Social Engineering a General Approach

Valerică GREAVU-ŞERBAN, Oana ŞERBAN
Alexandru Ioan Cuza University of Iaşi
valy.greavu@feaa.uaic.ro, oanaserban.so@gmail.com

Social engineering is considered to be a taboo subject in nowadays society. It involves the use of social skills or to obtain usernames, passwords, credit card data, or to compromise or altering the information and systems of an entity. Social engineering methods are numerous and people using it are extremely ingenious and adaptable. This technique takes advantage of the intrinsic nature of mankind, to manipulate and obtain sensitive information, persuading people into divulge it, using exceptional communication skills. Thus, five models of persuasion were identified, based on: simplicity, interest, incongruity, confidence and empathy, exploiting key factors which predispose people to fall victim to attacks of social engineering such as greed, self-interest, guilt or ignorance. It is well known fact that security is as strong as the weakest link in its chain (individuals) therefore, beyond technical measures, staff training is the key to success in defending against such attacks.

Keywords: *Social Engineering, Persuasion, Trust, Risk, Sensitive Information, Online Security, Confidence, Manipulation, Attack, Staff Training*

1 Social Engineering

The society of 21st century has been defined as being based primarily on knowledge. Furthermore it has been founded on the exchange of data between all fields of activity. Nowadays, the amount of information held is directly proportional to the power that an individual can have on others; therefore, a very important aspect is not only acquiring but also protecting it from potential attacks. The emergence of numerous systems and protection mechanisms seemed to have solved the security problems. However, it has been discovered that the crucial element as remained the individual and not the machine, that installing the latest applications does not guarantee a complete protection of the system as it is not necessary to force it to infiltrate yourself, it is easier to get the information needed using persuasion or goodwill. Social engineering is a set of methods by which an individual or group of individuals are manipulated to provide access to certain information or to print a certain behaviour

2 Social Engineering from a Non-Technological Point of View

Social engineering represents a set of methods through which an individual or a group of individuals are manipulated into providing access to certain information or used to induce certain behaviour. [1]

In order to avoid technical security measures set to prevent attackers from breaking into systems, they have developed various procedures to bypass the software or hardware elements utilized. Social engineering is based on using psychological stratagems on system’s users, thereby obtaining important data, such as usernames, passwords, security codes, access codes, credit card numbers and additional information for immediate benefits or ulterior ones. [2]

Under the conditions listed above, plus given the fact that despite the automation of the machines and networks, nowadays, there is not a single computerized system that does not depend on human factor; social engineering is a hot topic in modern society. There will always be people responsible for providing information and maintenance of the systems. However social engineering has existed since the beginning of all times and this due to people’s predilection to be polite, to help each other and trust each other. It is in human nature [3]. This technique takes advantage of the intrinsic nature of mankind

DOI: 10.12948/issn14531305/18.2.2014.01

to manipulate others and obtain sensitive information. In fact, most people who disclose data are aware of that, but they often believe that the information provided is not essential. The goal of social engineers, however, is to join pieces of information gathered from various sources.

As for non-technological view, social engineering overlaps to some extent with the policy above all as a social science. Its development made possible the gathering and analysis of information about social attitudes and trends, as it is necessary to establish the initial state of a society and to predict the effects of decisions that might be taken.

Social engineering, however, arose from the beginning of all time. "The fall into sin" of the first two people would not have been possible without the serpent using its power of persuasion on Eve and Eve on Adam. Amenhotep III, himself, during Egypt's perhaps most prosperous period has managed with his skills as a diplomat to impose and maintain power on today's Syria and Palestine, without the need of military control. Even the Greeks used their social skills in order to obtain their goals; see the well-known story of the Trojan horse built under the command of Ulysses, but brought in city by the Trojans themselves. The importance of persuasion and "deception" has been described by Sun Tzu in the "Art of War", stating that it is very important to simulate failure and passivity when you are active, forcing the enemy to perceive weaknesses and strengths and contrariwise. [4]. In 1979, Kevin Mitnick introduced a new concept related to the art of persuasion, by taking into consideration the technical aspects of this science. This new domain was called social engineering. Mitnick demonstrated that despite the numerous measures of assuring information security and the latest technologies, security is as strong as its weakest link, the human factor. [3]

3 The Taxonomy of Vulnerable Users

It is said that there are several key factors that prone people to fall victim to social engineering attacks, for example: greed, self-interest, guilt, likelihood to trust others, ignorance and so on.

Successful social engineers are confident and in control of the conversation. They simply act as if being part of the system even though they should not be and their self-confidence will dispel the doubts of others, with ease.

Social engineers will also use humour and compliments in conversation. They may even offer small gifts to employees, establishing a connection that could be used in the future. These kinds of gestures are often successful manners of winning people's trust because sympathy and cooperation are great ways in which people interact naturally, under suitable conditions. [5]

If a program cannot be upgraded, downloaded or there are no patches available the solution is simple: it can be replaced or removed. In terms of people decisions are not so simple. A person who has been victim of a social engineering attack cannot be replaced by another version of the same individual; moreover, hiring a more capable one is not necessarily the most feasible solution because the time used for their training can be a waste of resources, considering that the methods of attack are rapidly expanding. [6]

People are very careful when it comes to unauthorized installation of software in order to extract information from the operating system, but their ability to cope with social engineering especially under pressure, lacks. Individuals tend to trust strangers or partially unknown people, accepting to share more or less precious information about their work due to either for being ignored or craving to be noticed. The solution to this problem is to notify, educate and inform employees about the existence of areas and dangerous actions, regardless of their job.

It has been noticed that offering bonuses or favours often creates an obligation of reciprocity to the person who has received them. It has been shown, however, that the value of these small favours depreciates over time, so it is vital that the interlocutors remember and perceive the importance of the services/goods; so a good social engineer will always remind the members of staff about their acts of kindness. [7]

Curiosity and the fact that the victims are not well informed are other faults exploited by social engineers. Huge buttons and windows with attractive design promising interesting experiences makes people to access web links without verifying the information submitted.

Generating the impression of imminence and must have service/product leads users to behave correspondingly, regardless of the potential negative effects involved by their actions.

Another characteristic of individuals that is exploited by social engineers represents kindness to those in need. It is a well-known, classic way to acquire unauthorized access to buildings without using any kind of force; intruders are helped by employees just because they are carrying a huge stack of folders.

Greed is what makes us susceptible to some form of bribery or seduction. Thus, people in lower positions within companies such as porters, janitors, messengers, dissatisfied with their remuneration, are more easily persuaded to provide information or access to buildings in exchange of financial benefit, than those involved in management.

Self-distrust. People are very reluctant to ask a foreign person to identify or tend not to watch as passwords or access codes are entered; as social engineers are masters when it comes to self-confidence and dissimulation, they can easily intimidate their interlocutors.

Thoughtless or frivolity are seen as signs that are indicate failure of attention. It is known that most users are not experts in security systems, but it is easy to disguise this small defect through proper education and implementing realistic policies. [3]

Another flaw that undermines the security of a system is the apathy of employees. This is a problem connected with human resources management including the process of selecting the staff. Associated with indifference and insensitivity, apathy characterizes an individual completely detached from the environment, lack of response and will and they will passively witness any events that will threat system's security.

Boredom is also menacing factor information's security being induced by repetitive tasks. Thus, individuals learn shortcuts to ease their tasks' accomplishment, using minimal effort. Soon, such persons become lazy and unchallenging to attack; the social engineer knowing that he will receive the necessary information without difficulty, due to the attitude adopted by these people towards their work. [8]

Fear of authority. Many people are reluctant in presence of someone perceived or having an authoritarian attitude, feeling intimidated by them most of the time. Attackers assume similar roles such as lawmen or senior officials in companies in order to extract sensitive information regarding the organization/entity.

4 Persuasion Seen as the Art of Manipulation

"*People will do anything for those who encourage their dreams, justify their failures, allay their fears, confirm their suspicions and help them throw rocks at their enemies.*"

Blair Warren

The purpose of persuasion is to make the one next to you feel fulfilled even if you managed to convince him. Persuasion is not only a science; persuasion is an art, and sometimes involving compromise beyond exceptional communication skills. To be persuasive involves knowing to ask the right questions at the right time, convince people to accept your opinions, all by themselves, and not by using force. Unlike manipulation, the outcome of persuasion is sustainable; persuasion being nothing but a victory over the others. [9]

The purpose of persuasion is to convince people to support an individual. Subjects are those rather undecided, while limiting the effects that people with strong convictions can have on the individuals concerned.

Thus five models of persuasion were identified based on: simplicity, self-interest, mismatch, trust, and empathy. [10]

Simplicity refers to the technique of presenting the arguments supporting a cause and not the topic itself; the more complex the speech will be, the more confused the listener will get. If the goal is to determine someone to remember something, then a subtle message will be more effective (using simple titles- based on the principle “less is more”).

Self-interest. Despite the fact that humans are social animals characterized by selfishness, after all what motivates them itself- interest. Faced with the fact that others may have as a goal taking advantage of others, the temptation is to be the first to act. It has been proved that helping others, being altruistic, triggers fulfilment which is the ultimate goal.

Another important concept when it comes to self-interest is related to perception. People do things that they consider assumed in their advantage. Therefore, the individual’s belief that an idea is his benefit will determine him to apprehend it, regardless of the veracity of its accuracy.

Mismatch. Congruent shapes are those that are identical in all aspects; coinciding exactly when superimposed. The incongruous do not seem to belong together. In an attempt of understanding their personal universe, people will continuously seek for well-known known models. The main advantage is that the models are reliable and predictable, and the brain generates the perception of retrieval in their harmony. The reverse is feeling uncomfortable when things cannot be assigned to existing models. If things are different than the pattern imagined, confusion may occur, and the subjects often resort to self-deception and predisposition to see what people want to see, not reality.

Confidence will cover a lot of shortcomings. The ability to present things as an expert guarantees success. This goes for people granted with authority; symbols of power are accepted and followed unconditionally. For example, in the famous Milgram experiments, about 65 % of people involved were persuaded to administer lethal doses of electricity to strangers just because they have been ordered to do so by a man in a white coat. When the supervisor was not wearing his uniform, the number of those complying has been decreased with almost 25 %.

Empathy. Humans evolved in small communities and then in societies. Living together has been advantageous for survival, based on the existence of trust and for gaining it one must understand how others think and feel. Empathy is nothing but evidence of exaggerated worry towards the rest of the community. Showing empathy and trust increases considerably the chances to prevail upon a certain person.

All elements mentioned above show signs of being deeply embedded in the human psyche. Among all the need for identity comes first and is supplied largely by interactions between individuals. A factor of great social importance is creating connections with other members of the society thus emerging a mix of identities.

Aristotle described three ways of changing others’ opinions and imposing one’s own beliefs. Thereby the ethos uses trust and focuses mainly on the speaker, designating him/her as a moral person, having good character. Reputation and credibility depend on the competence and the way they are depicted. Self- confidence, according to Aristotle, is one of the key factors when it comes to persuasion, often coexisting with mimics, gestures, and eye contact signalling self-reliance.

Pathos often appeals to listener’s emotions and aims to stimulate his interest. An effective way to arouse passion is to appeal to one’s moral and spiritual values; ethos facilitating then the process of displaying individual’s values and juggling with objectives, interests, and even opinions of others. [11]

Language has also a significant effect on emotions, keywords being able to prompt sensations and feelings.

Logos focuses on arguments using logic and rational explanations or conclusive evidences. The latter, together with science are based on the use of empirical evidence. Providing evidence makes it difficult to pledge a negative response in the context of non-existence of prior knowledge of one of the participants at the act of persuasion. Evidence can include statistics, photos or even experiments.

Cialdini, however, believes that persuasion is based on six principles: reciprocity, social proof, sympathy, authority, consistency, and rarity.

People generally seek to return favours, to pay debts and to treat others as they are treated. According to the principle of reciprocity, this attitude can induce the need to offer concessions to people who have previously provided them. [12]

Social proof is a psychological phenomenon where people assume the actions of others in an attempt to reflect correct behaviour for a given situation that is the behaviour adopted; individuals tend to judge the correctness of their actions according to others' apprehension about them. Cialdini states that we are often influenced by people we like mainly because we perceive them as being similar or familiar.

Rarity. This principle says that things tend to be more interesting when their availability is limited or when the opportunity to purchase them, under favourable conditions, is low. For example, one could buy something immediately, if advertised that it is the last item or a special offer concerning it will soon expire.

Regardless of the principles' classification, persuasion remains the most popular form of influence. Argument is the method through which a person tries to persuade another person or group of persons to believe or to act in a certain manner. Persuasion is a process of guiding people into adopting ideas, attitudes or actions (rational or less rational), based on discussions and attractive presentation of the topic instead of using any means of force.

5 Methods of Obtaining Information

Daily attacks on personal or corporate information may take multiple forms, while the level of protection adopted by users is still low most of them surmising that most antivirus or firewall solutions will suffice to protect attacks.

What is a cyber-attack?

Cyber-attack is an action intended to affect an organization's network or its components, disrupting its activities, disrupting data flows, causing a delay in the delivery of services. The purpose of these actions is to obtain confidential information related to accounts, customer lists, technical data, or immediate material benefits, most often through illegal transfer of money in different accounts. [13]

What is a social engineering attack?

A social engineering attack supposes the use of social skills in order to compromise or alter the information and information systems of an entity. Thus an attacker may seem bashful and respectable, claiming to be a new employee, a maintenance person or even research, being willing to provide papers in order to prove it. Asking various questions and putting together the responses obtained, one can gather enough information to get into an organization's network. If an attacker is not able to gather enough information from one source, the may contact other individuals within the same organization and based on his anterior data he will strengthen his credibility. [14]

What to expect from a social engineering attack?

In order to gather information the attacker will have to gain the trust of his future victims. Tricks used are multiple, ranging from assuming the identity of another person (most often an employee of the IT department or someone higher in the hierarchy) to more intelligent techniques involving research and more effort. These methods have appropriate results in most cases because people usually are gullible, and addressed questions are most of the time rational and do not rise too much suspicion (for which the generally attacker usually has well prepared answers). Phishing and spamming are closely related to social engineering.

Examples of social engineers: Kevin

Mitnick, Badir brothers (Ramy, Muzher and Badir Shaddai), Christopher Hadnagy, Steve Stasiukonis, Mike Ridpath, Frank Abagnale, David Bannon, Peter Foster, Steven Jay Russell and Pappy Boyington.

The main types of attack are: phishing, pharming, phreaking, dumpster diving, reverse social engineering, and whaling.

The first two types of attacks are directed towards obtaining personal information such as username, password, and data on credit card by impersonating an entity which has already gained the user's trusts. As mechanism for distribution are used the messaging system, email or various social networks. For example, phishing consists in sending an email containing a link to a website that mimics the original site. As a result of the increased training of the personnel and their responsibility towards phishing another form of bullying in the online environment has appeared, named pharming. This consists in redirecting traffic originally intended to the original page, to a different address, thus compromising the system that accesses it, or it's DNS (Domain Name Server). [15]

Phreaking involves the illegal access of telecommunications infrastructure. Initially the purpose of this action was to make long distance calls for free; soon Once Voice over Internet Protocol technology (VoIP) has been implemented, phreaking took on a new dimension and started to threat to companies has grown considerably. A successful action offers access not only to the voice infrastructure, but also the electronics and by default to the company's data. [16]

Dumpster diving can provide important information about an organization's activity, without requiring, in most cases, direct contact with employees. [8] This can provide details about phone numbers, upcoming activities, events, source codes, sensitive information on floppy disks, CDs and hard drives. Auspicious moments to act are designated to be prior to fusion between firms, reorganization or beginning of a new year. [17]

Reverse social engineering comprises a series of three steps: sabotage, disclosure of the problem and assistance. In the first phase, the intruder launches an attack on the system, then announcing subjects of a potential problem or flaw in the system then pretending to be a security consultant he offers his services. This allows attaining access to numerous data on the systems and installing specialized programs to record the keys struck on the keyboard (key loggers). [18]

The whaling is launched usually on the staff management; information about executives or other persons in charge can be found frequently on websites of companies as Curriculum Vitae-s or biography. Attackers may find such information about education or their passions permitting them to assume different roles (peers, teachers, and friends) and to invite the victims to various false events, to access various websites that require personal information such as name, address, phone number, credit card number for reservations, etc.

6 Business Risk

The issue of security has become essential, given the fact that organizations tend to become completely dependent on the optimal functioning of the systems owned. [19] The needed solution is therefore to invest in adequate security systems. Protection measures can be framed in one of following categories: prevention, detection and response. (Figure no. 1).

Small Business Technology Institute (SBTI) together with Symantec published in July, 2005, a report on security incidents experienced by small businesses. The report confirms that systems are increasingly vulnerable to attacks and recommends proactive security measures and vigilance in the management of the organization, plus data protection in order to mitigate business risks. [20]

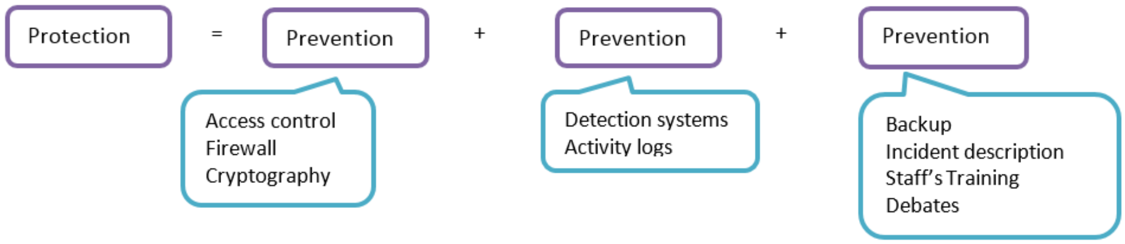

Fig. 1. Safeguards

Source: Meghantan, N., Network and Information Security Principles, Policies, and models, Jacksson State University, 2011, p 12.

Thus, switching to sophisticated architectures of information systems, automated processes within the company involves an increased risk exposure of information. When sensitive information about the activity of the entity or its employees are compromised as a result of viruses or other persons entering the system, it appears a delay in the production cycle and economic losses, affecting the company's ability to operate.

The same study, conducted by Symantec showed that often the companies, although they are aware of the importance of information's security, they are not willing to invest in projects that could protect them. Thus, the research revealed that 20 % of the systems administered mail boxes of employees but they were not secured properly, and 60 % of their wireless networks were unreliable. Additionally, most small businesses (75 %) did not take any action in order to secure their systems. [20]

Security breaches together with the fines received for non-compliance with international standards, result in loss of competitiveness, investor confidence and even their support. [21]

However, it must be considered that unrealized gains and loss of customer databases, theft or loss of capital prototype image and the time needed to regain customer confidence, market position, implementing security solutions can also be considered as being negative aspects of social engineering.

In Romania, 90 % of IT managers are unaware that their systems may store confidential data, while 75 % of them stated that employees have portable storage devices and they could always store important files on them. Moreover, 25 % of companies said that along with the departure of employees, they had experienced significant losses of sensitive information. [22]

Considering all these aspects, it is essential that companies protect their data, by using both classical methods: antivirus, firewall, anti-malware, etc. and customized solutions that fully meet the users' requirements. Above all, the most effective method of combating social engineering remains staff's training.

7 Case Study

In order to support the facts stated in the present paper, we applied an anonymous questionnaire (used for research purposes only) containing 20 questions on 131 students of the Faculty of Economics and Business Administration distributed during an exam.

Some of the main objectives of this survey were:

- To identify the frequency of use of social networks and e-mail platforms;
- If the subjects use the same passwords and same user-name in multiple accounts;
- To determine the subjects' willingness to reveal their passwords and their significance;
- To determine whether students have provided passwords to others;
- To determine students' readiness to offer their passwords for various benefits (exam promotion, money);
- To identify whether the subjects were resistant to disclose they credentials under teachers' pressure;

DOI: 10.12948/issn14531305/18.2.2014.01

- Network administrators' influence on students;
- To reveal the size and reasons for which users are willing to allow other people use them accounts.

Centralising the answers received from the subjects resulted that they frequently use the email services and are quite active on social networking sites. To the first two questions ("Do you use frequently e–mail services", "Do you use social networking? ") 82%, 83% of respondents answered yes. This shows that they might be victims of social engineering attacks, especially phishing attacks and/or pharming.

The third question was whether they use the same username and password to different e-mail accounts; 69 % of respondents stated that they use the same username and password to different email accounts. This answer, correlated with the following question ("Do you Use the same password on e-mail accounts and social network accounts?") on which 62 % answered that they do not, we can deduce that the respondents are aware of the importance of using different passwords and usernames for each service they access.

Question number four was addressed in order to identify the availability of respondents to disclose anonymously, their most commonly used passwords. Thus 83 % of respondents revealed their most frequently used password. Analysing we found out that passwords of 52 % of the respondents had a low complexity, mostly consisting in names and other personal data. Also, 25 % of them have a special meaning passwords (question number six "What is the meaning of this password? ").

The goal on the seventh question was to identify individuals who have information about usernames or passwords of other people ("You happen to know the password from various e- mail systems, social network or portal of other people or colleagues?" "If yes, what is the most common password you have heard?"). 42 % of respondents said they know the other people' passwords, and, most of the times they set as passwords, names or other personal data.

To check confidentiality of passwords used the following question was asked: "Have you ever given your e-mail or portal password to someone" A significant proportion, 47 %, admitted that they did not respect the confidentiality of their passwords and have shared information about them with other people. This shows that some of the respondents are aware of the secrecy of these forms of identification. The same number of individuals confirmed that their account has been compromised at a particular point in time. Moreover, 50 % of respondents said that they have written passwords on sheets of paper, notebooks, post -it or student cards.

Regarding the conditions in which people surveyed would disclose passwords, 27% of them said they would disclose the password in exchange to 100 euros, while 35 % would disclose it in exchange to 200+ euros. Regarding the pressure exerted by a teacher on a student, promising to pass him, 44 % of individuals said they would provide information concerning their e- mail accounts.

The study shows that most respondents know their network administrators, but only 42 % are willing to provide them the password used to logging on to the portal. Also 12/20 students think that the password can be changed without their consent and that it is already known by administrators, but only 7 are think that this is impossible.

Questions number eighteen and nineteen were asked in order to identify the availability of those questioned tallow another person to use their account and under what reasons. Thus 53 % responded that they are willing to let other people to use their e - mail. The main reasons stated were: that a harmless email could not compromise their account's safety (16%) or that want to help a person in a difficult situation (21%), they would allow them under close supervision because nothing can happen (20%), 6% of respondents are willing to offer their help in case of an emergency , the same percentage say they do not trust others so they will not allow access. 23% of respondents , however, stated that it is not normal for people to use others' e- mail in order to send messages.

The questionnaire was applied to a total of 131 people, aged between 19 and 20 years, enrolled in the first year at Economics, in the presence of a teacher.

The questionnaire shows that the people surveyed do not manage their accounts and their passwords properly and could always be victims to a social engineering attack. I believe that the presence of a teacher and that the survey was done anonymously greatly influenced the responses of people interviewed.

References

[1] D. Irani, "Reverse Social Engineering Attacks in OnLine Social Networks", 2011.

[2] Federal Communications Commission, "Computer Security Notice: Social Engineering," Computer Security Week, p. 2, 2002.

[3] Enterprise Risk Management, "Social engineering: People Hacking," 2009.

[4] S. Tzu, "The art of war", Oxford: Oxford University Press, 1990, p. 66.

[5] J. Goodchild, "Social Engineering: The Basics.," 05.12.2012. [Online]. Available:<http://www.csoonline.com/article/514063/social-engineering-the-basics?page=3#psychology>. [Accessed 05 12 2012].

[6] H. Harley, "Re-Floating the Titanic: Dealing with Social Engineering Attacks", London: EICAR, 1998, p. 13.

[7] N. J. Golstein, S. J. Martin, R. Cialdini, 50 de secrete ale artei persuasiunii, Iaşi: Polirom, 2009, pp. 59-61.

[8] ISACA, "Social engineering," no. 7, june 2002.

[9] D. Lakhani, "Persuasiunea, arta de a obtine ceea ce vrei", Bucureşti: Almatea, 2009.

[10] K. F. Dutton, The Art of Split-Second Persuasion, Essex: Arrow Boks, 2011, pp. 23-45.

[11] "Three ways to persuade: Changingminds," [Online]. Available: <http://changingminds.org/disciplines/argument/making_argument/three_persuade.htm>. [Accessed 03 12 2012].

[12] R. Cialdini, "Influence: The Psychology of Persuasion", USA: William Morow and Co., 2006.

[13] Regulamentului privind managementul situaţiilor de urgenţă specifice tipurilor de riscuri din domeniul de competenţă al Ministerului comunicaţiilor şi tehnologiei informaţiei. Vol. cap. I. Art. 3.

[14] us-cert.gov., "Cyber security tips," [Online]. Available: <http://www.us-cert.gov/cas/tips/ST04-014.html>. [Accessed 03 12 2012].

[15] M. Cristea, "Atacuri DOS. Taxonomie, prevenţie, consecinţe şi atacuri mixte", Timisoara, 2011, p. 32.

[16] "Phreaking" [Online]. Available: http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Phreaking.html. [Accessed 15 11 2012].

[17] "Dumpster Diving," [Online]. Available:http://iss.net/security_center/advice/Underground/Hacking/Methods/WetWare/ Dumpster_Diving/default.htm. [Accessed 19.12 2012].

[18] A. Whitaker, "Top 10 Social Engineering Tactics," [Online]. Available:<http://www.informit.com/articles/ article.aspx?p=1 350956&seqNum. [Accessed 19 12 2012].

[19] I. Pascaru, "Incidentele de securitate-cum abordam aceasta problemă?," [Online]. Available: http://www.security.ase.md/publ/ro/pubro22.html. [Accessed 03 12 2012].

[20] "Small business security risk is high," [Online].Available:www.allbusiness.com/operations/3872586-1.html. [Accessed 01 03 2013].

[21] ISACA Whitepapers, Top 5 Social media risks for business, 2010.

[22] "Pierderea sau furtul datelor confidenţiale costă companiile," [Online]. Available: http://www.securitatea-informatica.ro/ securitatea-informatica/pierderea-sau-furtul-datelor-confidentiale-costa-companiile. [Accessed 15 12 2012].

DOI: 10.12948/issn14531305/18.2.2014.01

Valerică GREAVU-ŞERBAN has graduated the Faculty of Economics and Business Administration in 1998. He holds a PhD diploma in Cybernetics from 1999 and he had gone through all didactic positions since 2006 when he joined the staff of the Alexandru Ioan Cuza University of Iaşi, teaching assistant in 2006 and senior lecturer in 2009.

Oana ŞERBAN has graduated the Faculty of Economics and Business Administration in 2013 and actually is student at Master Level, specialisation Business Information Systems in Alexandru Ioan Cuza University of Iaşi. In 2013 was finalist in Economics Olympiad hosted in Timişoara.

DOI: 10.12948/issn14531305/18.2.2014.01