Journal of International
Academic Research for Multidisciplinary

A Global Society for Multidisciplinary Research

www.jiarm.com

Editorial Board

INVESTIGATING THE AWARENESS OF SOCIAL ENGINEERING ON CURRENT AND FUTURE EMPLOYEES

FELEX MADZIKANDA[1]
TALENT MUSIIWA[2]
MAXMILLAN GIYANE[3]
AMANDA MUTEMBEDZA[4]
PATRICK MAMBOKO[5]
TAURAI REBANOWAKO[6]

[1, 2, 3,4,5,6] Dept. of Computer Science and Information Systems, Midlands State University, Gweru, Zimbabwe

ABSTRACT

Information security can be divided into two main approaches - technological approach and human based security. In this paper we discuss and experiment the effect of social engineering which targets the human element of security to obtain access into a target company or system. Social engineering is continually on the rise as technical security measures are getting more and more complex and harder to break. Psychological vulnerabilities in human behavior allow a skillful social engineer to achieve his/her goals with great ease. In this paper, we investigate the awareness of current and future employees through two experiments. It has been noted that the majority of respondents are not aware of social engineering and can easily provide sufficient information for an attacker to gain access into a system. Several security measures have been highlighted that prevent or minimize social engineering.

KEYWORDS: Security, Social Engineering, Psychology, Vulnerability

I. INTRODUCTION

Social engineering refers to the manipulation and persuasion of a target individual by another person with the intention of performing a desired action. From the information security perspective, social engineering refers to the non-technical methods of penetrating a network or computer system by manipulating a user(or users) of a system into providing the required log-in credentials or performing the attacker's intended actions themselves. This form of deception is performed through meticulous planning which relies significantly in psychological vulnerabilities present in all human beings.

Although a social engineering attack may take various forms its main routes of attack are either face-to-face interactions or remotely in proactive form e.g. telephone conversation or through other technology such as emails. Social engineering and its various guises have been

around for a very long time. Its underlying principles have found their way into everyday life in many areas of interpersonal dealings between people. In order to achieve the upper hand, individuals have used social engineering tactics either consciously or unconsciously to achieve an advantage or to persuade their adversary into performing a desired action. Traditionally, social engineering has remained an unexplored area and continues to be so due to its cross-over nature between information security and human psychology. Because computer scientists are more familiar and comfortable to dealing with concrete technical issues they have somewhat neglected the deeper analysis of the ever varying and complex human psyche. However, significant advances and new research in human psychology have allowed us to identify common trends in human behavior and more worryingly the ease with which typical psychological vulnerabilities can be exploited by someone with good knowledge of these concepts. Also, due to many incidents of social engineering going unreported by targeted individuals or organizations for risk of loss of reputation or liability, it continues to remain an issue that not many people are aware of or think about on a regular basis.

II. Social engineer potential targets

It is currently a widely accepted view that the human aspect of information security is one of the most important elements of a secure and stable security infrastructure. The people using the technically secure systems must also themselves be penetration-proof because they are in fact the weakest link into those systems. In many occasions workers tend to violate security procedures because the procedures are inconvenient as they seek to accomplish their tasks faster. Below are some of the potential targets of a social engineer:

Office Staff – The most common target is office staff who have access to systems within the organization. In a survey carried out by Siemens Enterprise Communication, 85% of office workers were found to be vulnerable to social engineering attacks [2]. This highlights a worrying trend that could be quite costly, unless addressed, for an organization.

Receptionist – A receptionist is the first contact during a face-to-face social engineering attack at a company's premises and can provide much valuable access to waiting rooms or empty offices where there are internal login connection points to a social engineer. Due to the nature of their job, receptionists can be more willing to perform routine, everyday tasks such as forwarding a fax or sending an email as instructed by an attacker thus enhancing the obscurity of the social engineer during an attack.

Dumpster Diving – This refers to the activity of sifting through the refusal containers used by the target companies. Many companies fail to securely dispose their sensitive documents by

either shredding or carefully separating it from the rest of refuse for specialist disposal, thus giving an attacker a lot of important, sensitive information about the company. Often information gathered through this source could be sufficient enough for the attacker's purposes. Examples of documents that can be found in bins belonging to a target company could range from company's bank account details, employee name and ID lists, business documents regarding important products or dealings that could be beneficial to a competitor and others.

Outsourced Suppliers (Contractors) – An aspect often overlooked by companies when performing security evaluation is that of the security implications of hired contractors or security practices in place at the outsourcing companies who are being used for various services. The risk they present is that these companies can be a gateway to the targeted company if their security measures are weak for example the breaking in into an extranet might affect all the companies on the network. Many large organizations outsource their cleaning duties to a third party. Often cleaning of offices is carried out late in the evening after the end of a working day. Thus an attacker could try to gain access to the premises at these times by pretending to be a legitimate employee of the company and tricking cleaning personnel into allowing him or her into the building.

Passive attacks the main objective of passive social engineering is information gathering. This is a subtle attack that leaves the victim unaware that an attack is taking place.

Physical Security staff is often neglected when it comes to social engineering awareness and training. Due to the nature of their work they are assumed to be heavily security conscious thus are by default assumed knowledgeable about these threats. This is not the reality in that security staffs are often manipulated by an attacker pretending to be from a known associate of the target company, or under the pretext of having forgotten an ID but otherwise being a legitimate employer of the company.

Teleworker – An employee working from home with direct access to a company's network is just as valuable a target as one of their colleagues inside company premises. Teleworkers in a more relaxed home environment are likely to be less security conscious under the assumption that due to their physical distance from company networks no one would be interested to attack the company via them. This is of course a misguided view as a teleworker's system may in fact be the easiest point of entry into a company's network because it may not have strong security measures in place and is more subject to passive attacks

III. Social engineering attacks

Social engineering attacks can be classified into two main groups: technology-based deception involving the use of computer systems to carry out the attack and human-based deception requiring human interaction between the attacker and her intended victims [3], [4].

1) Human Based Social Engineering Attacks: The majority of social engineering attacks require some form of human interaction either face-to-face or over the phone. Mitnick identified several approaches [5] which include:

- Impersonating staff (often IT personnel)
- Pretending as someone in authority
- Posing as a new employee
- Intimidating the victim into providing help or information
- Reverse (social) engineering – where the attacker engineers the attack so that the victim will turn to the attacker for help consequently enabling the attacker to perform his/her desired action such as for example installing malicious software on user's computer.
- Posing as a partner company, client or law enforcement

2) Computer Based Social Engineering Attacks: One of the most popular and prevalent computer based social engineering attacks are phishing emails which target individuals in order to obtain private details such as bank account log-in information. Other types of attacks incorporating social engineering tactics include:

- Popup Windows e.g. advertising various product or competitions
- Email attachments e.g. containing viruses or backdoors
- Fraudulent Emails e.g. scam emails
- Dumpster diving
- Shoulder surfing i.e an attacker sneaks behind a target's back and put herself in a position to be able to see what the victim is typing for example a password

Warning Signs

Some of the common warning signs as identified by Mitnick [5], [6] that a social engineering attack is underway are:

- Refusal to give callback number - a good countermeasure when a victim becomes aware that an attack is under way is to request a callback number
- Out-of-ordinary request

- Claim of authority
- Stresses urgency
- Threatens negative consequences of noncompliance
- Shows discomfort when questioned
- Name dropping in order to gain trust and acceptance
- Compliments or flattery

IV. Psychology behind social engineering

Social engineering is made possible by "in-built" psychological weaknesses in human behavior. The main skill employed by a social engineer is that of persuasion. Peripheral route of persuasion [7] allows an attacker to solicit the acceptance of a message by a victim based on the now widely accepted six factors of persuasion identified by Dr. Cialdini: (i) reciprocation, (ii) consistency, (iii) social validation, (iv) likeability, (v) authority, and (vi) scarcity [8] Often and attacker during the early stages of an attack will use reciprocity by providing gifts, favors as well as concessions towards her victim so that at a later stage the victim feels obliged to reciprocate back by doing the attacker a favor when requested. A skillful attacker is also aware of the strong inclination of people towards being consistent in their action. They will use this persuasion tactic on their victim by first getting them to commit to a much smaller request such as for example providing some trivial non-sensitive information so that at a later stage the victim is less likely to decline a request for now sensitive information since he/she has already complied to a few smaller less significant information requests. Social validation in the context of a social engineering attack can take different forms. Firstly, an attacker can notify the victim that many of his/her colleagues have already complied with similar requests thus putting pressure on the victim and creating the assumption that it is fine to cooperate with such requests. Secondly, through a technique called name-dropping the attacker will intentionally mention the names of colleagues of the victim, obtained through the information gathering stages of the attacker, in order to make the attacker more trusted i.e. socially validate his/her status. Liking is perhaps one of the most potent weapons in a social engineers arsenal. It allows the attacker to create immediate rapport with their victims thus also establishing a certain level of trust which will allow them to achieve their objectives unobstructed. Through, extensive research the attacker can obtain trivial information about the attacker such as where they are from, their hobbies, schools they went to etc and on the course of interacting with them she will often pretend to have the same background and/or have gone to the same school, have the same hobbies as the victim in

order to build rapport and liking. One of the most popular pretexts adopted by the social engineers is that of a high position manager requesting immediate help or information. In many organizations with a strong hierarchical structure people will tend to comply blindly to requests made by their supervisors or managers so that not to appear obstructive and potentially risk their relationship with them or even their job. Therefore, by pretending to be someone in authority, social engineers often find an easy path to success and are able to obtain immediate results. The concept of scarcity is engineered into various situations. The social engineer will often appear to be in a hurry, have limited resources or appear to be in a real emergency thus employing the idea of scarcity in terms of time, information and resources. All of the above factors used on their own or combined have been shown to provide concrete results in various experiments [9]. They are the fundamental building blocks of persuasion recognized and classified originally by Aristotle's three types of persuasive proofs: Ethos (ethical-character and reputation factors), Pathos (emotional appeal) and Logos (or logical, the actual words used). [10]

V. Methodology

To test the awareness to social engineering tactics, fifty staff members of a university were identified for the research. A fake commercial bank of Zimbabwe website was hosted on our machine on the university network. All the identified users were sent an electronic mail with an attachment from an unknown user. The subject of the electronic message was written," Hurry!! Hurry! Limited loans at the Commercial Bank of Zimbabwe". The message had accurate bank details and proved to be a genuine letter from the bank and requested users to click a link for them to register and get an instant loan from the Commercial Bank of Zimbabwe. The link would then direct users to our web server where the users would fill in their registration information include their profiles, preferred usernames and passwords and card banking details. The technique used is mainly called phishing.

The other experiment conducted was to check whether students (future employees) were also familiar with social engineering. The attacker simply visited a computer laboratory smartly dressed in a suit with a security badge and holding a clipboard with forms requesting the first fifty students to fill in their name, surname, date of birth, name of parents, hobbies and their usernames and passwords as they entered the computer lab.

VI. Results and Discussion

Table 1: Phishing Attack

Web link	Respondents
Opened link and registered	25
Opened link and did not register	10
Did not open link	15

Results show that 15 staff members did not open the link to our web server. Amongst the users who did not open the link, said they were aware of social engineering attacks especially when they received an electronic mail from an unknown sender. Further discussions with this group showed that they were from the department of computer science and had a vast background in computer security and they had an understanding in the concept of phishing. They also highlighted that they feared the issue of viruses that may be activated by opening links to different websites. The 25 targets who opened the link to our webserver admitted that it was due to the subconscious psychological engineering of the electronic mail subject that was scribed,"Hurry!! Hurry! Limited loans at the Commercial Bank of Zimbabwe". They confessed that they registered and were actually waiting for the bank to contact them in connection with the loans. Questioned if they knew of phishing or social engineering in general, they professed ignorance and that it was their first time to hear those terms. Amongst the group that opened the link and did not register said they became suspicious when they noticed that a lot of personal information was being required for them to just register. On this group some said they had heard of hackers who break into systems and thus they feared to input their credit details on the registration process. The remainder of the people who opened the link and did not register said when they visited the website; they noticed that there were no digital certificates that authenticated the site as a genuine Commercial Bank of Zimbabwe website. From the analysis of the results we note that a lot of people are not aware of social engineering tactics and there is need to educate the staff on the issue of security so as to protect organizational assets.

Table 2: Computer lab social engineering

Entrance form	Respondents
Fully filled entrance form	30
Partially filled entrance form	15
Did not fill entrance form	5

When the thirty students who filled the entrance form to the computer laboratory were asked why they filled the form yet they are usually not requested to do so, they replied that by noticing the security guard at the door and smartly dressed they thought he was performing his university duty and thus they had to comply with him so that they easily gain access into the laboratory. Asked whether they knew that their usernames and passwords were their privacy, they confessed that they knew thus later realizing that they had been tricked and had simply filled the forms unconsciously. The students who partially filled the entrance form did not input their usernames and passwords but had filled the rest of the information. They said they knew that usernames and passwords were their privacy. Through further discussions, it was noted that although the group did not input their usernames and passwords, most of their password were their names, date of birth, surnames, and the names of their parents which they had filled on the forms. This also shows that they were also a victim of passive social engineering by providing important information unknowingly. From this we noted that students can be aware that their usernames and passwords are private information but still fail to acknowledge that these usernames and passwords come from their characteristics and profiles that they gave out to the fake security guard. The five students who did not fill the entrance form questioned the security guard why he wanted a lot of their personal information and that they knew by providing such information their accounts could be illegally accessed. Asked if they knew of social engineering they said they did not know but they were aware that their usernames and passwords are private and should not be given to any third party.

VII. Countermeasures and Defenses

The fundamental countermeasures model against social engineering attacks includes the following 3 fundamental steps as highlighted in the Extended Model by Ian Mann[11]:

1. Barriers on availability of target information or system in public domain – the initial control lie on the outer layer of security by putting certain steps in place in order to reduce visibility of company details and making it difficult and inconvenient for an attacker to gather knowledge about a target company or system. This can include information such as, contact names on company website, contact information related to companies website often available from Internet Domain Name Servers, etc.

2. Staff Awareness/Education and Established Incident Response Procedures – It is vital that all levels of staff are made aware and educated on the risk of social engineering regardless of their level of technical security expertise or position held. Members of staff from all positions, ranging from lower to higher ranks are vulnerable thus they should all be included

in the educational program. Also, included in the awareness program must be agreed response procedures that all staff must adhere to in the event that an attack is discovered.

3. System Protection Mechanisms refers to the technical measure that could be put in place to stop a social engineer in succeeding. A current popular example being undertaken by many organizations is that of 2-factor authentication. By implementing 2-factor authentication mechanisms in conjunction with one another such as for example “chip & pin” technology or biometrics with tokens, the company would make it very difficult for an attacker. However, it must be noted that even these defenses are liable to fall prey to a social engineering attack since a skillful social engineer can simply let the target authenticate herself using biometrics or token based technology, to access the system and then manipulate them into performing the actions the attacker has planned. Regular penetration testing and security audits must be performed to test their effectiveness and discover potential weaknesses that must be addressed. Many penetration testing and security audits now include standard, social engineering testing due to the proliferation of this practice by attackers.

VIII. Conclusion

In this paper we discussed the psychological tricks that skillful social engineers have at their disposal when it comes to deceiving and persuading their victims to perform the required action. However, it is often recognized, as highlighted by Okenyi and Owens [12] that social engineers do not only exploit the psychological weaknesses or the trusting nature of people but also their lack of security education and awareness makes it much more easier for an attacker to be successful. Social engineering is a problem that will continue to proliferate as technical advances in security products make it harder and harder for attackers to break a system via technological means. The human approach is a lot easier and provides quicker results. We have shown that through passive means, an attacker can easily gain full access to a victim’s system. This passive approach also reduces considerably the risk of discovery, another reason why social engineering is a preferred weapon in an attacker’s arsenal compared to a technological attack which in many cases would leave plenty of electronic traces. Although, difficult to eradicate in its entirety, social engineering could be significantly hampered with good education and awareness programs for staff in all positions of a company. It is imperative that the training is on-going and up-to-date so that members of staff do not become complacent and begin to forget what they have been taught. Regular security audits must also incorporate testing for social engineering vulnerabilities and amend weakness if any are discovered. It is recommended that the student’s i.e our future employees

be equipped in the field of computer security so that they carry and practice the knowledge at their workplace.

REFERENCES

1. T. Qin and J. K. Burgoon. An investigation of heuristics of human judgment in detecting deception and potential implications in countering social engineering. IEEE Intelligence and Security Informatics, May: 152–159, 2007.
2. S. E. C. Group. 85 per cent of office workers duped by social engineering, May 2009.
3. R. Power and D. Forte. Social engineering: attacks have evolved, but countermeasures have not. Computer Fraud & Security, Elsevier, Volume 2006, Issue 10:17 – 20, October 2006.
4. R. Gulati. The threat of social engineering and your defense against it, October 2003.
5. K. Mitnick and W. L. Simon. The Art of Deception – Controlling the Human Element of Security. Wiley Publishing Inc, 2002.
6. T. Thornburgh. Social engineering: The "dark art". In Proceedings of the 1st annual conference on Information security curriculum development, pages 133 – 135. ACM, 2004.
7. M. Workman. Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of American Society For Information Science and Technology, 59(4):662–674, 2008
8. R. B. Cialdini. The science of persuasion. Scientific American, February:76 – 81, 2001.
9. P. Robert B. Cialdini. Influence: The Psychology of Persuasion. Harper Business, revised edition edition, 2007.
10. J. Borg. Persuasion - The Art of Influencing People. Pearson Education Ltd, 2nd edition edition, 2007.
11. I. Mann. Hacking the Human - Social Engineering Techniques and Security Countermeasures. Gower Publishing Ltd, 2008.
12. P. O. Okenyi and T. J. Owens. On the anatomy of human hacking. Information Security Journal: A Global Perspective, 16:6:302–304, 2007.