Social Engineering Attack Detection Model: SEADM

Monique Bezuidenhout
Department of Psychology
University of Pretoria
Pretoria, South Africa
monique.bezuidenhout@up.ac.za

Francois Mouton
Department of Computer Science
University of Pretoria
Pretoria, South Africa
moutonf@gmail.com

H.S. Venter
Department of Computer Science
University of Pretoria
Pretoria, South Africa

Abstract—**Social engineering is a real threat to industries in this day and age even though the severity of it is extremely downplayed. The difficulty with social engineering attacks is mostly the ability to identify them. Social engineers target call centre employees, as they are normally underpaid, under skilled workers whom have limited knowledge about the information technology infrastructure. These workers are thus easy targets for the social engineer. This paper proposes a model which can be used by these workers to detect social engineering attacks in a call centre environment. The model is a quick and effective way to determine if the requester is trying to manipulate an individual into disclosing information to which the requester does not have authorization for.**

Keywords:Social engineering, social psycholgy, emotional state, information sensitivity.

I. Introduction

Social engineering, in this context, refers to various techniques that are utilized to obtain information in order to bypass security systems, through the exploitation of human vulnerability [1]. As clearly stated by various authors [2], [3], [4], [5], the human element is the 'glitch' or vulnerable element within security systems. It is the basic 'good' human natured characteristics that make people vulnerable to the techniques used by social engineers, as it activates various psychological vulnerabilities, which could be used to manipulate the individual to disclose the requested information [2], [5].

Individuals make themselves even more vulnerable to social engineering attacks by not expecting to ever be a victim of such an attack, and many will never know that they were a victim of such an attack. The majority of the public are not aware of this technique, and do not fully comprehend the extent to which these techniques to obtain information, can be used, and the potential it holds for dire personal, economic and social consequences and losses for the individual and institution. An individual may believe that the information they posses is of no particular value to another person, nor could it be used for any malicious act, and will thus be more willing to disclose information freely. However, the social engineer is dedicated to researching various aspects and gathering information from various sources. Combined the acquired information can have dire consequences.

On the other end of the spectrum, the individual might believe that they will not fall prey to such an attack, as they would be able to recognize such an attack instantaneously. However, the social engineer is a skilled human manipulator, preying on human vulnerabilities using various psychological triggers that could foil human judgment.

The problem is to successfully detect social engineering attacks whilst working in a stressful environment, where decisions must be made instantaneously. It is for this reason that a practical model, that can be easily implemented and used by all levels of employees, is necessary and proposed within this paper. This model should be used in combination with training on various social engineering techniques, the psychological vulnerabilities it may elicit, and institutional policies and procedures.

The two main perspectives of social engineering - the psychological perspective and the computer science perspective - are accounted for within this model. The psychological perspective focuses on the emotional state and cognitive abilities of the individual. The computer science perspective focuses on information sensitivity, one of the cornerstones of information security. Other important factors incorporated within this model are the urgency of requested information and an individual's comprehension of the requested information.

The remainder of the paper is structured as follows. Section 2 provides background about Social engineering, and Section 3 discusses background on the process of human reasoning and decision-making. Section 4 introduces the proposed model, as presented within this paper, which was developed for social engineering attack detection and provides an in-depth discussion of each of the pertinent elements of the model. Section 5 provides scenarios in order to demonstrate the effectiveness of the model. Finally, Section 6 concludes with a summary of the social engineering attack detection model and suggested future work.

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

II. Social engineering

According to [1] social engineering is defined as the techniques used to exploit human vulnerability to bypass security systems in order to gather information. As indicated by this definition, social engineering attacks imply interaction with other individuals, indicating the psychological aspect of social engineering.

Various psychological vulnerabilities and triggers, used by social engineers, have been identified, which aim to influence the individual's emotional state and cognitive abilities in order to obtain information. To successfully defend against these psychological triggers, the individual will need to have a clear understanding of these triggers in order to recognize each during a social engineering attack. Seven psychological vulnerabilities has been defined by [6]. These psychological vulnerabilities are the following [2],[3],[7],[8]:

Strong Affect: When a strong emotion is triggered, such as anger, excitement, fear or anxiety, an individual's cognitive ability may be seriously hampered**.** This may include their ability to make decisions rationally, evaluate the situation, make counterarguments, and reason logically, which is why this is such an effective technique used by social engineers [8]. A phishing attack could be used as an example. These are thoroughly planned criminal attacks, where websites are designed to masquerade as the authentic site, in order to obtain another individual's authentication credentials and confidential information illegally for financial gain. Phishing attacks are mostly distributed over e-mail as this is one of the easier ways to reach a large distribution of the population in order to ensure the success of the attack. A disparity is created between the individual's perception and the truth, eliciting a heightened fear response, where cognitive abilities are compromised, and the probability of ensuring that the correspondence is legitimate will be minimal [9].

Overloading: This technique has a time element, with the result that the individual becomes cognitively pacified or compliant, through the bombardment of a series of hurried persuasive axioms [8].

Reciprocation: "One good deed deserves another"; Social exchange theory states that individuals, on receiving a kind gesture from another, feels obligated to reciprocate with kindness. The social engineer might create a problem for the individual, only to fix it again, in order to make the individual feel obligated to reciprocate by disclosing information [7].

Deceptive Relationship: To obtain information, the social engineer will identify an individual to purposefully build and establish a relationship. This is done with a particular purpose, as individuals tend to share information freely within established relationships [8].

Diffusion of responsibility and moral duty: The individual is made to believe that their actions - to disclose information, even though it is against policy - will have greater benefits and important beneficial consequences, such as to help save an employee or helping the institution, and that they will not be held solely responsible for their actions [8].

Authority: By the social engineer portraying an authority figure, the individual is more likely to comply with the request to disclose information, as an authority figure almost implicitly elicit a conditioned response to adhere to their wishes and demands, combined with a fear of punishment if the individual may appear to undermine their authority by verifying their legitimacy [7],[8].

Integrity and Consistency: Individuals have an intrinsic desire to uphold their commitments, even if it were not their own [8].

These triggers could be used to perform a social engineering attack on an unsuspecting victim, which could lead the victim to experience a sense of discomfort, whether just an uneasiness or even anxiety, as all these attacks prey on the victim's psychological vulnerabilities. One would expect that a victim would be able to use these clues of discomfort to detect that he is being targeted by a social engineering attack. However, this is the ideal and not realty, as the human reasoning and decision-making process is extremely complex, and prone to error.

The following section discusses the human reasoning and decision-making process and how it applies to detecting social engineering attacks.

III. Human reasoning

The human ability to make conscious, rational judgments, which underlie their decisions, will not always be the ideal. This can be ascribed to various human factors, such as limited information-processing capacity, the use of heuristics (mental processes, or shortcuts, used to simplify the process of judgment, which can lead to judgmental error), personal preferences, and a vulnerability to be influenced by emotions and manipulated by others. Human decision making is a complex process, where most decisions that need to be made will not have only one ideal option, and the same decision will not be made by all people [10],[11].

Within the subjective utility theory, the subjective experience of an individual is taken into consideration, where the goal is to maximize gain and to avoid losses. This subjective experience refers to the individual's own personal judgment on value (utility) and likelihood (probability), instead of objective criteria and computations, where personal characteristics have an impact [11],[12].

The individual will follow a series of steps to come to a decision. First, for each option, they will multiply the subjective probability by the positive subjective utility, followed by subtracting the calculation, as before, for negative subjective utility. Based on these expected values, individuals will make their decision [11].

Risk will always be an integral part of decision-making, as the possible outcome is uncertain. The subjective expected utility theory is the most widely applied model regarding risk decisions. Within this extended version of the subjective expected utility theory, it allows for subjective probabilities, where judgments are made based on the person's belief on likelihood, and where no objective mathematical probabilities are available. This theory cannot, however, predict human

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

decisions. As indicated by the term subjective, each person will have their own set of values and characteristics. By considering the particular individual's subjective expected utilities and their subjective estimates of probabilities of cost and benefits, one can predict the optimal decision for that particular individual [10],[11].

Within this subjective expected utility theory model it is believed that the individual will try to achieve a well-reasoned decision by considering all the possible alternatives and information available, calculating the probability of each probable outcome and the cost and benefits it may hold [10]. Based on this theory, a decision to disclose information will be based on risk-benefit analysis [10].

Decision analysis, a technology based on subjective expected utility theory, attempts to aid better decision making [10]. This approach attempts to aid people to comprehend and have clarity regarding their goals and values, to search for possible options and verification of facts. One of the techniques used by decision analysis is decision trees. Decision trees are representations of decisions, which aid complex decision-making by breaking it down into more manageable components. Values are assigned to each element, whereupon ideal decision principles are applied to integrate these elements. By combing the probabilities and the utilities that correspond to each possible outcome, the best alternative is selected [10].

People do not possess a stable set of pre-existing values that are simply applied; their decisions will be determined by the present context, and the demands of the decision [10].

As indicated by literature, individuals find it difficult to make rational decisions in a limited time frame, especially regarding complex matters. With the skill of the social engineer and the complexity of the attack he is performing, at best, an uninformed individual would only be able to make an educated guess regarding the likelihood of being targeted by a social engineering attack. An individual would need a predefined set of guidelines on which to measure the likelihood of a social engineering attack in order to make a more informed decision.

The following section is devoted to proposing a practical application model to determine if a social engineering attack is being performed.

IV. Social Engineering Attack Detection Model (SEADM)

As indicated, a model is needed as guideline to detect social engineering attacks. The authors propose a social engineering attack detection model, making use of a decision tree, by breaking the process down into more manageable components, and guidelines to aid decision-making (SEADM) in figure 1.

This paper firstly addresses each of these states individually as shown in figure 1 before the full model is discussed with examples. Throughout this discussion the term individual is defined as the person dealing with the incoming call and the term requester is defined as the person whom is making the call and requesting the information.

A. How would you describe your emotional state?

The first necessary step in this model, and one that will have to be considered throughout the process, would be for the individual to be conscious of, and able to evaluate their emotional state, on an ongoing basis. This implies a consciousness of emotion and how it can affect one's decisions.

In the same manner, the individual should evaluate the emotion the requester elicit within themselves, as the psychological vulnerabilities, that might be triggered by a social engineering attack, is directly aimed to create certain emotional states in order to obtain information.

We are all familiar with a day that start off horribly and seem to continue with every possible thing going wrong. For example, the car broke down on the way to work, followed by a negative emotional experience whether it be family problems or a argument with a spouse or colleague. All factors and negative events influence our emotional state and hamper our ability to make rational, thought-through decisions [13]. In such a negative emotional state it is more likely to be a victim of social engineering: concentration is low, irritability and frustration is high, where an individual can possibly provide a requester with information just to get rid of them.

It is necessary to emphasize again what a critical role an individual's emotional state can play in the safekeeping of privileged information. If an individual is in a negative emotional space, the individual will not always be able to make a rational decision on the sensitivity level of the information of a request, or to whom it may be disclosed. This could result in costly losses to the institution and individual.

Awareness and consciousness of one's emotional state will not be an easy task, or even always a possible task for all individuals. With training and rehearsal this skill can and will improve. For this reason the authors are in the process of developing a quick self-evaluation electronic questionnaire that individuals will be able to use. However, in combination with the model, training by the institution can be emphasized on the various techniques used, the psychological vulnerabilities the attacker may elicit, and institutional policy and procedures.

It is important to note that judging one's own emotional state could be a tedious matter and some individuals are unable to perform this task. It is for this reason that an automated self-evaluation electronic questionnaire would be implemented. The questionnaire would consist of a large database of questions, of which only a few would be used per evaluation of this state. Only a few would be used each time as there is a time constraint associated with the model and individuals would be unable and reluctant to perform a self-evaluation task if it takes an excessive amount of time. The timeframe for completing this state should be within a few seconds.

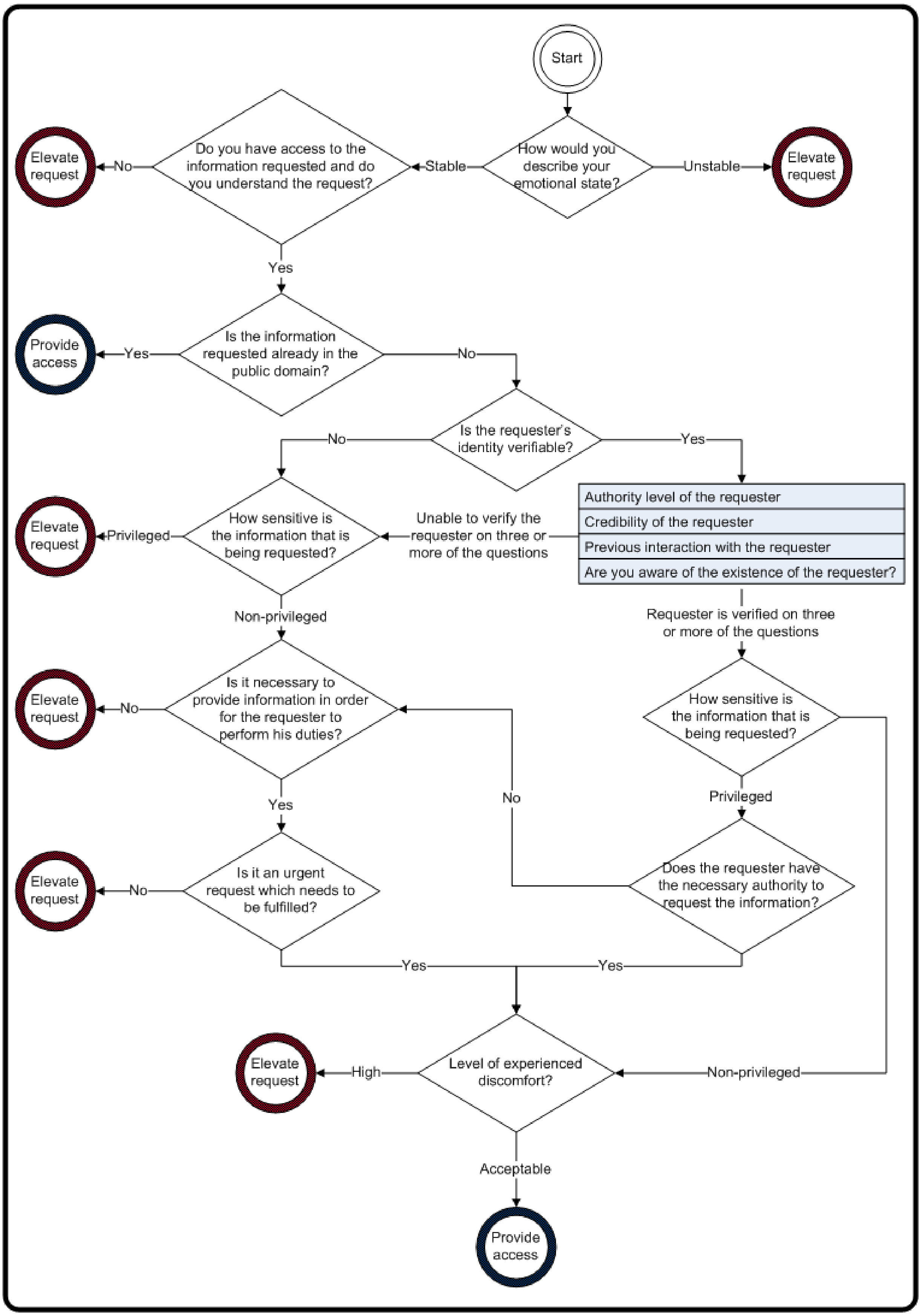
Start
How would you describe your emotional state?
Unstable
Elevate request
Stable
Do you have access to the information requested and do you understand the request?
No
Elevate request
Yes
Is the information requested already in the public domain?
Yes
Provide access
No
Is the requester's identity verifiable?
Yes
Authority level of the requester
Credibility of the requester
Previous interaction with the requester
Are you aware of the existence of the requester?
Unable to verify the requester on three or more of the questions
No
How sensitive is the information that is being requested?
Privileged
Elevate request
Non-privileged
Is it necessary to provide information in order for the requester to perform his duties?
No
Elevate request
Yes
Is it an urgent request which needs to be fulfilled?
No
Elevate request
Yes
Requester is verified on three or more of the questions
How sensitive is the information that is being requested?
Privileged
Does the requester have the necessary authority to request the information?
No
Yes
Non-privileged
Level of experienced discomfort?
High
Elevate request
Acceptable
Provide access

Figure 1. Social Engineering Detection Model

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

If the individual or the self-evaluating questionnaire finds that the individual is too emotional, the call or email request should rather be escalated to another individual. Of course this has the implication, and danger, of people using this as a tool to shift their work responsibilities to another, as well as promote further frustration for all people involved. However, the dangers of social engineering, obtaining privileged information, which can lead to great losses to the institution and possibly the individual, are a much greater threat.

B. Do you have access to the information requested and do you understand the request?

When a request for particular information is made, the individual needs to judge if they possess adequate knowledge regarding the requested information, and if they have access to the information which is being requested, to adequately provide this information. Obviously, if the individual does not have the knowledge required, they will not be able to provide the information, and could refer the requester to another individual, who will also then follow this model. If the individual judge that they have adequate knowledge on the subject in question the following step can be taken.

C. Is the information requested already in the public domain?

Individuals should have a clear understanding of what information are readily accessible to the public regarding their institution and related information. The information in the public domain could include contact details and working hours, which could be available on the institutions website, and thus be legally provided to a requester.

D. Is the requester's identity verifiable?

The individual now needs to verify the identity of the requester, to enable them to make an informed and rational decision if information should be provided to the requester at a later stage of the model. If the requester's identity cannot be verified, a different set of states will be examined to determine if the information should be provided.

Important to remember is that the social engineer might be portraying himself as an authority figure within the institution, a computer technician, or any other persona that might elicit compliance. As humans we are inclined to make quick assumptions regarding people and their stature, based on trivialities such as clothing. If someone is dressed in the proper attire, use the appropriate institutional jargon, using an important individual's name, does not necessarily indicate that the individual is trustworthy. Social engineers do an enormous amount of research before an attack if warranted. If at any time the individual feels unsure, they should contact their manager, to obtain authority to provide, or not provide, the information requested.

To verify the requester's identity, the following should be taken into account and used to form a global impression to base the decision on whether to provide or not provide the requested information: authority, credibility, previous interaction, and knowledge of the person's existence will have to be taken into account.

Some of the techniques that can aid in the verification process of an individual's identity are the following: Caller Identification; Calling back the requestor on a predetermined phone number; To request a secure email; To request a secure password; To request a face-to-face interaction with the individual, where he would provide proper identification, Where another employee can vouch for the requester; To contact the requester's immediate supervisor in order to verify his/her identity; To use an employee directory [3].

In this model it is suggested that the individual should be able to determine at least three of the four components to successfully verify the individual. Each of these qualities will now be individually addressed.

1) Authority level of the requester

Authority is part of any institution, with an almost conditioned response from employees to adhere to their wishes and demands, combined with a fear of punishment if the individual may appear to undermine their authority [7]. For this reason it is a very effective technique used by social engineers to obtain privileged information. The institution needs to provide an environment where the employee feels comfortable, and are expected to question the authority figure's identity when disclosing sensitive information.

With the determining authority, the employee also needs to know, with the help of a clear institutional policy, what authorization level a particular person of authority has, in regards to what privileged information can be provided.

2) Credibility of the requester

The employee needs to judge the level of credibility of the requester. However, this is a challenging task, as establishing credibility is the first step the social engineer undertakes, and what the attack will be based on.

If the requester knows the jargon used by the particular institution, people easily assume that the requester is an employee at their particular institution. The requester could, for example, be an ex-employee, quite knowledgeable about the jargon and procedures. Such ex-employee might seek revenge with the goal of obtaining particular sensitive information.

The credibility of the requester is measured on the basis of how he/she responds on predefined of set of questions which can be used to determine the credibility of a requester.

3) Previous interaction with the requester

If the individual had previous interaction with the requester, especially a longstanding history of interaction, the decision and knowledge to what information can be provided will be an easy task. However, few interactions with the requester, especially by telephone and email alone, should be considered in conjunction with other verification techniques, to be able to make an informed and safe decision regarding the disclosure of information.

4) Are you aware of the existence of the requester?

This refers to the knowledge that the requester exists within the institution or an outside collaborating partner on a project can support the verification of the requester. However, this should also be used in conjunction with the other verification techniques, as the requester could be a social engineer portraying himself as the well-known figure in order to obtain privileged information.

It is suggested that within institutional policies and procedures, a classification system of information should be established, whereupon a document should be compiled and made available to all, of all personnel indicating what level of information authorization each has, which will simplify the process.

E. How sensitive is the information that is being requested?

It is critical that the individual are knowledgeable, and have absolute clarity, what information is privileged, and what information are authorized to be provided, and to whom, thus depicting the level of information sensitivity. This skill can be nurtured and enhanced through training on institutional policies and procedures.

For the purpose of this model, information is divided into two categories, privileged and non-privileged information. Privileged information indicating information requiring a form of authorization, and non-privileged information indicating information that requires no authorization and are freely available.

The proposed model should be used in conjunction with an institution's policies and procedures on information sensitivity. These policies and procedures should include clear, easily understandable and easily accessible guidelines to verify the authorization level needed in order to request the specific information.

As each institution is unique, each will have to create and establish their own security policies to address the classification of sensitivity of particular information, under which circumstances it may be divulged, and to which particular individuals or institutions. These policies should also include processes and accountability for reporting suspected incidents [7].

After determining whether information is privileged or non-privileged, the individual will need to determine if the requester has the necessary authority to request the information.

F. Does the requester have the necessary authority to request the information?

With the aid of the previous steps the individual possess the necessary knowledge regarding the requester's identity and authority level, together with the information classification. The individual can now determine whether the requester has a level of authority on the same level or higher as the level of sensitivity of the information. If the requester possess authorization on the same authority level or higher needed for the particular information, the next step - the level of experienced discomfort - can be considered.

However, if the authority figure does not have the necessary authorization, or if the individual feels that the request made is not legitimate, the model will treat the requester as a non-verified individual. In this scenario the following step - to determine the necessity of the information to fulfill required duties - will be considered.

G. Is it necessary to provide information in order for the requester to perform his duties?

A subjective estimation needs to be made if it will be beneficial or detrimental to provide the information to the requester at the particular time of the request, as well as how it could empower the individual to complete their work. The individual should be sure that if he/she provides information to the requester that it would indeed be beneficial to both parties involved.

Apart from establishing if the information would help the requester to complete his duties, one would also need to consider the urgency of the request.

H. Is it an urgent request which needs to be fullfilled?

The individual needs to assess the urgency that the requested information is needed. If the information is not urgently needed, and any doubts exist, the information does not have to be provided, or can be provided at a later time. With the time leniency, an authority can be consulted, who can choose to further investigate, or provide authorization to divulge the requested information.

If the information is urgently needed, whether it is to complete an urgent project, or in a life threatening situation such as where an individual's medical insurance number is required as he was injured at work, the employee should consider the next step of level of experienced discomfort.

I. Level of Experienced Discomfort

Evaluation of one's emotions is again emphasized, where an individual will have to trust the emotions they are experiencing at that particular time, e.g. "trust your gut". If the level of discomfort experienced is evaluated as too high, information should rather not be provided, as certain techniques used by social engineers may elicit high levels of emotional discomfort, enabling them to obtain privileged information. Part of the social engineer's skill set is the ability to profile individuals, using the appropriate technique for the particular individual, forcing them into a desired role. This technique is called altercasting [1]. In a certain scenario they may be aggressive and threatening towards the individual, causing high levels of anxiety, where the individual's cognitive ability to reason, to be able to stay calm and focused, and to be able to make rational counterarguments, are detrimentally influenced. In another scenario, and also the most frequently used form of this technique, the individual will be ascribed to the role of helper, where the individual could experience discomfort and possibly guilt - an emotion most people try to avoid - if they do not oblige to the request.

If, however, the individual does not experience any discomfort or if the level of discomfort is understandable and acceptable, information can be provided, as the previous steps have been successfully completed.

The next section demonstrates the application of the model by use of examples.

V. Discussion

Three example scenarios are provided within this section. The first scenario is a legitimate request by a bank account

978-1-4244-5494-5/10/$26.00 ©2010 IEEE

holder, requesting his bank account balance. The second scenario also depicts a request for a bank account balance, however, by a social engineer. The third depicts a basic scenario where a request is made regarding the closing time of a store.

Within all the provided scenarios in this paper, it will be assumed that the individual dealing with the request is in a stable emotional state.

A. Scenario one

A telephonic request is made to obtain a personal bank account balance. The process, according to the SEADM model, will be following:

Emotional state of the call centre agent will be analyzed, which will equate to stable.

Do you have access to the information requested and do you understand the request? Yes.

Is the information requested already in the public domain? An individual's bank balance is not public information and will, thus, be necessary for the agent to verify the identity of the requestor.

The requestor will need to identify himself, and establish his credibility by providing the call centre agent with his personal information. The call centre agent then verifies the information by comparing it to the information on the system when the bank account was created. This verifies the question of being aware of the existence of this requester, as well as the authority level of the requestor.

How sensitive is the information being requested? A bank account balance is classified as privileged information.

Does the requester have the necessary authority to request the information? Yes.

Lastly the call centre agent would need to analyze his level of experienced discomfort, which would be acceptable as there were no issues in this call.

Within the process completed, in this scenario, access can be provided, allowing the call centre agent to provide the requester with his bank balance.

B. Scenario two

This scenario also depicts a request for a bank account balance, however, by a social engineer.

Emotional state will be analyzed, which will equate to stable.

Do you have access to the information requested and do you understand the request? Yes.

Is the information requested already in the public domain? An individual's bank balance is not public information, and will thus be necessary for the agent to verify the identity of the requestor.

The requestor, who, in this scenario is a social engineer, will attempt to identify himself. This can proceed in one of two ways. The social engineer could be in possession of adequate information pertaining to the victim's personal and banking details. This information used in conjunction with his various skills and techniques, for example overloading, can convince the call centre agent he is the legitimate requester. This could lead the call centre agent to experience a high level of discomfort. The call center agent could elevate the request to another individual with higher authority to adequately manage the request, or could deny access to the information.

To fully explain the model, this paper will examine the alternative route, where the social engineer failed to validate himself as the owner of the bank account but he has validated himself as a friend of the owner of the bank account.

How sensitive is the information being requested? A bank account balance is classified as privileged information.

Does the requester have the necessary authority to request the information? Within this alternative scenario the answer would be no. A friend will not have authorization to privileged information as a bank account balance.

Is it necessary to provide information in order for the requester to perform his duties? The social engineer could portray himself as the bank account holder's accountant, explaining that he needs the information to complete his duties. Assuming the call centre agent allows this, he will move onto the urgency test.

The call centre agent needs to determine the urgency of the request. However, a legitimate accountant would ask the account holder to contact the bank and obtain the necessary information. In this scenario the call centre agent would need to elevate the request, and report the request as a suspicious.

This scenario depicts how a social engineering attack could have been thwarted. The last scenario depicts a request to public information.

C. Scenario three

Within this scenario a request is made regarding the closing time of the institution.

Emotional state will be analyzed, which will equate to stable.

Does the individual have access to the information requested and understand the request? Within this scenario the individual have the necessary information regarding the operating hours of the institution and understands what information is being requested.

The operating hours of the institution is information which is already in the public domain, and thus can be provided to the requester.

This paper concludes by providing a brief summary and the potential advantages it may hold to an institution if applied together with adequate training.

VI. CONLCLUSION

Social engineering is very difficult to detect, as the social engineer possess various skills and effective techniques, preying on human vulnerabilities, which makes these attacks often go without notice. What makes detection even more difficult is that many people are unaware of this technique and the potential threat, and dire consequences it holds for the individual and for institutions.

As of yet, only training has predominantly been considered as preventative measure to social engineering. However, it has been shown that training is soon forgotten, especially in the real work environment, rendering training only as ineffective against social engineering. It is proposed that a visible practically applied, user-friendly aid, as the SEADM, will aid in the daily awareness of the threat, and thus protection against social engineering.

It has been shown by the use of scenarios that the proposed model is indeed feasible as a preventative measure to social engineering attacks. This model makes a valuable contribution to the field of social engineering, as it aids in the detection of social engineering attacks, by breaking down the decision-making process into manageable components.

Future research will aim to improve the SEADM, by designing an automated electronic emotional self-evaluation questionnaire. This will aid the model by removing the subjectivity from the emotional state question and provide an objective way to measure an individual's emotional state. The authors will also explore research by [2] to illustrate the probable increase in awareness of an individual's own vulnerability to such an attack, through practical application of social engineering in training. Lastly, some action research in a call centre will be completed in order to verify the usability of SEADM.

REFERENCES

[1] K D Mitnick and William L Simon, *The art of deception: controlling the human element of security*. Indianapolis: Wiley Publishing, 2002.

[2] J W Scheeres, R F Mills, and M R Grimaila, "Establishing the human firewall: reducing an individual's vulnerability to social engineering attacks," in *3rd Internation Conference on Information Warfare and Security*, April 2008.

[3] K D Mitnick and William L Simon, *The art of intrustion: the real stories behind the exploits of hackers, intruders and deceivers*. Indianapolis: Wiley Publishing, 2005.

[4] J Debrosse and D Harley, "Malice through the looking glass," in *Virus Bulletin Conference*, September 2009.

[5] G L Orgill, G W Romney, M G Bailey, and P M Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computing systems," in *Conference On Information Technology Education*, Salt Lake City, October 2004, pp. 177-181.

[6] Gragg D. (2002, December) A Multi-Layer Defense Against Social Engineering. Sans Institute Reading Room.

[7] M Workman, "A test of interventions for security threats from social engineering," *Information Management & Computer Security*, vol. 16, no. 5, pp. 463-483, 2008.

[8] A Chandler and R Boadhurst, "Social Engineering and Crime Prevention in Cyberspace," Queensland Univeristy of Technology, Brisbane, 2006.

[9] X Dong, J A Clark, and J L Jacob, "User behaviour phishing websites detection.," *Proceedings of the IMCSIT*, vol. 3, pp. 783-790, 2008.

[10] N Braisby and A Gellatly, *Cognivite Psychology*.: Oxford University Press, 2005.

[11] R J Stemberg, *Cognitive Psychology*, 4th ed.: Thomson Watsworth, 2006.

[12] G Bansal, F M Zahedi, and D Gefen, "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems*, vol. 49, no. 2, pp. 138-150, May 2010.

[13] M T Siponen, "A conceptual foundation for organizational information security awareness," *Information Management & Computer Security*, vol. 8, no. 1, pp. 31-41, 2008.