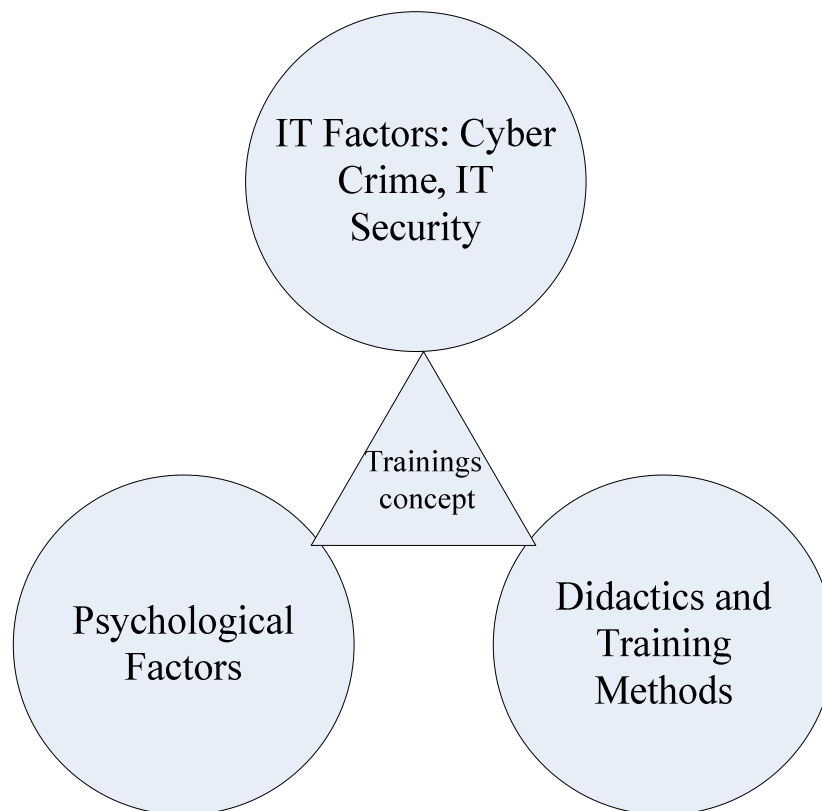
## 1.2. Conclusion

This master thesis has its focus on the vulnerability of humans to manipulation in the context of Information Technologies. This is also referred as Social Engineering. In which the manipulation of the person is the key element to assist or commit illegal activities. This crime may be committed by the victim conscious or not conscious.

The term illegal includes breaches against national or international laws or private industry rules and regulations (e.g. company wide IT Security policy).

Comprehensive analysis of psychological factors results into a training concept. This training concept is the foundation to deliver trainings to prevent the manipulation.

Figure 1.5 below shows the three main pillars of the trainings concept to prevent SE attacks. Each pillar has its own chapter in this thesis.



**Figure 1.5.:** Three main pillars building up the trainings concept

## 2. Analysis of Psychological Aspects

### 2.1. Introduction

Knowing the anatomy of Cyber Crimes involving the manipulation of people, some questions have to be answered. Most of all, the question, why people are vulnerable to manipulation has to be discussed into detail. Such details including, the types of manipulation approaches and what “thinking processes” are involved.

The answers are found in the disciplines of Psychology, especially Social Psychology. This will help, to build the foundation before developing a training concept.

A good information processing theory on persuasion that has been recently used in conjunction with the electronic media is the Elaboration-Likelihood Model (ELM) [Petty & Cacioppo, 1986].

The ELM and the Heuristic-Symantec Model (HSM) [Chaiken, 1980] are trying to explain the psychological mechanism behind persuasion. These dual process information theories are showing the factors involved that makes a persuasion respectively, a manipulation communication, successful.

The following chapter sets these theories into the context of Social Engineering. Furthermore other perspectives on the psychological field that could be relevant for the topic of this Master thesis are discussed.

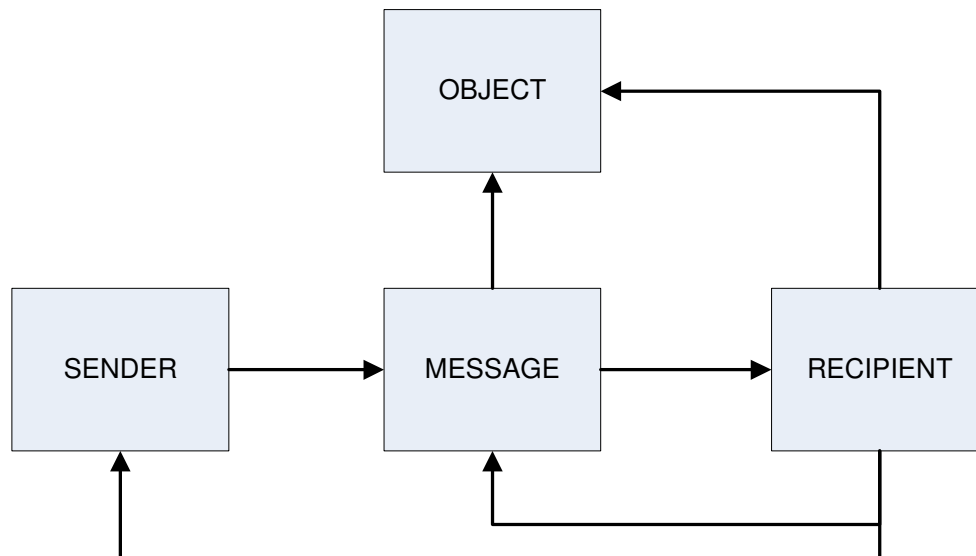
Note from the Author:

On the research of the primary literature on Social Engineering, the psychological aspects are not discussed on a level, which would provide enough substance, to build a training concept upon.

## 2.2. Information Process

As described under “Cyber Crime Aspects” in the chapter before anatomy of a successful SE attack in the context of Cyber Crime depends on the successful manipulative communication. The Buehler [1934] model (Figure 2.1) shows all relevant factors involved during the communication. These parts are the sender, the recipient and the message about a certain object. The sender wants to change the attitude of the recipient in regards to the object. This change depends on all factors and their interrelation. Later in this chapter examples about SE attacks show how the different interrelations, lines with arrows in Figure 2.1, are working. For example how a fake email sender address has influence on the recipients perception about the message and the object respectively content of the email.

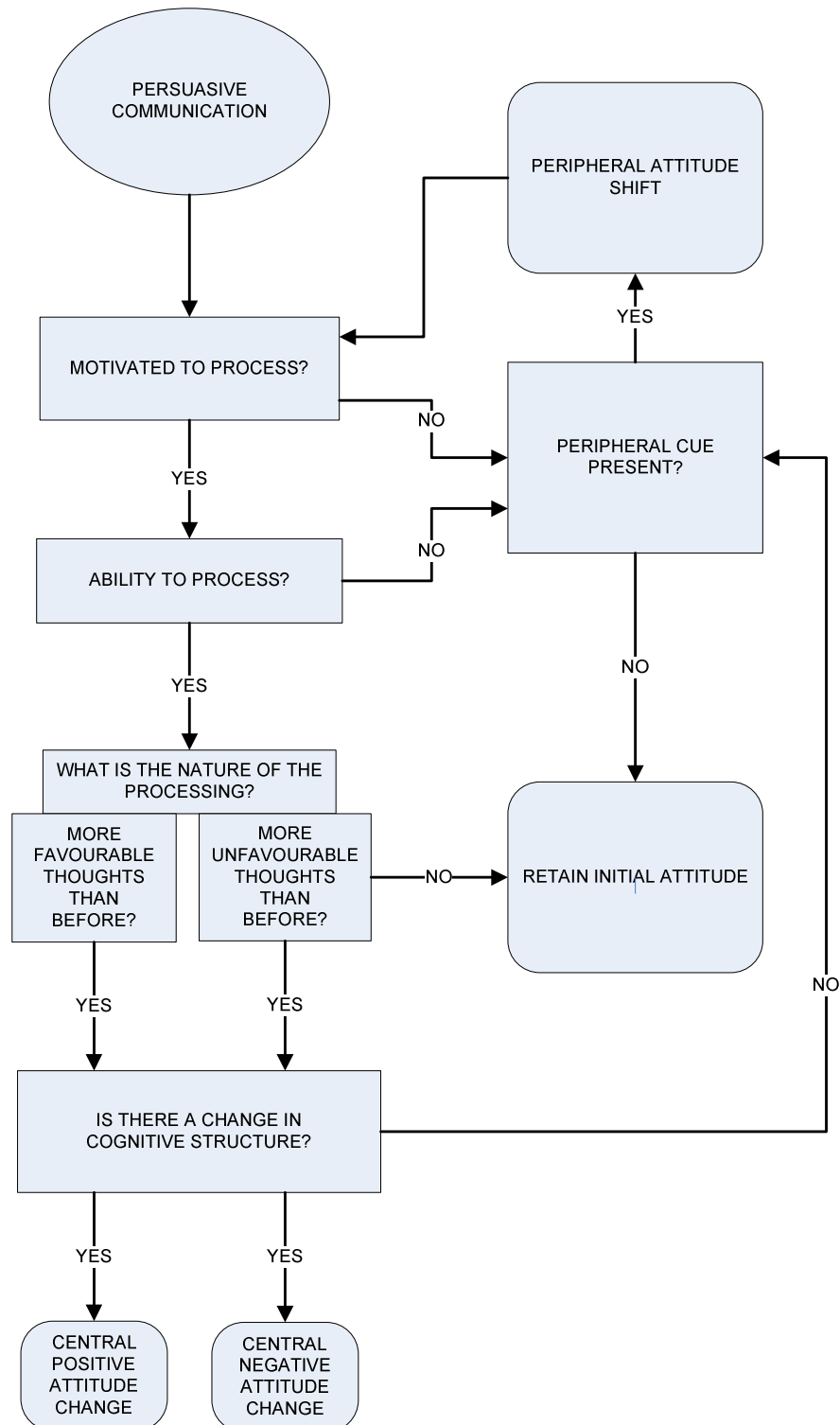
The attitude change on the receiver side does not depend on the objective attributes of the factors but how it's being perceived. [Herkner, 2001]



**Figure 2.1.:** Communication factors [Herkner, 2001]

The next step is to examine the processes involved on the recipient side on how the perception is reached. A dual information process model that has been used in context of persuasion and electronic media is the ELM [Petty & Cacioppo, 1986; Caldini, 1993]. The ELM model tries to explain the psychological processes on the recipient side that are involved in an attitude change.

The Figure 2.2 shows the ELM from Petty and Cacioppo. The central idea is the assumption that a change of attitude can be reached via the two routes. The left route is the so called central route and the route on the right side is the peripheral route.



**Figure 2.2.:** Elaboration-Likelihood Model [Petty & Cacioppo, 1986]

The central route explains the change of attitude based on carefully weighted cognitive processing of the offered information. The person taking the central route pays ultimate attention to the information before changing the attitude.

The peripheral route means less cognitive effort for the person. It is based on assumptions and relying on simple cues in the persuasive situation.

If a person takes the central or the peripheral route depends on motivation and the ability of processing the information. If the motivation is high and the ability to process is high, the central route is taken. Whereas if the ability and/or the motivation is low, the peripheral route is likely to be taken. [Petty & Cacioppo, 1986]

The motivation of the recipient to take the central route depends primarily on three factors: [Bongard, 2002]

#### 1. Involvement of the recipient

It means the Outcome relevant involvement is either high or low. The outcome relevant involvement is a factor that describes how important the outcome of the messages to the individual is. If the outcome relevance is high the central route is likely to be taken and if it is low the peripheral route is preferred. [Slater, 1997]

Example: The IT database administrator receives a request for a new user account. This account would have very high system privileges. The database administrator is concerned about the integrity of the database especially, as he would be personally fully held accountable for any misuse. That would fulfill the need of personal importance and the database administrator is very likely to process the request on the central route respectively very carefully.

#### 2. Number of information sources

If the same information has multiple sources the arguments are gaining trustworthiness.

Example: If an employee receives one email from a not trusted source, with the request of information, then it is less likely processed. But if the employee receives an email, a fax and, a phone call, with the same content but from different sources, it is more likely that the request will be processed.

### 3. Cogitation need of the person

This factor involves the individual nature of each person in regards to their motivation to process the information on the central route of the ELM.

“Some individuals generally take greater pleasure in thinking than others and thus these individuals tend to engage in effortful thought because of its intrinsic enjoyment, without regard to the importance of the issue or the need to be correct.” [Petty & Wegener, 1999]

Next to the motivation of the individual to process the information on the central route, the ability to do so, plays also an important role. The ability to process the information on the central route depends primarily on two factors:

#### 1. Distraction in the situation

The degree of distraction has a direct influence on the ability to elaborate the information. [O’Keefe 2002]

Example: If the recipient works on the computer while someone is working with a very loud drilling machine the recipient might be just able to process the information less intensively (low level of involvement).

#### 2. Prior Knowledge

If the recipient has in good knowledge of the topic in the information it is more likely that he will process it more intensive (high involvement). [O’Keefe 2002]

Example: A police officer specialized in Cyber Crime is less likely to be a victim of a Social Engineering attack.

When it comes to Social Engineering the attacker tries to convince the victim on the peripheral route. This has the greater chance of success as it is based on the following facts:

”When the elaboration likelihood is low, people follow the peripheral route to persuasion. Under this second route, attitudes are influenced by relatively simple cues in the persuasion context [...] “  
[Petty & Cacioppo 1986]

The opinion reached via the central route is more likely to have a correlation with the attitude changes. The experiments of Wilson and Dunn [1986] have shown, that the correlation between attitude and opinion is kept, if the person thinks about the reason about the opinion. The thinking about the opinion itself could lead to a change of the attitude.

The HSM from Chaiken [1980] has similarities to the ELM. Like the ELM the HSM predicts that comprehensive information processing is done, if the motivation and the ability is high. Unlike the ELM, Chaiken focuses on the peripheral route of information processing. This route is taken based on simple cues. Some of these simple cues are:

- Experts are trustworthy
- Likeable people are trustworthy
- More arguments are better arguments
- Longer messages are more powerful

Chaiken introduces, next to motivation and ability, a third factor, salience and vividness. To use a simple cue, the memory has to be activated. This is more likely; if the simple cue is has more salience and vividness. [Chaiken & Eagly 1983]

## 2.3. Peripheral Route – Simple Cues

There are many types of peripheral cues. In terms of Social Engineering, Caldini [1993, 1994] identified six common cues that signal the use of a peripheral message: authority, commitment and consistency, liking, reciprocity, scarcity and social proof.

The following chapter will explain these simple cues and how they are used in Social Engineering attacks in the context of Cyber Crime.

Note from the author: In the opinion of the author “simple cues” are not just limited to the six mentioned by Caldini but these have been proven by experiments and respected by the scientific society.



### 2.3.1. Authority

The idea behind is to hide the manipulative request into a authority vehicle. As authority has a strong persuading influence on people.

“People have a tendency to comply when a request is made by a person in authority. A person can be convinced to comply with a request if he or she believes the requestor is a person in authority or a person who is authorized to make such a request.” [Mitnick, 2002]

The attacker using the power of authority can directly approach the victim by email or telephone to retrieve information or trigger a certain action.

To use this kind of persuasion technique the attacker needs a lot of information about the victim before hand. Such information would be for instance the position of the person in the company in regards to who the person reports to and/or who is gives this person usually directions. The process is also called Information Gathering and includes various ways to retrieve the information (e.g. Dumpster diving, search engines ...).

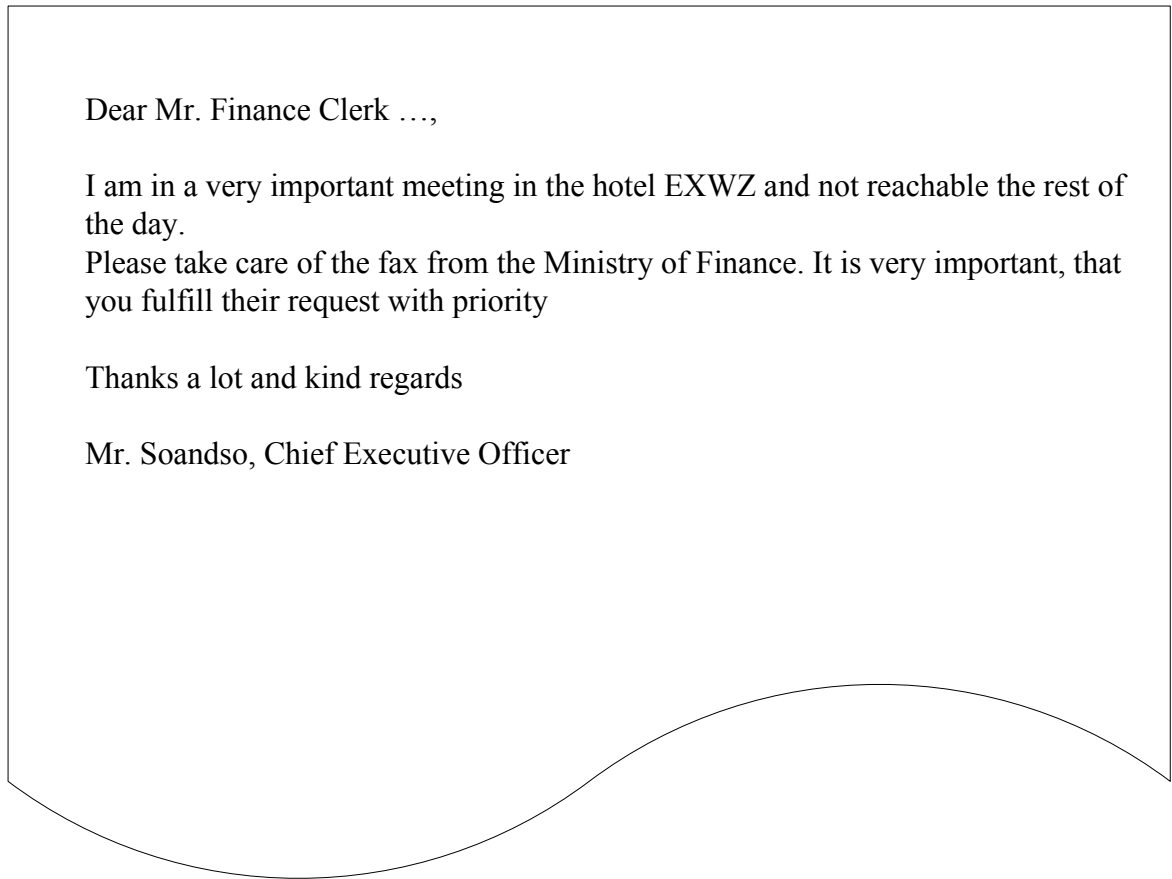
This technique also includes abuse of signs of authority such as cloths, titles and trappings [Cialdini, 1984] these would also fulfill the salience and vividness requirement from Chaiken.

People are likely to obey to authority, as the person takes over the responsibility. The Milgram experiment has shown that clearly.

Example:

In this example, a forged fax is used to show the technique of authority in the context of Social Engineering. The fax has been composed to trick a clerk in the finance department.

The Figure 2.3 below shows that fist page of the fax. It uses the element of authority in the sense that the Chief Executive Officer gives the finance clerk the instruction to fulfill the request of the Finance Ministry. Another important element is that urgent nature of the request. Creating pressure, respectively stressing the urgent nature, is sometimes a good amplifier for persuasion.



**Figure 2.3.:** The first page of a forged fax

The next Figure 2.4 shows the second page of the fax sent by criminal to the finance department.



**Figure 2.4.:** The Second page of a forged fax<sup>4</sup>

The second page of the fax is made up in a way that it looks very professional, to support the idea of salience and vividness, in order to bring the person on the peripheral route. That is done by using the symbol of the Finance Department. Furthermore it has more details to support the proof of authority with the picture of the signature. Sometime fake authorities can go along with Identity Theft.

<sup>4</sup> Logo from Austrian Ministry of Finance, [www.bmf.gv.at](http://www.bmf.gv.at) (accessed December 29, 2009)

If someone from the finance department receives such a fax and it seems to come from the chief executive officer asking for help, it is very likely, that the instructions will be followed resulting into leakage of sensitive account information.

This example shows only how to retrieve sensitive information about accounts but it is not limited in any way. Other possibilities would be an order of goods or money transfer.

The criminals are hidden with the possibilities that modern IT technologies can offer e.g. fake fax caller identifier.

### 2.3.2. Commitment and Consistency

People have the strong need to be consistent with what they have already done. This justifies our earlier decisions. The behavior to be consistent is strong enough to be automatically consistent, even thou it does not make any sense. This persuading technique's enabler is commitment.

"If I can get you to make a commitment (that is, to take a stand, to go on record), I will have set the stage for your automatic and ill-considered consistency with that earlier commitment. Once a stand is taken, there is a natural tendency to behave in ways that are stubbornly consistent with the stand," [Cialdini, 1984]

Example:

The criminal contacts a new employee to inform him of the agreement to abide by certain security policies and procedures as a condition of being allowed to use company IT systems. After the criminal has explained a few security practices it asks the user for the password in order to verify compliance with the IT security policy. After the user has revealed the password, the criminal makes a strong recommendation to construct future passwords in such a way that the criminal will be able to guess it. The victim complies because of her prior agreement to abide by company policies and her assumption that the caller is merely verifying her compliance. [Mitnick, 2002]

### 2.3.3. Liking

People have the tendency to agree and trust others, if they are known and likeable. This goes along with the statement from Chaiken [1980], that likeable people are trustworthy.

The way to persuade others with linking could be achieved by:

- people who are physically attractive
- people who are similar to us
- people who give us compliments
- people who are familiar to us
- or familiar to people whom we cooperate
- people with whom the associations are positive

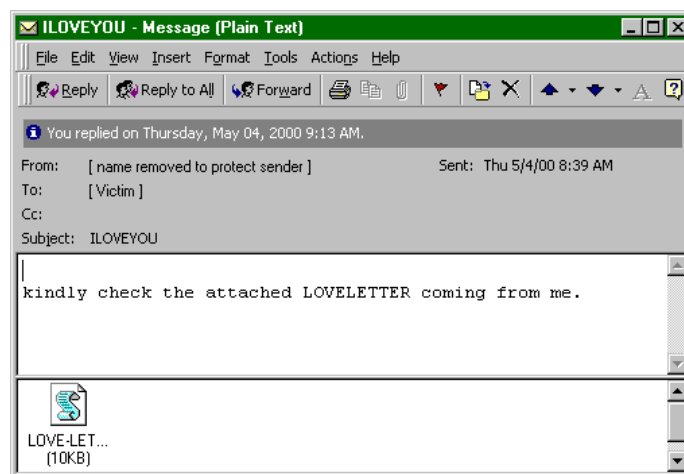
All these could be abused to persuade a person. Often it is not only the factor linking that counts but in combination with other persuading tactics it is very powerful.

Example:

Very often this technique is used by computer viruses spreading via email. The Figure 2.5 shows the so called “Love letter virus”. This computer virus spreads by with a very tricky distribution method.

It uses the local address book to mail replicates from itself to others. In this case the user knows most likely the senders address and trusts the content more likely.

Furthermore by pretending to contain a love letter the users might be more motivated to open the mail.



**Figure 2.5.:** Picture of the “love letter Virus” [WEB 4, 2009]

Another field where this SE attack technique is used is the so called “Social Network”. Social Networks are internet based web platforms where people keep contact with each other and exchange information. In most of this Social Networks people have to acknowledge and identify their “friends”. These friends are trusted and if people get an action request from a friend, as this someone they know, it is most likely that it will be processed. The Figure 2.6 below shows how such attack would work on the Social Network platform Facebook<sup>5</sup>.



**Figure 2.6.:** SE attack on Social Networks [Chai, 2009]

In this case Bob receives link from a friend and if he follows the link a computer malware program is downloaded to his PC.

---

<sup>5</sup> [www.facebook.org](http://www.facebook.org)

### 2.3.4. Reciprocity

The simple cue reciprocity works with gifts or even with the promise of value that lead us on to the process the information on the peripheral router in the context of the ELM. Kevin Mitnick [2002] describes how reciprocity is used as SE attack technique:

“We may automatically comply with a request when we have been given or promised something of value. The gift may be a material item, or advice, or help. When someone has done something for you, you feel an inclination to reciprocate. This strong tendency to reciprocate exists even in situations where the person receiving the gift hasn't asked for it. One of the most effective ways to influence people to do us a "favor" (comply with a request) is by giving some gift or assistance that forms an underlying obligation.” [Mitnick, 2002]

An example (Figure 1.1) showing how reciprocity works is the “Mule Recruitment” explained under the chapter “Cyber Crime Aspects”. The victim has the promise to get some money if he/she provides their bank account information for the wire transfer. By doing so the victim plays a part in the international money laundering mafia.

Another example of an SE attack with the element of reciprocity is showing in Figure 2.7 of a phishing mail.

From: Support  
Subject: Internal Revenue Service - Please read.

---

**Tax Refund Notification!**

Internal Revenue Service Department Notice.  
After the last annual calculation of your fiscal activity we have determined that you are eligible to receive a tax refund of **\$192.50** .  
Please click on the following link, submit the tax refund request and allow us 6-9 business days in order to process it.

<http://www.irs.gov/tax-refund/>

**Please Note:**

If we do not appropriate records within 48 hours, then we will assume this email is invalid and the refund will be suspended.

Regards,  
Internal Revenue Service - IRS GOV

**Figure 2.7.:** Phishing email [411 a, 2009]

The email in Figure 2.7 requests action from the user and click a link. After the user has clicked the link it will be redirected to a fake web site, that has been made up to steal the users personal data respectively, commit the crime Identify Theft.

### 2.3.5. Scarcity

Scarcity works with our feelings of value if things are rare. In fact opportunities are more valuable to us if they are limited available. According to Cialdini [1984] things difficult to possess seem to be typically better than those that are easy to possess.

An example matching the use of scarcity is the Cyber Crime “auction fraud”. In this case the seller of a good makes the buyer believe, that there are only a few left. In combination with time pressure, buyer is more likely to buy the good without checking the credibility of the seller.

But this method works also in combination with fake online surveys (Figure 2.8). Such a survey could ask the user via pop-up window, email or chat to participate in a survey to improve the security of a web site. The first 100 participants are going to get a free gift. If the user follows the link then a malware program is downloaded and installed on the PC.



Visit our other sites for more Holiday Ideas: [Sears](#) [Kmart](#) [the great indoors](#) [LANDS'END](#)

**Kmart** [my profile](#) [customer service](#) [order status](#) [recently viewed](#) [Shopping Cart 0 items \(\\$0.00\)](#)

[Jewelry](#) [Clothing](#) [Bed & Bath](#) [For the Home](#) [Health & Beauty](#) [Fitness & Sports](#)  
[Baby](#) [Entertainment](#) [Electronics](#) [Toys & Games](#) [Tools & Outdoors](#) [Appliances](#)

Search   [Store Locator](#) [Pharmacy](#) [Clearance](#) [Gift Registry](#) [Gift Cards](#) [E-Mail Specials](#)

**GET TWO \$5 K MART COUPONS** When You Sign Up For Kmart Emails [Sign Up Now](#) [Weekly Ad](#)


[Store Accessibility Comments](#) [FTC Giftcard Settlement](#) [Discover The Easy Way To Pay. Kmart Layaway](#)

**FREE SHIPPING SITEWIDE ON ORDERS OVER \$49**  
Exclusions apply. See details.

**Customer Satisfaction Survey**

Thank you for taking the time to respond to this survey.  
 In return, we will credit \$150 to your account - just for your time.

**Please enter your account to credit your \$150 reward**


\* Card Number:  

\* Card Expiration Date:  Month  Year

\* Card Verification Value:  The last 3 digits on the back of your card

\* Card PIN:

Your Card Number and PIN are being used for bank authentication.  
 Your account will be credited within the next 3 business days.  
 It will appear as "Kmart Stores Survey" on your account history.  
 After card verification you will be redirected to the main page.

<b>Top Searches</b> <a href="#">Jewelry</a> <a href="#">Bed in a Bag</a> <a href="#">Clothing</a> <a href="#">Martha Stewart</a> <a href="#">Jaclyn Smith</a> <a href="#">Fisher Price Toys</a> <a href="#">Baby Toys</a> <a href="#">Riding Toys</a> <a href="#">Hasbro Toys</a>	<b>Kmart Resources</b> <a href="#">Store Finder</a> <a href="#">Gift Cards</a> <a href="#">Pharmacy</a> <a href="#">Store Accessibility</a> <a href="#">Comments</a> <a href="#">Wishlist</a> <a href="#">Order History</a> <a href="#">My Account</a>	<b>Kmart Deals</b> <a href="#">Weekly Ad</a> <a href="#">Sign up for email savings!</a>	<b>Company Links</b> <a href="#">Kmart Company Info</a> <a href="#">Sears Holdings Corporation Info</a> <a href="#">Careers</a> <a href="#">Join My SHC Community</a> <a href="#">FTC Gift Card Settlement</a>	<b>Customer Service</b> <a href="#">Shipping Information</a> <a href="#">Contact Us</a> <a href="#">Return Policy</a> <a href="#">Credit Cards</a> <a href="#">more</a> 
--	--	---	---	---

Product Recall | Terms of Use | Privacy Policy (Revised 8/22/08) | California Privacy Policy | Security Information | Children's Privacy Policy (Revised 3/6/07)  
 Business Opportunities | Site Map | License Info | © 2008 Sears Brands, LLC. All Rights Reserved.

**Figure 2.8.:** Fake survey from Kmart [411c, 2009]

### 2.3.6. Social proof

The principle of a "Social proof" simple cue is: one means people use to determine what is correct is to find out what other people think is correct [Cialdini, 1984]. This is even truer if the people have similarities among each other. Say they are working in the same department.

To illustrate the concept of the simple cue "Social Proof", Cialdini has cited the infamous New York murder of Catherine Genovese in which 38 "respectable, law-abiding citizens" watched the killer stalk and stab her. In this case psychologists believe no one took action because (..)

"(...) everyone else observing the event is likely to be looking for social evidence, too. And because we all prefer to appear poised and unflustered among others, we are likely to search for that evidence placidly, with brief camouflaged glances at those around us. Therefore, everyone is likely to see everyone else looking unruffled and failing to act. As a result... the event will be roundly interpreted as a non-emergency." [Cialini, 1984]

An example from Mitnick shows how the "Social proof" tactic is used in a SE attack:

" The caller says he is conducting a survey and names other people in the department who he claims have already cooperated with him. The victim, believing that cooperation by others validates the authenticity of the request, agrees to take part. The caller then asks a series of questions, among which are questions that draw the victim into revealing his computer username and password." [Mitnick, 2002]

### 2.3.7. Fear

The correlation between fear and change of attitude and/or beliefs are proven by the experiments of Janis and Feshbach [1953, 1954]. Both had the assumption that a certain level of fear can change believes of a person. In their experiment they have shown, the risks of insufficient dental hygiene to create fear. The experiment used three different levels of fear: low, medium and strong. The group under the low fear had the greatest likelihood of believe change.


Other experiments have shown that too much fear does not facilitate the change of believes. But this theory lacks fundamental data and more variables have to be taken into consideration. [Herkner, 2001]

The fact is, that some manipulation techniques using fear to change beliefs and attitude of the victim. There are many aspects of fear and how it is used in the two modes of Cyber Crime.

The fist example explains how fear is used if the target is the human and IT the enabler. The second shows the mode if IT is the target and the human is the enabler.

Example 1: Figure 2.9 shows an email pretending to be send from the Bank of America. In this email it is written, that the account will be deactivated if the customer does not provide certain private information. In this case the user follows a bogus link and then his private information will be stolen and that could result in a financial loss.

From: BankOfAmerica Alert <Bankofamerica@alert.com>  
 Subject: **Bankofamerica Alert: Restore Your account.**  
 Date: August 31, 2008 6:49:57 AM PDT  
 To: undisclosed-recipients: ;  
 Reply-To: Bankofamerica@alert.com



**Higher Standards**

## Online Banking


---

Need additional  
up to the minute  
account  
information?  
[Sign In »](#)

**Dear Valued Customer :**

We recently have determined that different computers have logged in your Bank of America Online Banking account, and multiple password failures were present before the logons. We now need you to re-confirm your account information to us. If this is not completed by September 2, 2008, we will be forced to suspend your account indefinitely, as it may have been used for fraudulent purposes. We thank you for your cooperation in this manner. In order to confirm your Online Bank records, we may require some specific information from you.

To restore your account, please [Sign in to Online Banking](#).




**thank you for using Bank Of America Online Service.**


---

Your account might be place on restricted status. Restricted accounts continue to receive payments, but they are limited in their ability to send or withdraw funds. To lift up this restriction, you need to login into your account (with your username or SSN and your password), then you have to complete our verification process. You must confirm your credit card details and your billing information as well. All restricted accounts have their billing information unconfirmed, meaning that you may no longer send money from your account until you have reactive your billing information on file. [Sign in to Online Banking](#)

Thank You.

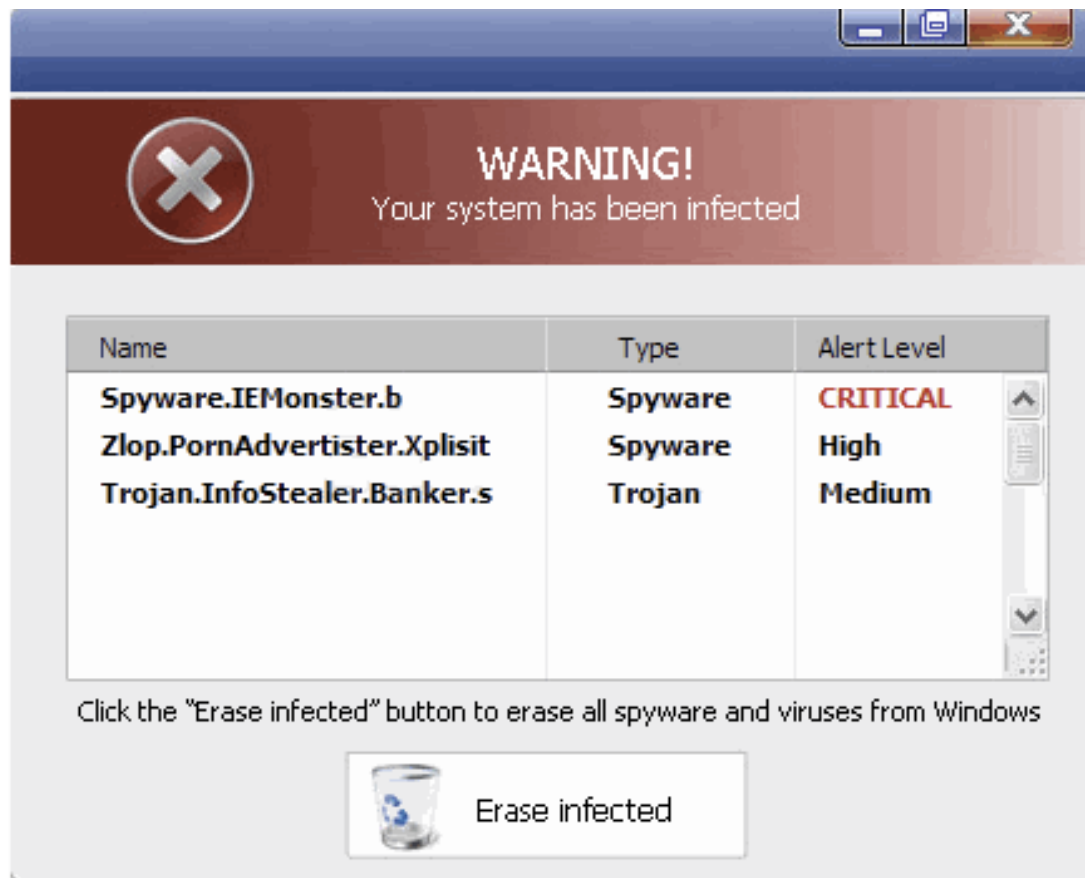
Please do not reply to this message. If you have any questions about the information in this e-Bill, please contact your biller. For all other questions, call us at 800-887-5749.

Bank of America, N.A. Member FDIC. [Equal Housing Lender](#)   
 2008 Bank of America Corporation. All rights reserved

Official Sponsor 2004-2008  
 U.S. Olympic Teams 

**Figure 2.9.: Fake mail from Bank of America [411c, 2009]**

Example 2: Figure 2.10 below shows a Pop-up window that scares the user that the system is infected with Spyware and Trojan programs. If the person clicks on “Erase infected” a malware program is installing.



**Figure 2.10.:** Fake Virus Removal [411b, 2009]

Note from the Author:

Gragg [2002] has given another three factors on the psychological aspect of Social Engineering: Strong Emotion, Stress and overloading. But they are not reflected in any social psychological literature or proven by experiments. Whereas fear is proven to be important to change beliefs and attitude.

### 3. Analysis of Didactics

#### 3.1. Background

In order to develop a trainings concept, it is important to select an appropriate didactical methodology. This didactical methodology has to be efficient and effective at transferring the knowledge. Based on this criteria, the Instructional System Design is a good candidate to serve as basic methodology to develop the training concept against Social Engineering attacks in the context of Cyber Crime.

#### 3.2. Instructional System Design

Leshin et al. [1992] labeled instructional design as instructional system development (ISD), in which an individual completes an ordered set of activities in order to develop instructional systems.

The ADDIE model is a synonym to ISD referring the major processes that comprises the ISD: Analysis, Design, Development, Implementation and Evaluation (ADDIE).

“The ADDIE model is a generic, systematic approach to the instructional design process, which provides instructional designers with a framework in order to make sure that their instructional products are effective and that their creative processes are as efficient as they can possibly be.”

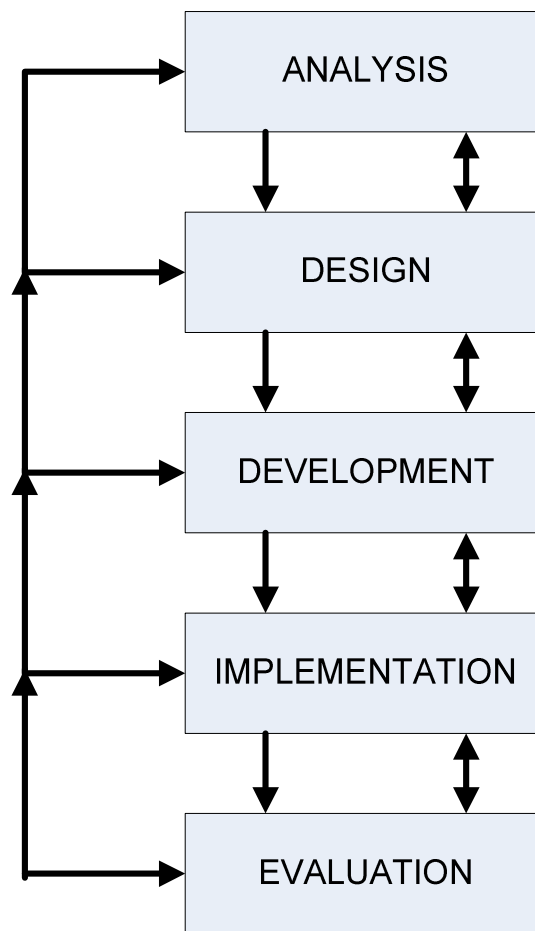
[Dick et al., 2001]

One reason to select the ADDIE model approach is that this kind of training development is also used in relevant standards from the National Institute for Standards in Technology (NIST). The NIST published a series of standards on the topic of Information Technology Security Awareness and Training Programs. These standards provide guidelines to develop training programs in the field of Information Security Awareness. They are focusing on the IT

Security aspect rather on the psychological aspects of social engineering but it is definitely related. [NISTa, 2009], [NISTb, 2003]

The United States Army uses the ISD approach, respectively the ADDIE model approach to develop their trainings.

Figure 3.1 below shows how each step of the ADDIE process depends on the outcome of the step before. The last step, evaluation, feeds the information to improve all other steps.



**Figure 3.1.:** ADDIE process model [Hodell, 2006]

### 3.2.1. Analysis

Analysis is the first step and the foundation for all following steps in the ISD. During this phase the actual problem is defined. This definition of the problem consists of the source and the possible solution to it.

According to Hodel [2008] these parameters have to be clarified:

- if a problem exists that can be appropriately addressed by training
- what goals and objectives the training should address
- what resources are available for the project
- who requires the training and their needs (population profiles)
- all additional data needed to successfully complete the project

### 3.2.2. Design

The design phase takes the output from the Analysis, to plan a training strategy for the development. This might include writing a target population description, conducting a learning analysis, writing objectives and test items, selecting a delivery system, and sequencing the instruction [McGriff, 2000]

The Design phase is the real heart of the ISD process. [Hodel, 2009] and these are some action points in this step:

- prepare instructional objectives
- develop instructional evaluation techniques and tasks
- develop a program evaluation plan
- develop the sequence and structure of the course
- prepare logic and objectives maps
- determine and prepare draft copies of necessary materials

### 3.2.3. Development

The purpose of the development step is to create a training schedule and training material. The actual instructions are developed including all media that will be used in the training as well as the documentation.

In this phase the designer has these action points [Hodel, 2009]:

- prepare all participant and instructor materials for the course
- prepare all support materials including audio, video, and other media
- program any computer-based materials
- field or beta test the project

### 3.2.4. Implementation

This phase refers to the trainings delivery. The training could be classroom based, lab based, or computer based. The purpose of the Implementation step is the effective and efficient delivery of instruction. The knowledge transfer is the most important parameter.

### 3.2.5. Evaluation

The effectiveness and efficiency of the implementation are measured. It is a continuous process that feeds all steps with new input to improve the training.

The designer of the training, in this phase, is expected to [Hodel, 2009]:

- confirm that all subject matter is correct and reviewed
- consult with stakeholders to ensure adherence to established project goals
- adhere to the design plan and procure sign-off on all critical design elements
- review and act on all evaluations from participants, facilitators, and other end users of the project



- ensure quality control of the process by constant and thorough evaluation of all remaining project elements

### 3.2.6. Information Security Awareness Programs

Information Security Awareness programs have to cover a lot more than just Social Engineering attacks they have usually a wide spectrum of content to teach.

The current list from NISTa [2009] 800-16 of topics in a Information Security Program includes:

- Roles and responsibilities in information security
- Ways to protect shared data (e.g., encryption, backups)
- Examples of internal and external threats (e.g., social engineering, hackers)
- Malicious code (e.g., viruses, worms)
- Security controls
- Ways to recognize an information security incident
- Principles of information security
- Passwords
- Social engineering
- Data backup and storage
- Computer viruses and worms
- Incident response
- Personal use and gain
- Privacy
- Personally identifiable information (PII)
- Identity theft
- Internet surfing
- Inventory control
- Physical security
- Spyware
- Phishing

- Scams and spam
- Mobile devices (e.g., laptops, PDAs)
- Portable storage devices (e.g., CDs, USB drives)
- Remote access
- Copyright infringement and software piracy
- Use and abuse of e-mail
- E-mail do's and don'ts
- Peer-to-peer file sharing threats
- National security information/systems, where applicable

Despite the fact that SE is just one point, the strategies to build up awareness can be used to enrich the development of the trainings concept. The importance of awareness in regards to Social Engineering is mentioned in the chapter "Trainings concept".

Some authors Equation [Granger 2001; Berti and Rogers 2002; Gragg 2002; ; Dolan 2004; Hoeschele et al. 2005; Rogers 2006] have professed that Education, Awareness and Training (EAT) are the right way to build a SE centric awareness program.

Roper et al., [2006] has enhanced the EAT approach by the factor of Motivation. Motivation is a key element on the central route of information processing in the ELM. Therefore this model is taken into consideration on the training concept development.

This enhanced approach is referred as TEAM. TEAM is an acronym for training, education, awareness and motivation.

### 3.2.6.1. Training

The proper training ensures that people have the skills, knowledge, and information they need to perform in their function (e.g. Finance clerk).

### 3.2.6.2. Education

Education enables people to understand the security principles, policies, purposes, and rationales. After that they have the ability to make intelligent contributions to the awareness program quality.

“If you think of training as helping people know the who, what, when, and where of security tasks, education can be seen as getting them to understand why.” [Roper et al., 2006]

According the ELM Motivation and Ability are key elements in the ELM on the “central route”. Education raises the ability of people to process information on the “central route” of the ELM.

### 3.2.6.3. Awareness

It is of utter importance to raise the level of awareness so that people are aware of threats to IT Security.

“Increasing awareness involves promoting the probability that people will consider security as they go about their work and personal lives by building a recognition of the reality and presence of the threat so countermeasures are recognized as necessary. When security educators use this term, they often mean awareness of a threat.” [Roper et al., 2006]

Awareness about the “simple cues” used in the ELM helps people so they will not process information on the peripheral route.

### 3.2.6.4. Motivation

Motivation plays a key role for the success of the IT Security program. The best training may fail if people are not motivated to apply the learned knowledge, skills and attitudes.

“At this point, we have people who are able to do their job for security (training), understand what they're doing (education), and think about doing it when it counts (awareness). Now we have to get them to do it.  
[Roper et al., 2006]

Increasing the Motivation is one factor that helps people to examine the manipulative information more carefully.

## 4. Trainings concept

### 4.1. Introduction

The use of highly sophisticated technology does not combat this crime. Due to the human factor in this type of crime it is more efficient to provide training for users. This training will help to raise the level of awareness and teach the necessary skills to be almost immune against Social Engineering attacks.

“Social engineering is a kind of attack, which cannot be remedied by technological measures, as it targets the weakest link in an organization security chain, the human factor.”

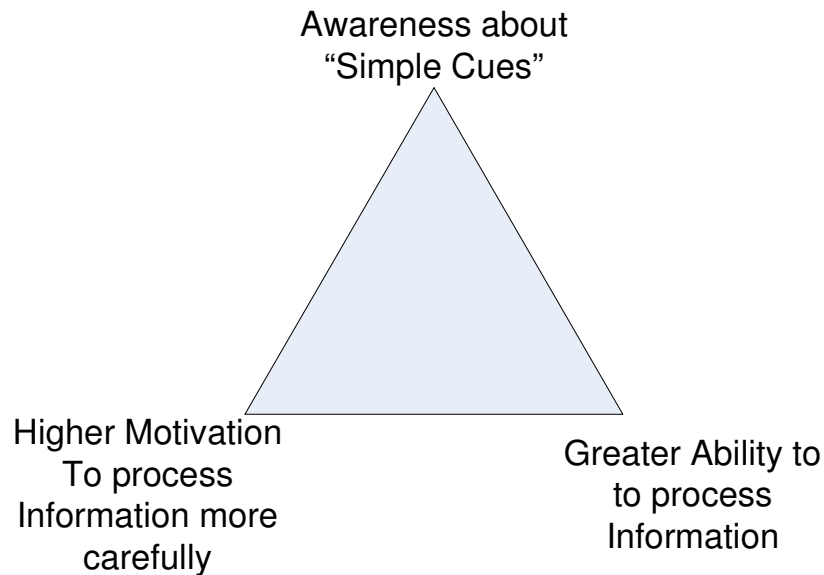
(...) “The most important step in doing so is to raise security awareness and keep it at a high level through continuous training, whereas purely technological countermeasures can be seen only as supplement.”

[Böck, 2007]

The findings in the psychological analysis chapter have identified some key factors. These key factors are the foundation for any kind of training program.

One factor is that people processing information on the central route are less persuadable. But they have to be motivated and they have to be able to process the information.

The question of how to deal with the simple cues that lead people on the peripheral route arises. The answer to it is awareness. Studies from Booth-Butterfield [1996] have shown that people who are aware of an attack on their beliefs, are less likely manipulated in their attitude.



**Figure 4.1.:** The three key elements of the training concept

The following chapter contains the trainings concepts to prevent Social Engineering attacks in the context of Cyber Crime. This training concept is developed on the ISD learning theory. But due to the fact that Social Engineering is also an important topic in Information Security literature, this area is also considered. Especially the NIST [2008, 2009] publications and the TEAM [Roper et al., 2006] approach.

The definition of the trainings concept does not provide a full training. It is summarizes the training course and its key features. Below is the definition from the online business dictionary.

"Summary of a training course or program that highlights its key features such as type of training, presentation environment, teaching techniques, and the benchmarks by which the learning performance will be measured." [WEB 1, 2009]

The idea is to create a kind of universal training concept that can be used like a pattern to develop a context based training. For instance to develop a SE training in the financial industry.

## 4.2. Concept

Following the ADDIE methodology, the first step is to answer seven key questions. This is part of the analysis phase in ADDIE. These questions are [Hodell, 2006]:

1. What is the need?

The need is to create awareness about the risk of SE attacks in the context of Cyber Crime.

2. What is the root cause?

If information with persuading content is processed on the peripheral route of the ELM then the persuasion is more likely to be successful.

3. What are the goals of the training?

The goals of the training are to create awareness about SE attacks and raise the level of Motivation and Ability in order to process information on the central route of the ELM.

More details on the objectives are under the point "Training plan".

4. What information is needed, and how is it gathered?

Information is gathered conducting a survey.

5. How will the training be structured and organized?

6. How will the training be delivered?

7. When should training be revised?

Questions 5 and 6 are going to be answered in "Trainings Plan" section.

Question 7 is going to be answered in the "Post-Training Phase" section.

### 4.2.1. Trainings sample scenario

In order to make the key elements of the trainings concept more visual and give good examples a fictive company is going to be used. This company is working in the field of biomedical research and has about 700 employees. The company name is Biocell.

The management has the concern that sensitive information could be stolen. Embedded into an IT security awareness program a session about Social Engineering is planned.

The duration for this program will be 2 days in a separate training center. The company sends groups with 20 people each to this training. The groups are mixed of men and women.

### 4.2.2. Pre-Training Phase

This is reflected in the Analysis part of the ADDIE approach. Important in this step is to identify the prior knowledge of the participants in regards to SE. A survey helps to create an even more specific content of the course.

The survey has to contain the following:

- prior knowledge about SE
- identify the level of motivation
- identify the level of ability to process an information request
- identify awareness level about "simple cues"

The results on the first question have an influence on the starting point in terms of knowledge. For instance if the course is going to be held for an IT Security department there is no need for an introduction of the importance of Information Security.

The analysis of the psychological aspects have clearly shown that the factors motivation and ability factors are very important for the success of the course. The results of this questionnaire can identify the degree of need for the course.

#### 4.2.2.1. Sample survey:

The sample survey on the next page should be done prior to the training. The time frame depends on the number of participants. It is essential for the training success to incorporate the result into the development phase of the training.



**Questioner on the Social Engineering awareness program**

Name (blank is anonymously): \_\_\_\_\_

Date (YYYY-MM-DD): \_\_\_\_\_

**Question 1:**

Can you associate something with the term “Social Engineering” in the field of Information Security?

☐YES ☐NO

If the answer is yes please write about you knowledge:

---

---

**Question 2:**

Do you think that information and the security of information is important in your company?

☐YES ☐NO

If the answer is yes please explain why you think it is important.

---

---

**Question 3:**

If you receive an email, fax, telephone call, or chat window from your boss requesting sensitive information, which of the following would you process with double checking?

- ☐FAX
- ☐TELEPHONE CALL
- ☐EMAIL
- ☐CHAT WINDOW

Please check all that applies.

**Question 4:**

You get a telephone call from someone you do not know and the person identifies himself as IT helpdesk assistant. The person asks you to change your password according to the new IT Security guidelines that you should receive in an email.

Would you give him your password?

☐YES ☐NO

Are you going to change your password according to the new rule?

☐YES ☐NO

What else would you do?

---

---

Comments:

---

---

Thank you for you input.

**Figure 4.2.:** Sample Pre-Training Questioner

### 4.2.3. Trainings plan

The trainings plan consists of the objectives, design matrix, instructional plan, program overview and lessons. These build the training plan and at each part the examples based on the sample scenario are provided.

#### 4.2.3.1. Objectives

Objectives are an integral part of the ISD respectively the ADDIE. They are used as a foundation for the design process.

“Objectives are the conceptual and operational framework that inspires and sustains the instructional design process. Without them, education and training have little more than content and contemplation to assure quality. From the perspective of an instructional designer, the art of writing objectives is a fundamental and irreplaceable skill that requires nurture, reflection, and practice for competence.” [Hodell, 2006]

Based on the ISD approach in the context of the Trainings Sample Scenario these are example objectives:

“Knowing the weakness of electronic communication (e.g. fax, email) in regards to Authenticity of the sender, the user has the ability to make a decision to proceed or drop the message, based on the content of the message. ”

“Knowing the importance of Information Security, the user is motivated to process sensitive information with due care.”

These are just examples of the objects that support the key elements of the trainings concept.

### 4.2.3.2. Design matrix

A design matrix is used to visualize the course or session.

“The design matrix provides a framework or skeleton for the course. You will then “put the meat on the bones” as you make decisions about methods and materials and prepare your instructional plan.”

[Lawson, 2009]

The design matrix consists of 4 parts: duration, content or learning points, methods or activities, and materials or aids.

#### 4.2.3.2.1. Sample design matrix:

The design matrix (Figure 4.3) shows the key lectures used in the trainings course. It is a rough sketch of the training. It helps to identify and sequence content subtopics, estimate the amount of time, selection of the methods, and identify the training material that is required. The lectures are not in sequenced at that point of the training development.

Duration	Content/Learning Points	Methods/Activities	Material/Aids
30 minutes	Internal SE attacks	Video	Beamer, Laptop
20 minutes	Introduction to Cyber Crime and SE	Lectures, Presentation	Beamer, Laptop
60 minutes	Internal SE attacks – practical Example	Role play	Video camera, role script
30 minutes	Awareness about “simple cues”	Lectures, Presentation	Beamer Laptop
20 minutes	Internet SE: Quiz	written test: multiple choice	Paper, pen
20 minutes	External SE attacks	Video	Beamer, Laptop
60 minutes	External SE attacks – Practical Example	Role play	Video camera, role script
30 minutes	Technical knowledge: Email, Fax, Chat, Internet	Lectures, Presentation	Beamer Laptop

30 minutes	Technical knowledge: Exercise	Computer based Exercise	Computer
20 minutes	External SE: Quiz	written test: multiple choice	Paper, pen
20 minutes	Company specific Policies and Procedures	Lectures, Presentation	Beamer Laptop

**Figure 4.3.:** Design Matrix as foundation for the Instructional Plan

The Design Matrix is used in the “brain storming” phase of the course development. It helps the developer to collect ideas on what lessons should be part and it is a starting point for the formal Instructional Plan.

#### 4.2.3.3. Instructional Plan

The instructional plan has all the information that is required to deliver the training. It has all the lectures and organizational points in a sorted manner. Whereas the design matrix is like a mind mapping tool, the instructional plan is the outcome of the lecture selection and a teaching method.

This instructional plan is developed based on the sample company but it can be easily adapted to fit other focus group (e.g. Governmental Organization).

An instructional plan consists of two parts [Lawson, 2009] :

1. The Program overview
2. The instructional guide

#### 4.2.3.3.1. Program Overview

##### 1. Title

Awareness training to prevent Social Engineering Attacks

##### 2. Course Description

This course provides participants with the knowledge, skills and techniques to detect and prevent Social Engineering attacks.

##### 3. Learning Outcomes

Participants will learn:

- what Social Engineering is
- how Social Engineering works
- the different ways of Social Engineering in order to detect it
- how to act in a Social Engineering attack
- the company perspective on Information Security

##### 4. Length

The course is designed as two full-day sessions.

##### 5. Format/Methodology

The course is classroom based and uses presentations and experiential activities. Such activities are: role plays, case studies, group discussion, quizzes, videos, and computer based exercises.

##### 6. Audience

For all employees of the company. Maximum twenty participants

##### 7. Participant Preparation

Pre-course questionnaire: The questionnaire is designed by the trainer and sent to each participant prior to the course. Details on the survey are discussed in the chapter "Pre-trainings phase".

## 8. Instructional Materials and Aids

### a. Document list

- Participant workbook containing reference materials and learning exercises
- role plays
- quizzes
- IT security policy papers

### b. Equipment list

- flip chart
- beamer
- 21 computers with internet access

### c. Media List

- videos about Social Engineering attacks

## 4.2.3.3.2. Instructional Guide

The instructional guide contains the training schedule. These lessons are grouped in two days following the requirements of the sample training for the biomedical research company. In addition to the schedule each lesson is explained into details. These details include the following information:

- Content of the lesson
- Method and activity
- Didactics background
- Social Engineering prevention factor

The content of the lesson is a description of what this lesson consists. Under method and activity the information on how the lesson is delivered is discussed.

The point didactics background tells about the relevant learning theories behind the lesson and what learning type is approached. Learning types<sup>6</sup> are audio, visual, tactile and kinesthetic.

The Social Engineering prevention factor tells about the why this lesson helps to prevent SE attacks in the context of Cyber Crime. In other words how this lesson delivers the key elements in the trainings concept.

The next pages (Figure 4.4) (Figure 4.5) show the actual time table of the lessons. The lessons have been grouped by days.

---

<sup>6</sup> Suite101, a web site where authors can publish their articles,  
[http://newteachersupport.suite101.com/article.cfm/learning\\_styles\\_in\\_the\\_classroom](http://newteachersupport.suite101.com/article.cfm/learning_styles_in_the_classroom) (accessed December 29, 2009)

**Time table first day**

Time	Duration	Content/Learning Points	Methods/Activities	Material/Aids
9:00-9:15	14 minutes	Organizational: e.g. Course begin, breaks,...	Lectures	Flipchart
9:15-10:00	45 minutes	Introduction round	Small group discussion	n/a
10:00-10:15	15 minutes	Questioner	Paper based questioner to fill in	Questioner
10:15-10:45	30 minutes	SE attacks	Video	Beamer, Laptop
10:45-11:00	15 minutes	Break	n/a	n/a
11:00-12:00	60 minutes	Introduction to Cyber Crime and SE	Lectures, Presentation	Beamer, Laptop
12:00-14:00	120 minutes	Lunch Break	n/a	n/a
14:00-15:30	90 minutes	SE attack role play	Role play	Role script
15:30-16:00	30 minutes	Analysis role play	Group work	Posters
16:00-16:15	15 minutes	Break	n/a	n/a
16:15-16:40	25 minutes	Presentation of posters	Presentation and discussion	Posters
16:40-17:00	20 minutes	Awareness about "simple cues"	Lectures, Presentation	Beamer, Laptop
17:00-17:20	20 minutes	Closing and feedback	Round table	n/a

**Figure 4.4.:** The Time table of the fist trainings day



**Time table second day**

Time	Duration	Content/Learning Points	Methods/Activities	Material/Aids
9:00-9:15	14 minutes	Organizational: e.g. Course begin, breaks,...	Lectures	Flipchart
9:15-10:00	45 minutes	Technical knowledge: Email, Fax, Chat, Internet	Lectures, Presentation	Beamer, Laptop
10:00-11:00	60 minutes	Technical knowledge: Exercise	Computer based Exercise	Computer
11:00-11:30	30 minutes	Company specific Policies and Procedures	Lectures, Presentation	Beamer Laptop
11:30-13:30	120 minutes	Lunch Break	n/a	n/a
13:30-14:00	30 minutes	"The Fax Experiment"	Lectures, Presentation, voting, group discussion	Beamer Laptop
14:00-14:20	20 minutes	SE: Quiz	written test: multiple choice computer based	Computer
14:20-15:00	40 minutes	Tools and techniques to prevent SE attacks	Lectures, Presentation	Beamer Laptop
15:00-15:15	15minutes	Break	n/a	n/a
15:15-16:00	45 minutes	Reflection of the learned content	"letter to me"	Paper, pen
17:00-17:20	20 minutes	Closing and feedback	Round table	n/a

**Figure 4.5.:** The time table of second trainings day

#### 4.2.3.4. Lessons

##### 4.2.3.4.1. Introduction Round

###### **Content of the lesson**

People are asked to introduce themselves. This includes their name, years in the company, and current position.

###### **Method and activity**

Small Group discussion asking every person

###### **Didactics background**

Such an introduction round helps to break the ice and shows the population profile of the course.

###### **Social Engineering prevention factor**

This lesson helps the course in general.

##### 4.2.3.4.2. Questionnaire

###### **Content of the lesson**

People are asked about their prior knowledge on Social Engineering, Information Security and their expectations from the course. This is an aid to the pre-training questioner and should fill the gaps if the results from the pre-training questioner were not satisfactory.

The questions should be similar to the pre-training questionnaire but there should be a possibility for open answers. Furthermore the questions should be adjusted to fit the local training requirements (e.g. Target group is IT Management)

Some sample questions could be:

Do you know what to do with information requests from unknown persons?

Do you know what Social Engineering is?

Given an email where the sender is someone you know. Do you trust the content?

Do you know your companies IT Security policy and procedures in regards to information handling?

**Method and activity**

The participants receive a paper based questionnaire and pens. They are asked to the questions in 15 minutes and to work alone. Furthermore they are told, that the questioner is anonymous but if they like they can provide their names.

Another method that could be considered is to let the participants fill in an online questionnaire.

**Didactics background**

The result of the questionnaire can provide the current level of knowledge. Furthermore it gives input for fine tuning the course content. For instance if they have already had an incident with Social Engineering.

**Social Engineering prevention factor**

The output of the questionnaire raises the course quality.

**4.2.3.4.3. Video “SE Attacks”****Content of the lesson**

A video about SE attacks is shown. The content of the video has to consist of some key elements:

Show practical examples of a successful SE attack via:

- telephone
- email
- a Social Networking site

**Applied on the Sample Scenario****Via Telephone**

The first scene of the video shows Mr. Maier who works in the research department of Biocell, receives a phone call from Ms. Berger from the company Chemosan. Chemosan is big competitor of Biocell. She pretends to be Chief of the research section and she wants to have an actual dump from the research database.

Mr. Maier is shocked and he refuses to give out this sensitive information.

Ms. Berger pretends to be curious that Mr. Maier is not aware of the upcoming merger between Biocell and Chemosan. Furthermore she wants to have this information beforehand and she offers Mr. Maier a good position in Chemosan.

Mr. Maier agrees and sends her the file. Mr. Maier realizes too late that he was a victim of a Social Engineering attack.

#### Via Email

The next scene in the video shows Mr. Sanders in the logistics department who receives an email from a friend. At least the senders address seems to be his friend.

Based on the senders email address he trusts the content of the email and opens the attachment. By doing this a Trojan Horse program is installed on his PC. The Trojan Horse sends all data from Mr. Maier's PC to the attacker.

#### Via Social Networking Site

The last scene in the video shows Ms. Chelsi from the finance department. She is enjoying the Social Networking site Facebook. All of a sudden a very good friend of hers wants to chat with her and send her a link to download a "very cool" astrology program.

Ms. Chelsi trusts her friend and downloads the program. She is not aware that her friends account has been hacked.

The program seems not to work in the field astrology but provides a backdoor to Ms. Chelsi's PC. This backdoor is afterwards used to steal money from the company by faking Electronic Banking logins to hijack the Transactions codes. [Behrens, 2009]

### **Method and activity**

From a laptop using a beamer a video is displayed. The video length is 15 minutes and it is shown two times. The second time the participants are ask to take notes.

In order to make this video based lesson successful the following should be taken into consideration:

"Introduce the video by explaining why you are showing it and what the video is about, including a brief description of the setting and characters.

Also, prepare participants for anything unusual or unique in the video."

[Lawson, 2009]

“Tell the participants what to look for as they view the video. In fact, it is a good idea to prepare a list of specific questions related to the video and create a handout or post the questions on a flip chart. The entire group can address each question, or different questions can be assigned to specific individuals or groups of participants. This technique will make the participants much more attentive because they know they will have to report their observations to the entire group.” [Lawson, 2009]

“Show the video in its entirety; then lead a discussion based on the questions or points the participants were to look for.” [Lawson, 2009]

### **Didactics background**

Cognitivism is the relevant didactical theory: To see and understand the content of the video. Audio and Visual learning types are approached.

### **Social Engineering prevention factor**

The video lesson raises the level of awareness. The awareness of the “simple cues” in terms of Information processing on the peripheral is crucial for the success of the training.

## 4.2.3.4.4. Introduction to Cyber Crime and SE

### **Content of the lesson**

During this lesson a presentation is shown using a beamer. The presentation has to have the following content:

- Definitions of Social Engineering and Cyber Crime
- Scope of the problem
- Basics about information security
- How Social Engineering works
- How to detect a Social Engineering attack
- Show the different kinds of Social Engineering attacks (e.g. FAX, Email, Telephone, Social Networks,...)
- 

The participants should learn the basic knowledge of the domain Social Engineering and Cyber Crime. The scope of the problem has to show the dimension of the problem in

numbers and how it could harm the company. The basic knowledge of information security lays the foundation for the lesson “Company specific Policies and Procedures”.

“How SE works” and “How to detect a SE attack” are containing the basic knowledge about the psychological pattern and conditions (e.g. time pressure). The last point about the different kinds of SE attacks gives an overview on the technical aspects of SE attacks.

### **Method and activity**

With the usage of a laptop and beamer, the teacher presents a set of prepared slides on the content. The participants are asked to make notes and to ask questions in the end of the presentation.

### **Didactics background**

The relevant learning theory behind lectures is Behaviorism and Cognitivism. The slides of the presentation should be designed in a way that both the visual and the audio type are approached.

### **Social Engineering prevention factor**

The content of this lesson raises the level of awareness about the topic in general.

Furthermore it helps to give people the ability to deal with information. That means in particular to strengthen the ability to process the process information on the central router in regards to the ELM.

#### 4.2.3.4.5. SE attack role play

### **Content of the lesson**

The participants should play a role play to gain the experience how SE attacks are working. Randomly the participants are split up into pairs. The role play has two roles, the attacker who would like to get the sensitive information, and the victim who has the access to the information.

Based on the sample company Biocell the role play script (Figure 4.6) on the next page can be used. In the role play Dr. Huber plays the attacker and Dr. Maier plays the victim.

Background story: Dr. Maier works in the research section of Biocell. He works there for several years and he has a very good reputation. Due to his good reputation he has full access to all research data on the database. Dr. Huber works also in the research section but in a different project team. His database account does not have full access. Both know each other from a chat in the coffee corner. Dr. Maier is reading his emails and all of a sudden Dr. Huber enters his office.

Huber: Good morning – how are you?

Maier: Good morning. Thanks fine. How can I help you?

Huber: Could you help me with the report for the CEO?

Maier: Of course - what can I do you for you?

Huber: Would you mind to provide my quickly your access to the database. I really need this urgently.

Maier: No, for sure not – then you will know my password. Why do you want to have accesses at all?

Huber: I need to write a report for the CEO and therefore I have to have the latest research data. I have already requested more access rights for my account from the IT department. But you know how it is, it will take ages to get them.

Maier: True – the IT guys are lazy.

Huber: You know what: You simply change your password to 12345 and I will let you know once I am done – ok?

Maier: I don't know – better not.

Huber: Come on, you know me. I always helped you.

Maier: Yes, that's true but...

Huber: There is no but. I need this access urgently otherwise I will get a lot of troubles from the CEO and you said you will help me.

Maier: Oh yes the report to the CEO.

Huber: Exactly! If you are not going to help me, I have to tell them and you will be held accountable. You know I know the CEO very well and he does not support such uncooperativeness.

Maier: - no comment-

Huber: Look, its very easy, change your password temporary, afterwards you change it back. Only for today. I will mention you name in the report.

Maier: Ok, I am doing it, wait the password is now 123456. The user is maier1.

Huber: Thanks my friend, I ovn you a coffee.

Epilog: Dr. Huber will leave the company Biocell and start working for a competitor. The data from the research database was very valuable for his new employer. Based on the data from Biocell the competitor had the new vaccine faster on the market. Biocell went bankrupt.

**Figure 4.6.:** Script to a role play to demonstrate a SE attack

This is just an example role playing script (Figure 4.6). The important elements of every role play in regards to this trainings concept are the practical application of manipulation techniques in a real world scenario. In this case the situation is based on the sample company Biocell and the manipulation techniques used in the conversation are:

- Authority

The CEO is important he needs the report

- Commitment

The commitment to get help on the report.

- Liking

Wording: e.g. my friend

- Fear

Wording: "You will be held accountable!"

"Need for Help" and "time pressure" can be also considered as manipulation techniques.

Note from the Author: The role play is in the opinion of the Author an essential part in any kind of SE prevention training as it helps people to gain understanding of the situation. These situations are sometimes very trivial.

### **Method and activity**

Out of the 20 course participants 10 pairs are grouped to perform the role play. The role play is performed in two rounds. In the first round, both the attacker and victim have a script. They are asked to play according to the script. In the second round the attacker has the script and the instructions to act independently to gain access to the information. The victim has no script and should defend the information. The scripts are handed out to the pairs with the instructions to make notes during the second round of the role play.

The Questions: "How would you have reacted?", "What manipulation techniques would you recognize?" and "What would be a good defense?", should be answered.

The material consists of the pre-made role script, notebook and pens.



**Didactics background**

Constructivism and cognitivism is the main learning theory behind this lesson. The participants develop the knowledge by themselves. Role plays in an instructional strategy seems to facilitate more the active construction of meaning. [Wilson, 1997].

The audio, visual and tactile learning types are approached.

**Social Engineering prevention factor**

Through the experience in the role play people will be more aware of the manipulation tactics. Furthermore they are more motivated to process the information more carefully as they have made the experience how easy it is to be a victim.

Role plays are a good method to promote understanding of the content and gain inside knowledge of the different perspectives:

“An effective role play promotes affective, cognitive, and behavioral learning. Participants practice the skills taught, demonstrating their knowledge and understanding of the content through their application in the role-play situation. They also have an opportunity to gain insight into their own behavior.” [Lawson, 2009]

**4.2.3.4.6. Analysis of Role Play****Content of the lesson**

Based on the notes from the former lessons the participants are asked to make posters. The posters should contain their findings in regards to SE.

Furthermore they are asked to find other examples for SE attacks.

**Method and activity**

Poster making in small groups of 4 people each. Posters in flipchart size and pens are provided by the teacher.

### **Didactics background**

This activity is based on cognitivism and also has a creative part that would more relate to constructivism. The course participants will reflect their knowledge about SE by writing down the new information will have a learning effect.

The lesson approaches the audio and visual learning type.

### **Social Engineering prevention factor**

The lesson supports the course in general by making the knowledge more visual and concrete.

## 4.2.3.4.7. Presentation of Posters

### **Content of the lesson**

The participants present their posters to the others. During the presentation questions are answered.

### **Method and activity**

Presentation of the posters from the small groups and discussion.

### **Didactics background**

Sharing the findings of the individual groups with the others will have a brainstorming effect.

### **Social Engineering prevention factor**

The lesson helps to raise the level of awareness among the group.

#### 4.2.3.4.8. Awareness about “Simple Cues”

##### **Content of the lesson**

During this lesson the teacher is going to show some “simple cues” of the ELM model in regards to SE attacks. Each “simple cue” will be explained and afterwards presented in a meaningful content.

Most important is to set different “simple cues” into a realistic situation. This situation should be customized to the environment of the audience. In case of the sample training for the company Biocell the following examples are useful:

##### **Email based SE attacks**

Taking into account that email plays an important role in the internal and external communication of the company Biocell. The following examples will help the participants to gain understanding of use of “simple cues” in regards to SE attacks.

Simple Cue	Example
Liking	You receive an email from a friend. The content of the email is a document attachment. As you trust your friends sender address you open the attachment. This causes the installation of malicious software (e.g. Computer Virus)
Authority	You receive an email from the IT department. In this mail you've been ask to change your password due to a IT Security check. After the password change you should open a web site to verify that the IT Security check is done. The email contains the link. The links seems to trustworthy as it seems to be under the domain biocell.com. After clicking the link your computer stops working. You have been a victim of a cross site scripting attack.

Phone based SE attacks

Telephones as way of communication are still an important factor when it comes to SE attacks. The way how telephones operate have changed, e.g. the usage of Voice over IP, but the tactics are the same.

## Simple Cue    Example

**Reciprocity**    You work as a secretary in the front office. During lunch time you get a call from a women that appears with an internal extension. She pretends to be new in the office and she would like to know if she can send her the latest organizational chart. Furthermore she says that still has no official email address but she will be able to receive this on her private email account.

PC based SE attacks

PCs are part of almost all workplaces in Biocell. Therefore its important to mention the influence of messages generated by malicious programs in regards to SE.

## Simple Cue    Example

**Fear**    A user gets a pop up window on the screen. This pop up windows informs the user that the PC is infected and if the users would like to start the antivirus download now. It seems the pop up window has just an ok button to press. After pressing this button a remote access Trojan (RAT) is downloaded to the users PC.

The given example are just a small selection that should show how customization would look like. The integral parts are the combination of the theoretical function of “simple cues” in the information processing and the practical application.

**Method and activity**

With the usage of a laptop and beamer, the teacher presents a set of prepared slides on the content. The participants should ask questions and make comments during the presentation.

**Didactics background**

The relevant learning theory behind lectures is Behaviorism and Cognitivism. The slides of the presentation should be designed in a way that both the visual and the audio type are approached.

**Social Engineering prevention factor**

This lesson will raise the level of awareness on techniques used in SE attacks. These techniques use “simple cues” in regards to the ELM are presented in a customized context in order to make the training more effective. The lesson approaches the audio and visual learning type.

**4.2.3.4.9. Closing and Feedback****Content of the lesson**

A plenum group feedback about the course in general. Remaining questions can be answered.

**Method and activity**

“Round table” activity with all participants. Each course participant should give a small statement about their impression of the first course day.

**Didactics background\**

Feedback increases the course quality.

**Social Engineering prevention factor**

This lesson helps the course in general.

**4.2.3.4.10. Technical Knowledge: Email, Fax, Chat, Internet****Content of the lesson**

The lesson has to contain the basic technical knowledge about modern electronic communication. The level of knowledge is set so, that people without an IT background are able to understand the weaknesses of electronic communication in regards to authenticity.

The main part in this lesson is to show how easy it is to fake the sender, respectively the source of the information in email, fax, chat and on the internet.

Practical examples are given to reach topic. The practical examples are the same used in the lesson “Awareness about Simple Cues” but this time the emphasis is on the technical aspect of the communication.

The lesson provides the technical fundamental for the practical application in the next lesson “Technical Knowledge: Computer Based Exercise”

**Method and activity**

With the usage of a laptop and beamer, the teacher presents a set of prepared slides on the content. The participants should ask questions and make comments during the presentation.

**Didactics background**

The relevant learning theory behind lectures is Behaviorism and Cognitivism. The slides of the presentation should be designed in a way that both the visual and the audio type are approached.

**Social Engineering prevention factor**

This lesson will raise the level of ability in order to process the information on the central route in regards to the ELM. By giving the course participants the necessary technical knowledge how, for instance emails, can be faked, they will be able to handle the information properly.

#### 4.2.3.4.11. Technical Knowledge: Exercise

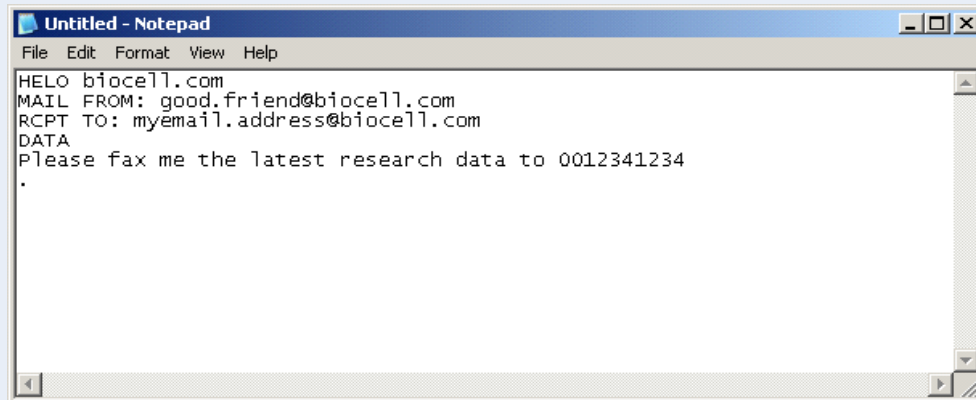
**Content of the lesson**

The technical knowledge gained from the former lesson will be taken to the next level. This will be done by an exercise.

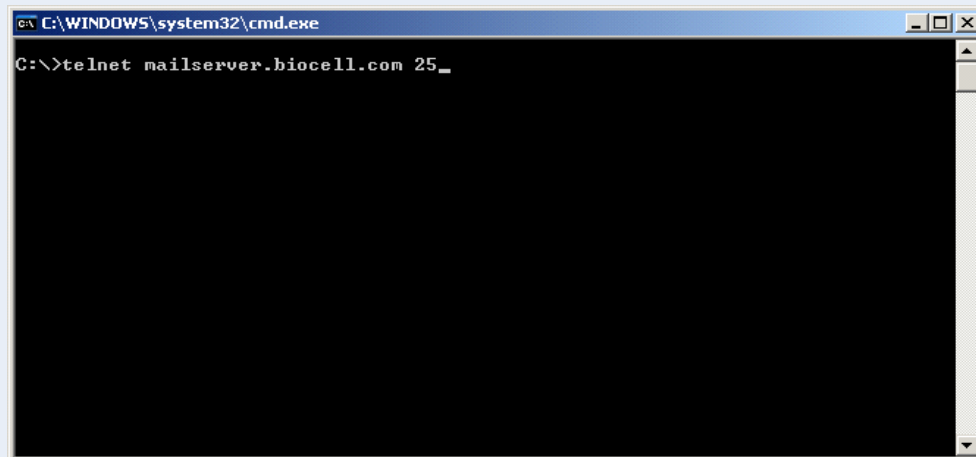
The course participants are asked to use their computers to create a fake email. In the case of the sample scenario the following instructions are given prior the exercise (Figure 4.7).

1. Please log on to your PCs.
2. Open a notepad.
3. Type in as shown in the picture below:

Note: Exchange the [myemail.address@biocell.com](mailto:myemail.address@biocell.com) with your address



4. Open a windows command prompt.
5. Type in as shown in the picture below:



6. Wait until you get a response from the mail server.
7. Copy the content from the notepad to the windows command prompt.
8. You should receive an email with the sender: good.friend@biocell.com

**Figure 4.7.:** Sample instructions for the technical exercise

This is just one example for a technical exercise used in the context of the sample scenario with the company Biocell.

It is from utter importance to provide as many exercises as possible, to show how the different technologies are used to facilitate SE attacks.

### **Method and activity**

The teacher hands out the instructions for the exercises. The course participants are asked to use their computers and follow the instructions. During the exercises the teacher will be available to answer questions and assist in case needed.

### **Didactics background**

The exercises lesson has Cognitivism as background theory but due to the experimental nature it also reflects some ideas of Constructivism learning theories. All learning types are approached by this lesson therefore the knowledge will sink in deeply.

### **Social Engineering prevention factor**

The practical knowledge gained in the exercises will promote the ability, awareness and the motivation.

## 4.2.3.4.12. Company specific Policies and Procedures

### **Content of the lesson**

“Security policies are clear instructions that provide the guidelines for employee behavior for safeguarding information, and are a fundamental building block in developing effective controls to counter potential security threats. These policies are even more significant when it comes to preventing and detecting social engineering attacks.” [Mitnick, 2002].

IT security policy papers in general are very complex to understand for people, that do not deal on a daily basis with IT and IT Security topics. But IT Security policies should contain a SE relevant part.

This lesson takes this part into to training and makes it understandable for the participants.



Applied on the sample scenario with the company Biocell the following from “Policies for all Employees” [Mitnick, 2002] is taken into the course:

- Computer Use
- Email Use
- Phone Use
- Fax Use
- Passwords

And from the “management policies” [Mitnick, 2002] the data classification and Information Disclosure part.

Each policy point should be presented including the location where the latest version of the policy document can be obtained (e.g. internal web site).

#### Sample points from the lecture

Computer use policy: Employees must not disclose any data from the research database to people who have not been identified and have the necessary access rights

Email use policy: Email attachments must not be opened unless the attachment has been cleaned and verified by the Antivirus System.

Phone use policy: Employees may not participate in surveys by answering any questions from any outside organization or person. Such requests must be referred to the public relations department or other designated person. [Mitnick, 2002]

Fax use policy: Prior to carrying out any instructions received by facsimile, the sender must be verified as an employee or other Trusted Person. Placing a telephone call to the sender to verify the request is usually sufficient. [Mitnick, 2002]

Password policy: Employees must never disclose any password. This includes password for data encryption and application access.

Data classification policy: All valuable, sensitive, or critical business information must be assigned to a classification category by the designated information owner or delegate. Such classification is: public, private, internal, confidential.

Information disclosure policy: The company should establish comprehensive procedures to be used by employees for verifying the identity, employment status, and authorization of an individual before releasing Confidential or Sensitive information or performing any task that involves use of any computer hardware or software. [Mitnick, 2002]

The above points are just samples. The whole lesson should make the participants aware of the company specific information handling procedure. Furthermore, part of this lesson is the introduction of an IT Security promoting initiative. The “Information Security Staff Member of the month” initiative will promote employees who have successfully applied the knowledge from this course in the company. At this stage of the course the teacher just introduces the initiative; details will follow in the lesson “Tools and techniques to prevent SE attacks”.

### **Method and activity**

With the usage of a laptop and beamer, the teacher presents a set of prepared slides on the content. The participants should ask questions and make comments during the presentation. A small discussion round on the “Information Security Staff Member of the month” initiative closes this lesson.

### **Didactics background**

The relevant learning theory behind lectures is Behaviorism and Cognitivism. The slides of the presentation should be designed in a way that both the visual and the audio type are approached.

### **Social Engineering prevention factor**

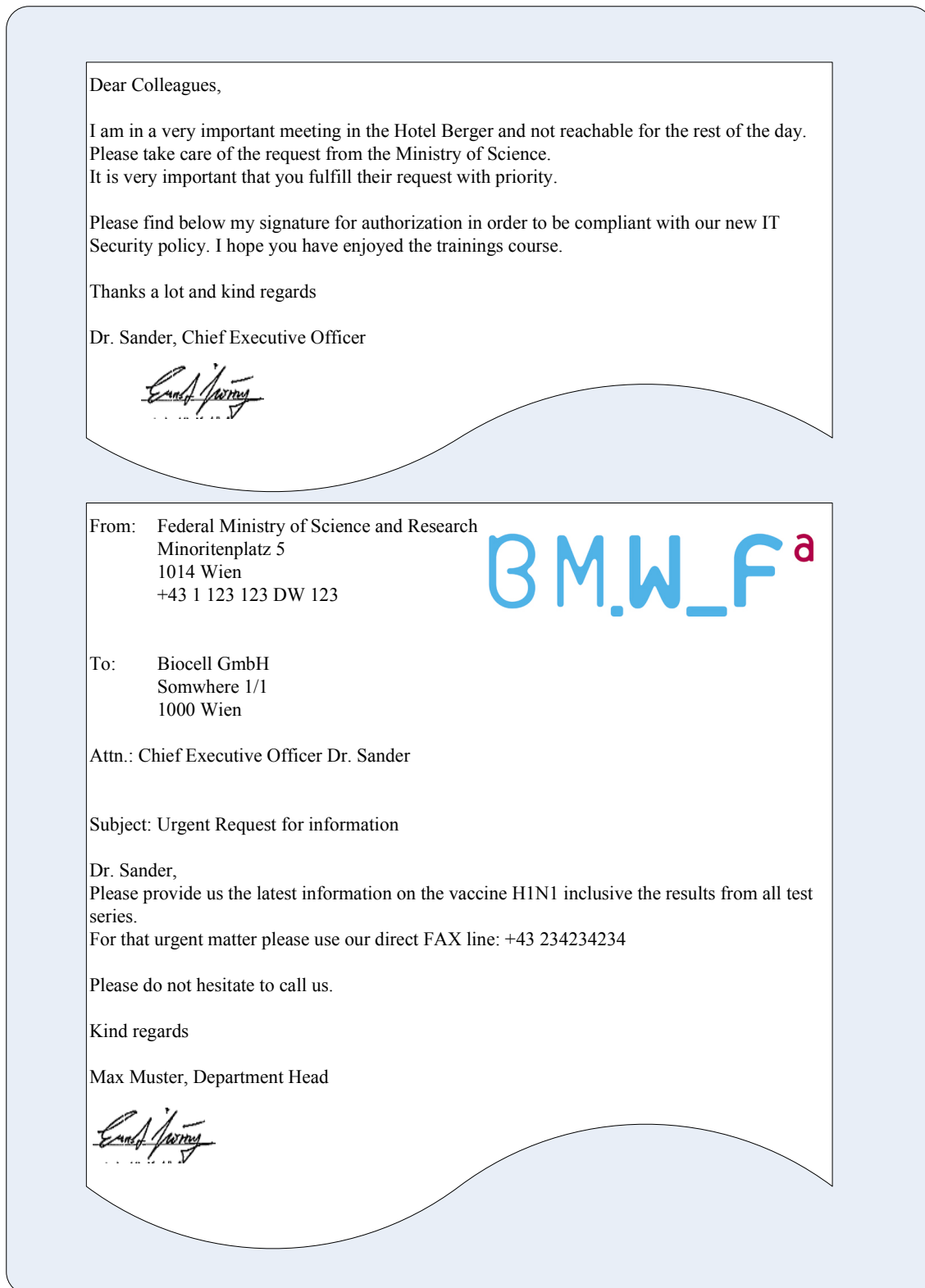
The knowledge how information and information requests are handled promotes the ability of the person to process the persuading information on the central route in terms of the ELM. Whereas the “Information Security Staff Member of the month” initiative should have a positive effect on the motivation.

#### 4.2.3.4.13. The Fax experiment

##### **Content of the lesson**

The fax experiment at this stage of the course has to evaluate the level of awareness. The participants should already have the right skills respectively, the ability to handle the following situation:

Each participant receives two pages received from the fax machine. They are told to read through the fax and build up their opinion how to proceed. The two fax pages (Figure 4.8) are designed in a way to meet the customization requirements from the sample scenario.



**Figure 4.8.:** Two pages of “Fax experiment” The logo is taken from [BMFW, 2009]

After the participants have read the content of the fax, there are two voting rounds conducted. The first is on the question of who would send the information. The second voting round is on the question, who would report this incidence.

The main part of this lesson is the discussion group in which the different elements of this SE attack are elaborated. Each person should make up his or her mind about the situation and the emotions along with it. The teacher has to make them aware to assume always the worst case, say other colleagues are on holiday and the CEO is really in a meeting.

### **Method and activity**

The teacher hands out the copies of the fax. The participants have 10 minutes to read through the fax and make notes. Afterwards two voting rounds are conducted and a group discussion on the topic is started.

### **Didactics background**

Experiments are elements of the Constructivism. The student has to make his own learning experiments. The result of the voting could be an indicator for the success of the training. The course participants should already be trained enough to identify the fax as fake. All learning types are approached.

### **Social Engineering prevention factor**

The fax experiment promotes the ability and the awareness about SE attacks. Especially the awareness of fax based documents.

#### 4.2.3.4.14. SE-Quiz

### **Content of the lesson**

The quiz is multiple choice and based on the course content. The difficulty level of each item should be adjusted in order to be able to pass the quiz without prior studying.

The quiz items should real world scenarios to reflect the company environment. Sample questions in the Figure 4.9.

Question 1: You receive a phone call from an external number. The caller seems to be very friendly and identified herself as Ms. Jones. She says that she is new in the department and currently on an external meeting. She asks you for a favour and transfer her call to the Mr. Berger from the finance department.

Based on the above situation, what will you do?

Check all that applies:

- a. She is new and it is ok to make mistakes. I will transfer her call.
- b. I will tell her that I cannot help her and ask her to call the switchboard.
- c. I will report that case to my supervisor.
- d. I will check in the cooperate phone directory if Ms. Jones exist and try to call her to verify.

Question 2: You have got an USB stick as Christmas present in your post inbox. The company seems to make business with you.

Based on the above situation, what will you do?

Check all that applies:

- a. Use the USB stick normally on my office PC.
- b. Use the USB stick only on my home PC.
- c. Ask the IT helpdesk for advice.
- d. Do not use the USB stick at all.

Question 3: Ms. Berger likes to go with you on a coffee. During the meeting she asks you to help her with a computer problem.

You have agreed to help her but you find out that she does not have sufficient rights with her account to retrieve the information she wanted. She pleases you to help her with your rights.

Based on the above situation, what will you do?

Check all that applies:

- a. Help her only one time to access the information. Do not give her the password.
- b. Let her ask the IT department to provide her the rights.
- c. Try to find out if she has the “need to know”.
- d. Tell her about the importance of Information Security and do not provide access.

**Figure 4.9.:** Sample questions for the Quizzer lesson

Important factor in the construction of the question items is the practical application. Only if the course participants can identify themselves with the situation they would be able to answer correctly.

The content of this lesson can contribute the course quality. If considered for the evaluation of the course in general, the results of the quizzer directly reflecting the level of knowledge already transferred to the participants, at this time.

### **Method and activity**

The course participants are asked to do a computer based quiz. The quiz is computer based with multiple choice questions. They are asked to work alone and no questions will be answered during the time of testing. After finishing they should leave the room.

### **Didactics background**

Tests are an integral part of ISD based course design. The participants will have a chance to test the level of knowledge. The test should be designed to be passable on the low rate in order to motivate the student.

### **Social Engineering prevention factor**

Practical application of the knowledge will promote the level of motivation and raise the ability. Furthermore the learned content can better settle.

#### 4.2.3.4.15. Tools and techniques to prevent SE attacks

### **Content of the lesson**

This key lesson in the course has been to provide tools and techniques to prevent SE attacks. The content of this lesson consists of a summary of ways to deal with manipulation in the background of the company specific environment. In this case the company Biocell.

In the first part of the lesson the employee receives a summary on how to detect SE attacks. Figure 4.10 shows how this should be composed. This approach is based on the recommendation from the European Network and Information Security Agency (ENISA) and suitable for any course customer.

<b>Legitimacy</b>	Does the request seem legitimate and usual? For example, should you be asked for this information, and is this how you should normally provide it?
<b>Importance</b>	What is the value of the information you are being asked to provide or the task that you are being asked to perform, and how might it be misused?
<b>Source</b>	Are you confident that the source of the request is genuine? Can you find a way to check?
<b>Timing</b>	Do you have to respond now? If you still have doubts, take time to make further checks or ask for help.

**Figure 4.10.:** LIST of issues and questions from ENISA [2008]

Legitimacy, Importance, Source and Timing can be abbreviated with the LIST. That simplification of issues and questions will help the course participants to remember.

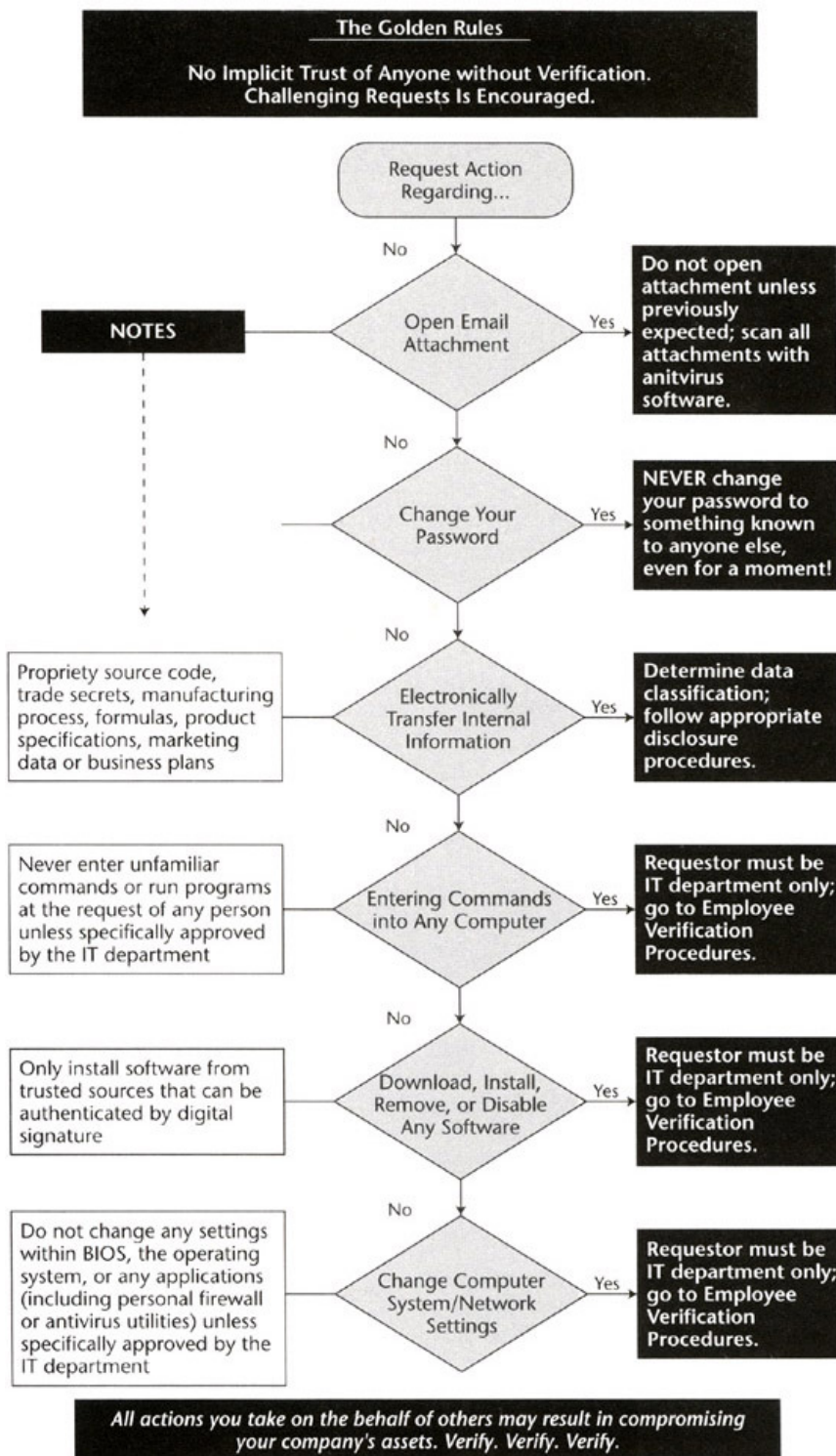
The second part of the lesson deals more in detail on how to deal with a request for action (Figure 4.11) and a request for information (Figure 4.12).

In the lesson the teacher should go through the different kind of requests, for action or for information, and explain each step in the process.

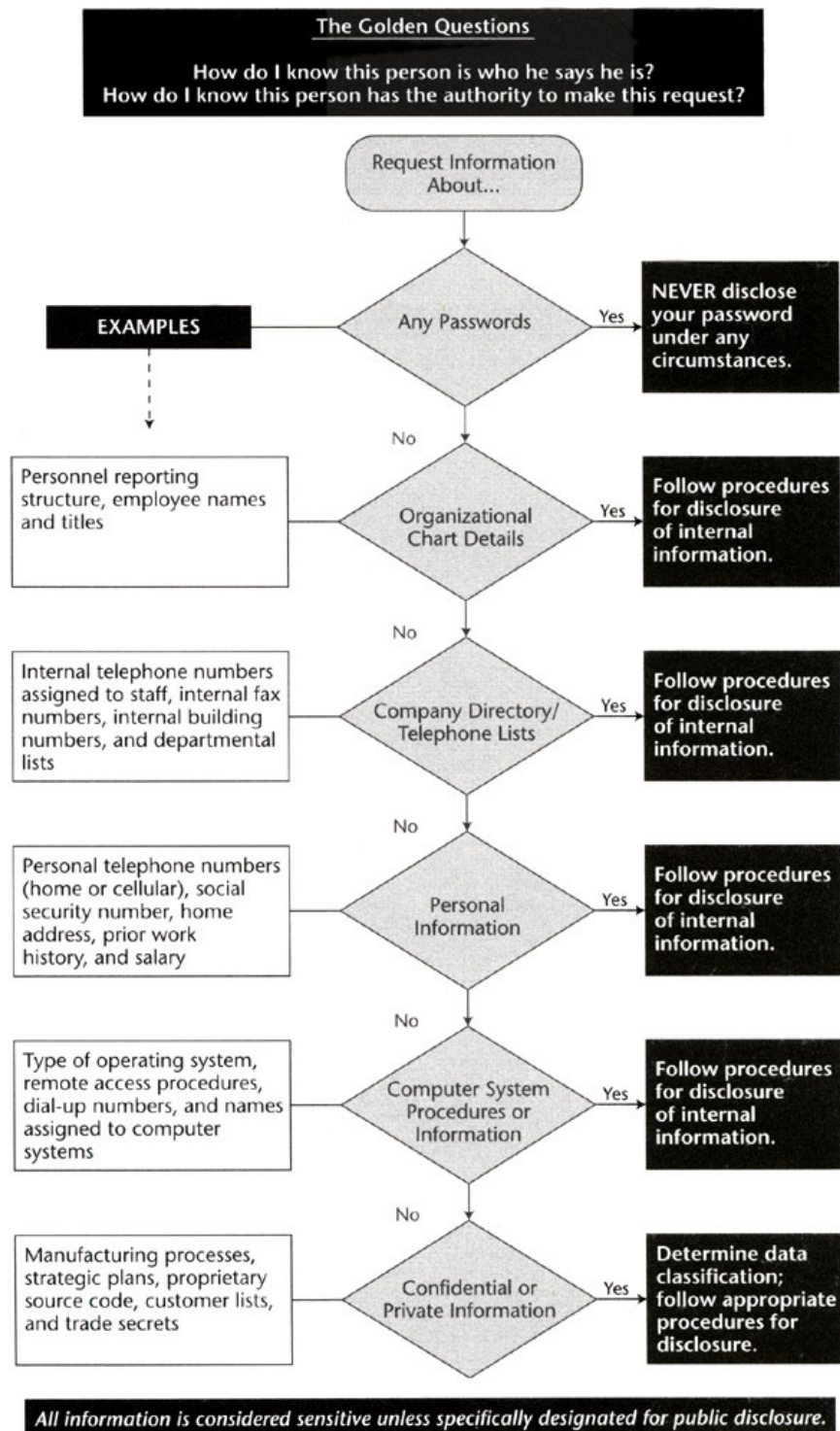
Furthermore the teacher has to bring this theoretical knowledge into a practical context. This could be achieved with examples in every step of the process. Applied on the sample scenario with the company Biocell this would be a good way to explain how the information request regarding a project should be handled:

1. Request Information about the project "Vaccine H1N1"
2. There is no password involved– proceed to step 3.
3. There is nothing about organizational chart details involved – proceed to step 4.
4. There are no telephone list details involved - proceed to step 5.
5. There is no personal information involved – proceed to step 6.
6. There is no information about Computer Systems or procedures involved – proceed to step 7.
7. The information on the project "Vaccine H1N1" has the classification "confidential". The appropriate information handling procedure according the IT Security policy is do not process this information electronically and request access from the project leader and the head of the research department.





**Figure 4.11.:** Request for Information [Mitnick, 2002]



**Figure 4.12.:** Request for Action [Mitnick, 2002]

After this lesson the participants should have enough tools and knowledge to handle information requests according to the company specific policies and procedures. It is important for the success of this lesson to mention the value for the participant in their private

lives when they have to deal with information requests in the context of IT. Good examples would be a phishing email.

The last part of this lesson gives the participants more details on the “Information Security Staff Member of the month” initiative. Herold [2005] underlined that such IT Security promoting programs must communicate the importance of information security outside the formal training sessions.

In case of the sample company Biocell the company is promoting every month a staff member who shows awareness in his or her daily business. For example to report any incidence in regards to SE attacks or to help others to understand the fundamentals of SE attacks.

### **Method and activity**

With the usage of a laptop and beamer, the teacher presents a set of prepared slides on the content. The participants should ask questions and make comments during the presentation. The lesson is more interactive due to the questions that are expected along with figures on the information respectively action request handling

### **Didactics background**

Behaviorism and Cognitivism are the main didactical theories behind this lesson. Audio and visual learning types are approached.

### **Social Engineering prevention factor**

The tools and skill from this lesson are raising the ability to handle information with persuasive context. Furthermore by implementing the “Information Security Staff Member of the month” program the motivation is higher to process request for information and actions more carefully.

#### 4.2.3.4.16. Reflection of the learned content

##### **Content of the lesson**

During this lesson the student should reflect the course content. The teacher has to summarize the key points of the course. Furthermore the teacher should encourage asking questions to ensure that there are not open points to discuss.

The students are asked to write a letter to themselves. The letter should include the knowledge that the course participant has learned from the lessons and the teacher also provides feedback forms to fill in.

##### **Method and activity**

The method called “Letter to me” [WEB2, 2009] is used. Hand out of feedback forms on the course quality in general.

##### **Didactics background**

The letter to me is a method that is based on the constructivism learning theory. While the student is writing the letter to herself, she brings her thoughts and her point of view to paper.

##### **Social Engineering prevention factor**

This lesson does not only supports the course in general but the letter can be used after the training to remember the content.

#### 4.2.4. Post-Training Phase - Evaluation

“Evaluation is more than just a post-course event. Evaluation takes place in every element of the ADDIE model. Designers even need to evaluate the evaluation process. This multidimensional approach to evaluation reflects ISD’s systems approach to instructional design. Not only are the traditional evaluations reflected in learner performance and content

mastery part of the design process, the ISD process itself is reviewed for conformance to best practice throughout the ADDIE elements.” [Hodell, 2006]

Donald Kirkpatrick [1959] introduced a model for evaluating training programs. It is based on four levels (Figure 4.13) and most widely accepted by training developers [Lawson, 2009].

	<b>What</b>	<b>Who</b>	<b>When</b>	<b>How</b>	<b>Why</b>
Level 1	Reaction: Did they like it?	Participants	End of program	"Smile sheet"	Determine level of customer satisfaction; may indicate need for revision
Level 2	Learning: What knowledge or skills did they retain?	Participants; trainer	During, before/after program	Pre-test/post-test; skills application through role plays, case studies, exercises	Identify whether trainer has been successful in delivery of course content and achieving program objectives
Level 3	Behavior: How are they performing differently?	Participants; bosses; subordinates; peers	3 to 6 months after program completion	Surveys; interviews; observation; performance appraisal	Determine extent to which participants have transferred what they learned in the session to the actual work situation
Level 4	Results: What is the impact on the bottom line?	Participants; control group	After completion of Level 3 follow-up	Cost/benefit analysis; tracking; operational data	Determine whether benefits outweigh costs; ascertain degree of contribution of program to organizational goals

**Figure 4.13.:** Four level model for trainings evaluation [Lawson, 2009]

#### Level 1: Reaction

Even thou level 1 evaluation focuses on the training participant satisfaction, it is an important step in determining the success of a training program. The reaction from the participants can help to improve the quality of the training program. This feedback would go into the all phases of the course design in the context of ADDIE.

In this trainings concept the Level 1 data is collected in the last lesson “Reflection of the learned content” via a feedback form.

Level 1 evaluation has the following constraints:

- it does not measure learning or the ability to apply learning on the job
- it also cannot measure changes in attitudes or beliefs
- because it deals only with participants' perceptions and reactions, a Level 1 instrument can in no way measure organizational impact
- participants cannot measure the trainer's knowledge

### Level 2: Learning

In level 2 of the evaluation model it is examined what the participants have actually learned in the training. It is relatively easy to determine what knowledge and skills the course participant acquired in the lessons than to find the ways in which the training changed their opinions, values and beliefs. [Lawson, 2009]

In the training concept level 2 evaluation is applied in “Analysis of the Role Play”, the voting part of “The Fax Experiment” and “The SE quiz”.

In the “Analysis of the Role Play” the participants level of new knowledge is reflected in the posters that they are asked to make.

In the voting part of “The Fax Experiment” lesson the number of people who votes for the correct way to handle the fax are indicating the level of knowledge.

The “SE quiz” clearly shows the level of the learned knowledge in the right answers of the multiple choice test.

### Level 3: Behavior

This level of evaluation deals with the long term effect of trainings. The time scope is 3 to 6 months.

“Although both managers and training professionals agree that the success of a training program is determined by what the participants do

with the information or skills back on the job, these results are often ignored. Level 3 evaluation is both time-consuming and costly. It also requires good organizational and follow-up skills and processes.”  
[Lawson, 2009]

To ensure a change of the behavior of the participants the “Information Security Staff Member of the month” program introduced in lesson “Company specific Policies and procedures” seems to be the right tool for that. This is also mentioned in the NIST recommendation [NISTa, 2008].

#### Level 4: Results

The level 4 of the evaluation model determines the impact of the training on the company. In this case if SE attacks are prevented. This could be achieved by looking into the figures of reported IT security incidences. In many lessons of the trainings concept the employee has been motivated to report any SE attack. If reported correctly the management of the company in which the training has been conducted has an idea of the threat and how the employees use their new knowledge to handle it.

### 4.3. Summary

The trainings concept has been applied on a fictive Biomedical research company. This was necessary to make it more visual and give practical examples. But it is important to understand that this is just a concept that consists of certain key elements. These key elements, e.g. the role play, can be easily modified to fit any other real life scenario to develop training against SE attacks.

Figure 4.14 shows the summary of the lessons and their function in the three pillar strategy.

<b>Lesson Name</b>	<b>Awareness about "Simple Cues"</b>	<b>Greater Ability to process Information</b>	<b>Higher Motivation to process Information more carefully</b>
Video "SE Attacks"			
Introduction to Cyber Crime and SE			
SE attack role play			
Presentation of Posters			
Awareness about "Simple Cues"			
Technical Knowledge: Email, Fax, Chat, Internet			
Technical Knowledge: Exercise			
Company specific Policies and procedures			
The Fax experiment			
SE-Quiz			
Tools and techniques to prevent SE attacks			

**Figure 4.14.:** Lesson Summary with details on prevention function

## 4.4. Ongoing Awareness

Kevin Mitnick [2002] proposes an ongoing awareness program to keep skills and knowledge of the employees vital:

"Most people are aware that learning, even about important matters, tends to fade unless reinforced periodically. Because of the importance of keeping employees up to speed on the subject of defending against social engineering attacks, an ongoing awareness program is vital." [Mitnick, 2002]

Mitnick [2002] mentions that one method to keep security at the forefront is to make people responsible for Information Security. This would encourage employees to recognize their crucial role in the overall security of the company.



An success full ongoing awareness program has to be creative and has to use multiple channels for communicating security messages [Mitnick, 2002]. The list below shows gives possibilities for an ongoing awareness program:

- Including informational items in the company newsletter: articles, boxed reminders (preferably short, attention-getting items), or cartoons, for example.
- Posting a picture of the Security Employee of the Month.
- Hanging posters in employee areas.
- Posting bulletin-board notices.
- Providing printed enclosures in paycheck envelopes.
- Sending email reminders.
- Using security-related screen savers.
- Broadcasting security reminder announcements through the voice mail system.
- Printing phone stickers with messages such as "Is your caller who he says he is?"
- Setting up reminder messages to appear on the computer when logging in, such as "If you are sending confidential information in an email, encrypt it."
- Including security awareness as a standard item on employee performance reports and annual reviews.
- Providing security awareness reminders on the intranet, perhaps using cartoons or humor, or in some other way enticing employees to read them.
- Using an electronic message display board in the cafeteria, with a frequently changing security reminder.

- Distributing flyers or brochures.
- And think gimmicks, such as free fortune cookies in the cafeteria, each containing a security reminder instead of a fortune.

The point “Security Employee of the Month” has been already embedded in the trainings concept. Sample Posters on Information Security Awareness are shown in the Appendix.

## 5. Prevention Success Parameters

In order to make training program more successful there are certain parameters that have to be taken into consideration. These parameters provide the environment in which the training should be nested to give a maximum protection against SE attacks in the context of Cyber Crime.

Hansche et al. [2004] categorize IT Security protection mechanism into three protection types:

- Physical Security
- Technical- Security
- Administrative Security

Furthermore Hansche et al. [2004] emphasizing that an adequately protection of Information Security assets, especially in case of a SE attack, the combination of all three parameters is required.

### Physical Security

Physical Security covers the real access to devices, such as servers, or buildings. It deals with keys, locks, alarms, and guards and refers to the protection of assets from damage, and from unstable environmental conditions such as electrical, temperature, humidity and other related problems. It is a vital component in most Information Security solutions.

In regards to SE attacks the importance lies on the protection against internal and external intruders. [Hansche et al., 2004] This could be achieved by the usage of biometrics access control.

Physical Security should also take care of access to the waste of the company in order to prevent the “dumpster diving” information gathering technique discussed in chapter “Cyber Crime Aspects”.

### Technical Security

This parameter covers security measures that employ a technical solution to protect the information assets. Examples include firewall systems, access control systems, Network Intrusion Detection Systems. Technical measures are very effective but they rely on the human element to control it. [Hansche et al., 2004]

In the context of the SE attack prevention, technical security controls can help to identify the caller or the sender of an email by providing the user with programs to do so. In terms of Email security, companies can set up their Email server systems to filter as much as possible of spam mails.

### Administrative Security

Administrative Security involve IT Security policies, procedures and guidelines. Training programs are also under Administrative Security. But it covers the human resource management part, such as the background check for new employees and termination processes. [Hansche et al., 2004]

To prevent SE attacks an effective countermeasure is to have very good, established Information Security policies and effective user trainings programs. The training program part has been covered in this thesis. On the Information Security policy part it is important to mention that it requires the leadership, commitment, and active participation of the top-level management.

“Critical Information Security strategies rely primarily on the appropriate and expected conduct on the part of personnel, and secondly on the use of technological on the use of technological solutions. This is why it is critical, for all Information Security programs, to address the threat of Social Engineering.” [Hansche et al., 2004]

## 6. Conclusion

Information Technology (IT) has changed the way people are communicating. These new communication is still rapidly growing and it has a great influence on how people live.

One thing that does not change that rapidly in the way the technology is changing is the way people are thinking.

Taking this into consideration, that the same techniques used to commit crime without the help of IT are nowadays taken into the cyber space, the internet, and people are more vulnerable to it. The reason is that their ways to prove authenticity or trustworthiness of the other side do not work in these new communication channels. People cannot apply their knowledge gained over thousand of years to judge on the content of the message nor the messenger.

Social Engineering exploits this vulnerability and this Master Thesis is just a start to make people more aware of the threats that come along with use of IT.

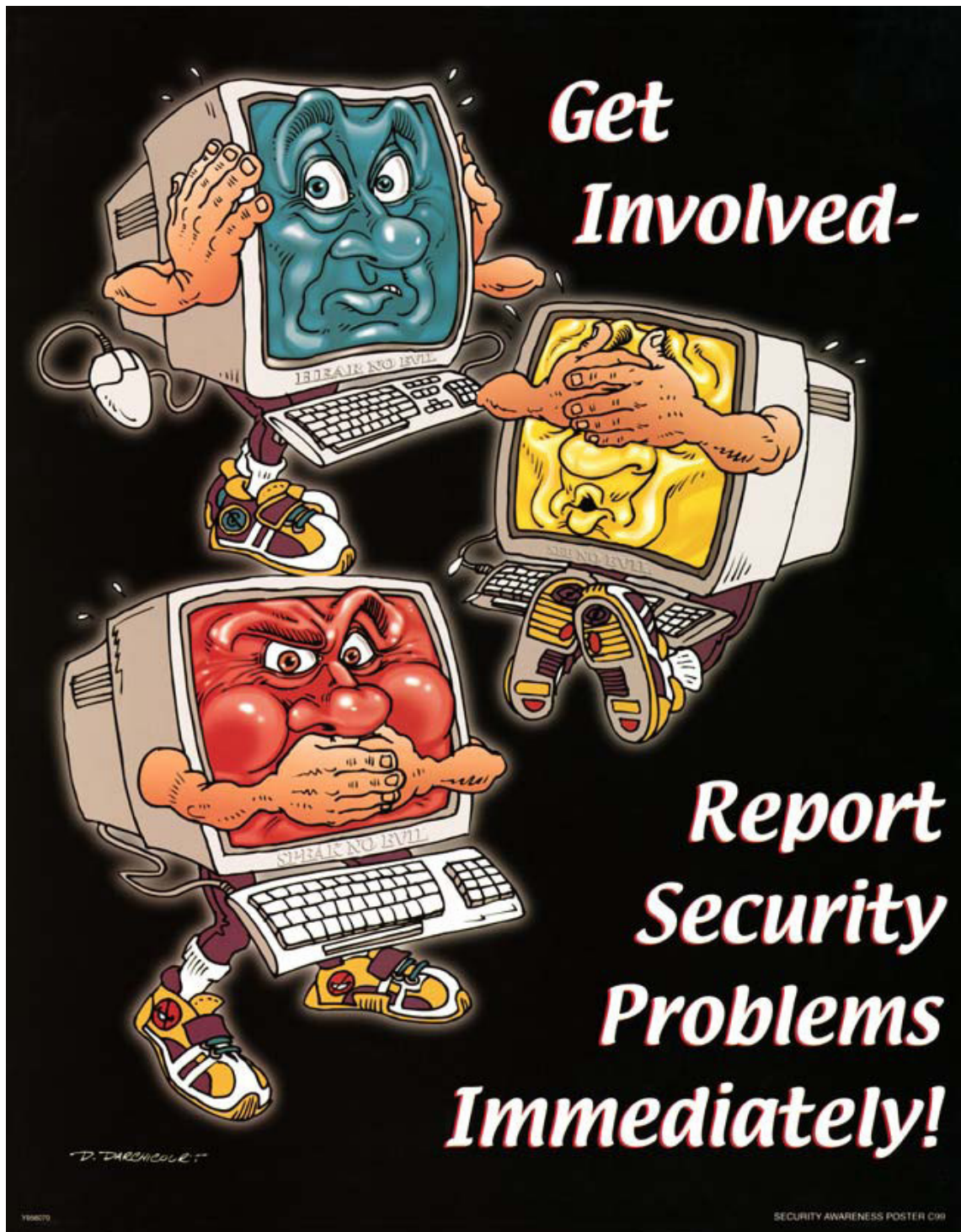
Note from the Author: In the opinion of the Author this Master Thesis is just the beginning that carries the hope of continuation and refinement in it.

## 7. Appendix

### 7.1. Information Awareness Poster examples



Figure 6.1.: Information Security Poster from NISTb [2003] on Email Security



**Figure 6.2.:** Information Security Poster from NISTb [2003] on Reporting Problems

## 8. Bibliography

- [411a, 2009] Web site about Spyware, <http://www.411-spyware.com/remove/phishing-email>, (accessed December 21, 2009).
- [411b, 2009] Web site about Spyware, <http://www.411-spyware.com/tag/virus-doctor>, (accessed December 21, 2009).
- [411c, 2009] Web site about Spyware, <http://www.411-spyware.com/>, (accessed December 21, 2009)
- [AHTCC, 2009] The Australian High Tech Crime Centre (AHTCC) public web site, 2009, <http://www.ahtcc.gov.au>, (accessed December 21, 2009).
- [Behrens, 2009] Daniel Behrens, 2009, Vorsicht - Falle Scam enttarnen, <http://www.pcwelt.de/start/sicherheit/firewall/praxis/2105893/scam-enttarnen/>, (accessed December 3, 2009).
- [Berti & Rogers, 2002] Berti, J. and Rogers, M. 2002. Social engineering: The forgotten risk. In Handbook of Information Security Management, CRC Press, New York.
- [BMFW, 2009] BMFW, 2009, public website from the Austrian Ministry of Science, [http://www.bmwf.gv.at/uploads/media/Logo\\_bm.w\\_f\\_4c-.gif](http://www.bmwf.gv.at/uploads/media/Logo_bm.w_f_4c-.gif), (accessed December 3, 2009).
- [Böck, 2007] Benjamin Böck, 2007, Social Engineering, Technical University of Vienna
- [Bongard, 2002] Bongard, Joachim (2002): Werbewirkungsforschung. Grundlagen - Probleme - Ansätze. Münster.
- [Booth-Butterfield, 1996] Booth-Butterfield, Steve., 1996, Inoculation Theory, <http://www.as.wvu.edu/~sbb/comm221/syllabus.htm> (accessed January 15, 2006).
- [Buehler, 1934] Buehler K., 1934 Sprachtheorie, Jena.
- [Chai, 2009] Ben Chai, 2009, Cyber Crime: Social Engineering and Social Networks, Published on Thursday 20 August 2009, <http://www.securityvibes.com/dave-endler-tippingpoint-dylabs-cyber-crime-social-engineering-social-networks-benchai7-news-3003356.html>, (accessed December 21, 2009).
- [Chaiken & Eagly 1983] Chaiken and Eagly, 1983, Communication modality as a determinant of persuasion: The role of communicator salience. Journal Pers. Soc. Psychol. Issue 45/1983.



- [Chaiken, 1980] Chaiken S., 1980, Heuristic versus systematic information processing and the use of source versus message cues in persuasion, *Journal Pers. Soc. Psychol.* Issue 39/1980.
- [Cialdini, 1984] Robert B Cialdini, 1984, "Influence" is a psychology classic, Published by Quill.
- [Dick et al., 2001] W. Dick, L. Carey, J. O. Carey, "The Systematic Design of Instruction", 5th Ed., New York: Longman, 2001.
- [Dolan, 2004] Dolan, A. 2004. Social Engineering, <http://www.sans.org/rr/whitepapers/detection/1365.php> (accessed December 1, 2009).
- [ENISA, 2008] Maria Papadaki, Steven Furnell, Ronald C. Dodge JR, 2008, Social Engineering – Exploiting the Weakest Links , European Network and Information Security Agency (ENISA), Whitepaper.
- [Gragg, 2002] Gragg, D., 2002, A Multi-Level Defense Against Social Engineering, [http://www.sans.org/reading\\_room/whitepapers/engineering/a\\_multilevel\\_defense\\_against\\_social\\_engineering\\_920?show=920.php&cat=engineering](http://www.sans.org/reading_room/whitepapers/engineering/a_multilevel_defense_against_social_engineering_920?show=920.php&cat=engineering), Sans, (accessed December 31, 2009).
- [Granger, 2001] Granger S., 2001, Social Engineering Fundamentals. Part I: Hacker Tactics, Infocus. <http://www.securityfocus.com/infocus/1527> (accessed December 31, 2009).
- [Hansche et al., 2004] Susan Hansche, John Berti, Chris Hare, 2004, Official Guide to the CISSP Exam, Auerbach Publications, New York.
- [Herkner, 2001] Herkner Werner, 2001, Lehrbuch Sozialpsychologie, Bern, Verlag Hans Huber.
- [Herold, 2005] Rebecca Herold, 2005, Managing an Information Security and Privacy Awareness and Training Program, Auerbach Publications.
- [Hodell, 2006] Chuck Hodell, 2006, ISD from the Ground Up: A No-Nonsense Approach to Instructional Design, 2nd Edition ISBN:9781562864552, ASTD.
- [Hoeschele et al., 2005] Hoeschele, M. and Rogers, M. 2005. Detecting social engineering. In *Advances in Digital Forensics*, Springer, New York.
- [IC3, 2008] Internet Crime Report 2008, 2008, United States Bureau of Justice and the Office of Justice Programs, US Government.

- [ITD, 2009] ITD - Identity Theft Daily (2009). Social Engineering, Cybercrime Will Be Challenges in 2009, Contributed by Identity Theft Daily Staff, [http://www.identitytheftdaily.com/index2.php?option=com\\_content&do\\_pdf=1&id=467](http://www.identitytheftdaily.com/index2.php?option=com_content&do_pdf=1&id=467), (accessed October 15, 2009).
- [Janis and Feshback, 1954] Janis, I. L. and Feshback, S., 1954, Personality differences associated with responsiveness to fear-arousing communications, J. Pers.
- [Janis and Feshback, 1954] Janis, I. L. and Feshback, S.: Effects of fear-arousing communications. J. Anorm. Soc. Psychol.
- [Kirkpatrick, 1959] Kirkpatrick, D. L. (1959) Evaluating Training Programs, 2nd ed., Berrett Koehler, San Francisco.
- [Lawson, 2009] Karen Lawson, 2009, The Trainer's Handbook, Updated Edition, Pfeiffer.
- [Leshin et al., 1992] Leshin, C., Pollock, J. and Reigluth, C., 1992, Instructional design strategies and tactics, Educational Technology Publications, Englewood Cliffs, New Jersey.
- [Malcom, 2007] Allen, Malcolm. ,2007, Social Engineering – A means to violate a computer system, [http://www.sans.org/reading\\_room/whitepapers/engineering/social\\_engineering\\_a\\_means\\_to\\_violate\\_a\\_computer\\_system\\_529](http://www.sans.org/reading_room/whitepapers/engineering/social_engineering_a_means_to_violate_a_computer_system_529), Sans Institute (accessed July 28, 2009).
- [McGriff, 2000] Steven J. McGriff, 2000, Instructional Systems, College of Education, Penn State University.
- [Mitnick, 2002] Mitnick, K. D., & Simon, W. L. ,2002, The art of deception: Controlling the human element of security. Indianapolis, IN: Wiley.
- [NISTa, 2009] NIST Special Publication 800-16 Revision 1 (Draft), Mark Wilson, Kevin Stine and Pauline Bowen, 2009 Information Security Training Requirements: A Role- and Performance-Based Model, United States of America - National Institute of Standards and Technology.
- [NISTb, 2003] NIST Special Publication 800-50, Mark Wilson and Joan Hash, 2003, Building an Information Technology Security Awareness and Training Program, United States of America - National Institute of Standards and Technology.
- [O'Keefe, 2002] O'Keefe, Daniel J., 2002, Persuasion: Theory and Research. Thousand Oaks.
- [Petty & Cacioppo, 1986] Petty, Richard E and Cacioppo, John T ,1986, Communication and Persuasion: Central and Peripheral Routes to Attitude Change. New York.

- [Petty & Wegener, 1999] Petty, Richard E. / Wegener, Duane T., 1999, The Elaboration Likelihood Model: Current Status and Controversies.
- [Rogers, 2006] Rogers M., 2006, The information technology insider risk. In Information Security Handbook, H. Bigdoli, ed., Wiley, New York.
- [Roper et al., 2006] Carl Roper, Joseph Grau, Lynn Fischer, 2006, Security Education, Awareness, and Training—From Theory to Practice, Elsevier Butterworth-Heinemann, Elsevier Inc.
- [Rusch, 1999] Rusch, Jonathon J. (1999). The “Social Engineering” of Internet Fraud. INET '99, Proceedings, [http://www.isoc.org/inet99/proceedings/3g/3g\\_2.htm](http://www.isoc.org/inet99/proceedings/3g/3g_2.htm), (accessed July 17, 2009).
- [Slater, 1997] Slater, M. D. ,1997, Persuasion processes across receiver goals and message genres. Communication Theory.
- [Stewart et al., 2008] James Michael Stewart, Ed Tittel and Mike Chapple, 2008, CISSP: Certified Information Systems Security Professional Study Guide, Fourth Edition by, Sybex.
- [WEB1, 2009] Business Dictionary, <http://www.businessdictionary.com/definition/training-concept.html> (accessed November 16, 2009).
- [WEB2, 2009] Web site from the NRW SCHULMINISTERIUM, <http://www.learnline.nrw.de/>, (accessed December 21, 2009).
- [WEB3, 2009] Web site about Identity Theft, <http://www.identitytheft.com/index.php/article/faq/>, (accessed December 21, 2009).
- [WEB4, 2009] Anti Virus Software Vendor F-Secure, <http://www.f-secure.com/v-descs/love.shtml>, (accessed December 21, 2009).
- [Wilson and Dunn, 1986] Wilson, T. D. & Dunn, D. S., 1986, Effects of introspection on attitude-behavior consistency: Analyzing reasons versus focusing on feelings. Journal of Experimental Social Psychology, 22/1986.
- [Wilson, 1997] Brent G. Wilson, 1997, Reflections on Constructivism and Instructional Design, University of Colorado at Denver, C. R. Dills and A. A. Romiszowski (Eds.), Instructional Development Paradigms, Englewood Cliffs NJ: Educational Technology Publications.

## 9. Table of Figures

- Figure 1.1.: Process of “Mule Recruitment” [AHTCC, 2009]
- Figure 1.2.: “Social Engineering” attack process [Malcom, 2007]
- Figure 1.3.: Financial Aspect of Cyber Crime [IC3, 2008]
- Figure 1.4.: Cyber Crime types [IC3, 2008]
- Figure 1.5.: Three main pillars building up the trainings concept
- Figure 2.1.: Communication factors [Herkner, 2001]
- Figure 2.2.: Elaboration-Likelihood Model [Petty & Cacioppo, 1986]
- Figure 2.3.: The first page of a forged fax
- Figure 2.4.: The Second page of a forged fax
- Figure 2.5.: Picture of the “love letter Virus” [WEB 4, 2009]
- Figure 2.6.: SE attack on Social Networks [Chai, 2009]
- Figure 2.7.: Phishing email [411a, 2009]
- Figure 2.8.: Fake survey from Kmart [411c, 2009]
- Figure 2.9.: Fake mail from Bank of America [411c, 2009]
- Figure 2.10.: Fake Virus Removal [411b, 2009]
- Figure 3.1.: ADDIE process model [Hodell, 2006]
- Figure 4.1.: The three key elements of the training concept
- Figure 4.2.: Sample Pre-Training Questioner
- Figure 4.3.: Design Matrix as foundation for the Instructional Plan
- Figure 4.4.: The Time table of the first trainings day
- Figure 4.5.: The time table of second trainings day
- Figure 4.6.: Script to a role play to demonstrate a SE attack
- Figure 4.7.: Sample instructions for the technical exercise
- Figure 4.8.: Two pages of “Fax experiment” The logo is taken from [bmwf, 2009]
- Figure 4.9.: Sample questions for the Quizzer lesson
- Figure 4.10.: LIST of issues and questions from ENISA [2008]
- Figure 4.11.: Request for Information [Mitnick, 2002]
- Figure 4.12.: Request for Action [Mitnick, 2002]
- Figure 4.13.: Four level model for trainings evaluation [Lawson, 2009]
- Figure 4.14.: Lesson Summary with details on prevention function
- Figure 6.1.: Information Security Poster from NISTb [2003] on Email Security
- Figure 6.2.: Information Security Poster from NISTb [2003] on Reporting Problems