IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 5, Ver. V (Sep. - Oct. 2016), PP 94-100
www.iosrjournals.org

Social Engineering: Hacking a Human Being through Technology

Akshat Jain[1], Harshita Tailang[1], Harsh Goswami[1], Soumiya Dutta[1],
Mahipal Singh Sankhla[2], Rajeev Kumar[3]

[1]Students of Bachelor of Technology Computer Science and Engineering, School of Computing Science & Engineering, Galgotias University, Greater Noida.
[2]Student of M.Sc. Forensic Science, Division of Forensic Science, School of Basic and Applied Sciences, Galgotias University, Greater Noida.
[3]Assistant Professor, Division of Forensic Science, School of Basic and Applied Sciences, Galgotias University, Greater Noida.

Abstract: *Social engineering is the art of extracting classified information by psychological manipulation. It is a strategical attack that depends on human interaction, a complex fraud system, tricking individuals into giving their password and bank information. It is a simple preference of criminals to exploit peoples trust rather than technology, since it is easier to exploithumans' natural inclination to trust. Lack of awareness has caused for such social engineering crimes to have been overlooked and not treated as a major threat. The objective of this review paper is to lay emphasize on the human element which is the biggest threat to the security of a company or organization and to highlight social engineering based attacks as one of the major threats to the society. The increase in the usage of such scams and con attacks on the weakest security links to information: humans, have caused major individual and occupational loss. The problem with social engineering is that it is among the most under researched and most effective cyber-crimes. It is viewed outside the domains of computer security since there are no technical solutions to this problem.*

Keywords: *Social Engineering, Psychology, Attacks, Human, Cyber-crime, Security etc.*

I. Introduction

Social Engineering is the art of exploiting the weakest link of information security systems: the people who are using them **[1].** Information systems (IS) security management depends not only on technological measures but also on managerial endeavors. A plethora of technological methods have been developed to address various security issues but human factors that contribute to significant security breaches have been comparatively neglected**[2].**Within the context of computer and information security, social engineering (SE) is a combination of techniques used to manipulate victims into divulging confidential information or performing actions that compromise security**[3].**As clearly stated by various authors, the human element is the 'glitch' or vulnerable element within security system **[4,5,6,7].** It is the basic 'good' human nature 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 **[4,7].**

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 possess 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. There are two main perspectives of social engineering - the psychological perspective and the computer science perspective. The psychological perspective focuses on the emotional state and cognitive abilities of the individual while the computer science perspective focuses on information sensitivity, one of the cornerstones of information security **[8].** A social engineer is considered to exist under the white hats society, welcome the information that is seemingly harmless for an organization; as it may play a crucial role in convincing others they are real**[9,10,11,12].** The secret of success for social engineering is that users are very much prone to being deceived if you gain their trust and if they are manipulated in a certain manner **[13,14].**

Social engineers frequently follow a certain route where the intention can be just the opposite in some cases. This is called reverse tricking **[10].** Essentially, the attacker creates a problem where the user will be directly affected; then contact is made by telephone leaving a number for the user to call back. This so called 'penetration' is a technique where an outsider disguises as a member of organization staff to obtain passwords, etc.**[15].**

Biggest Threat: The human element

The biggest threat to the security of a company is not a computer virus, an unpatched hole in a key program or a badly installed firewall. In fact, the biggest threat could be you and you should know, says Kevin Mitnick. Mr. Mitnick won notoriety as a hacker during the late 80s and early 90s and his exploits regularly became front page news.He served a one-year jail sentence, but on his release found it hard to give up his obsession. The FBI was soon looking for him again for breaking the terms of his parole, which tried to restrict what he could do with computers. He evaded capture for more than two years and won fame because of a series of articles that inaccurately portrayed him as some sort of master hacker criminal. Mr. Mitnick even had to get permission from his probation officer to use a computer to write his book, The Art of Deception, which is all about the biggest threat to the security of all companies: their own employees. The book details the ways that employees can inadvertently leak information that can be exploited by hackers to compromise computer systems."The lethal combination is when you exploit both people and technology," Mr. Mitnick said.

Those people are especially useful when they have access to the core computer systems that hackers would otherwise struggle to penetrate. Most of the time organizations overlook that human element. Armed with a little knowledge, a hacker can sound like an employee of a firm and get other workers to inadvertently supply them with enormously useful information **[16].**

The Art of human hacking

It's natural to yearn for a feeling of absolute safety, leading many people to settle for a false sense of security. Consider the responsible and loving homeowner who has a Medico, a tumbler lock known as being pickproof, installed in his front door to protect his wife, his children, and his home. He's now comfortable that he has made his family much safer against intruders. But what about the intruder who breaks a window, or cracks the code to the garage door opener? How about installing a robust security system? Better, but still no guarantee. Expensive locks or no, the homeowner remains vulnerable. Why? Because the human factor is truly security's weakest link. In most cases, successful social engineers have strong people skills. They're charming, polite, and easy to like--social traits needed for establishing rapid rapport and trust. An experienced social engineer is able to gain access to virtually any targeted information by using the strategies and tactics of his craft. Savvy technologists have painstakingly developed information-security solutions to minimize the risks connected with the use of computers, yet left unaddressed the most significant vulnerability, the human factor. Despite our intellect, we humans - you, me, and everyone else - remain the most severe threat to each other's security **[17].**

Psychological Manipulation

Recent research has discovered that there are certain terms and techniques that are associated with SE and go perhaps far beyond technology and more so into human error and social psychology. Three key aspects of social psychology, alternative routes to persuasion (i.e., central route and peripheral route), attitudes and beliefs that affect human interactions, and techniques for persuasion and influence, could help explain the emotional cues for manipulated SE attacks **[18].**In a central route to persuasion, SE attackers persuade victims to provide desired information without fabricating unreal scenarios. Thus, this comparatively direct route, which depends on the responder’s logical thinking toward the marshaled information from the attacker, does not normally succeed. The other route, peripheral route to persuasion, can be leveraged by SE attackers to bypass logical argument and counterargument and seek to trigger intrusion. In the peripheral route to persuasion, the attacker tends to make the intended victim more susceptible to persuasion by triggering strong emotions such as fear or excitement in order to interfere with the victim’s ability to respond. Attitudes and beliefs refer to the differences between the victim’s attitude and beliefs about the SE attacker and SE attacker’s attitudes and beliefs about his anticipated or definite victims. Rooted in social psychology, persuasion and influence techniques rely on peripheral routes to persuasion that are effective to influence others. Six factors can constitute effectual persuasions: authority, scarcity, liking and similarity, reciprocation, commitment and consistency, and social proof **[19].**Furthermore, SE attacks are categorized into human-based and technology-based intrusions. Human-based attacks are interactions between the attacker and the victim who possesses valuable information. In contrast, technology-based attacks access confidential information by employing computer software programs such as pop-up windows, e-mail attachments, and websites, etc. While maliciously generated e-mail attachments and websites seek the victim’s natural tendency to trust others to divulge information or perform actions, a vicious script-embedded pop-up window manipulates the victim’s psychological fear of getting into trouble by repeatedly prompting the victim to re-enter his/her user username and password because the network connection was interrupted and the window will surreptitiously deliver the information entered to the attackers**[2].** A typical SE attack is composed of four steps: information gathering, relationship development, exploitation, and execution. An SE attacker initially gathers information about the target(s) such as names, phone numbers, birth dates from publicly-accessible information such as directories and organizational charts.

Applying this information, he then can try to build rapport with the intended victim to gain his/her trust. Exploiting the established trust, the SE attacker can then persuade the victim to perform desired actions (i.e., revealing confidential information) which would not normally occur otherwise. In the last stage, the attacker uses the information collected from the victim to carry out attacks **[20].**

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 **[21,22].** 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 **[22,23].** 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 **[22].** 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 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**[21,22].** 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. Based on this theory, a decision to disclose information will be based on risk-benefit analysis. Decision analysis, a technology based on subjective expected utility theory, attempts to aid better decision making. 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. 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 **[21].** 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**[8].**

Common Personality Traits

An article entitled People Hacking [**24**], Harl discusses the following exploits, and discusses how various personality traits enhance the possibility of successful social engineering. When present, these traits increase the likelihood of compliance:

Diffusion of responsibility - If the target can be made to believe that they are not solely responsible for their actions, they are more likely to grant the social engineer's request. The social engineer creates situations with many factors that obfuscate and dilute personal responsibility for decision making. The social engineer may drop names of other employees involved in the decision making process, or claim another employee of higher status has authorized the action.

Chance for ingratiation - If the target believes compliance with the request enhances their chances of receiving benefit in return, the chances of success are greater. This includes gaining advantage over a competitor, getting in good with management, or giving assistance to an unknown, yet sultry sounding female (although often it's a computer modulated male's voice) over the phone. There is a belief in the hacker community that technological people who have the keys to the shop often lack the skills to carry on adequate social relationships. Social engineers are not above using any form of influence when attempting to gain information.

Trust Relationships - Often times, the social engineer expends time developing a trust relationship with the intended victim, then exploits that trust. Following a series of small interactions with the target that were positive in nature and problem free, the social engineer moves in for the big strike. Chances are the request will be granted.

Moral duty - Encouraging the target to act out of a sense of moral duty or moral outrage enhances the chances for success. This exploit requires the social engineer to gather information on the target, and the organization. If the target believes that there is a wrong that compliance will mitigate, and can be made to believe that detection is unlikely, chances of success are increased.

Guilt - Most individuals attempt to avoid guilt feelings if possible. Social engineers are often masters of psychodrama, creating situations and scenarios designed to tug at heartstrings, manipulate empathy, and create sympathy. If granting the request will lead to avoidance of guilty feelings, the target is more likely to comply. Believing that not granting the requested information will lead to significant problems for the requestor is often enough to weigh the balance in favor of compliance with the request.

Identification - The more the target is able to identify with the social engineer, the more likely the request is to be granted. The social engineer will attempt to build a connection with the target based on intelligence gathered prior to, or during the contact. Glibness is another trait social engineers excel at, and use to enhance compliance.

Desire to be helpful - Social engineers rely on people's desire to be helpful to others. Exploits include asking someone to hold a door, or with help logging on to an account. Social engineers are also aware that many individuals have poor refusal skills, and rely on a lack of assertiveness to gather information.

Cooperation - The less conflict with the target the better. The social engineer usually presents as the voice of reason, logic, and patience. Pulling rank, barking orders, anger, and annoyance rarely works for gaining compliance. That is not to say that these ploys aren't resorted to as a last ditch attempt to break unyielding resistance **[25].**

Common Social Engineering Threats

These are the some of the common attacks/exploits that a social engineering hacker uses:

Baiting/Trojan horse—an exploit that uses malware infected physical media (e.g., CD-ROM, USB drive) to perpetuate an attack. Looking legitimate, the Trojan horse relies on the curiosity or greed of the victim who finds and uses the device, enabling installation of the malware on the targeted organization’s internal computer network.

Fraudulent websites and social media—an exploit that uses a fraudulent website (or social media site such as Facebook) to trick the victim into clicking on a link that downloads malware to the victim’s computer.

Pretexting/reverse social engineering—an exploit that creates and uses a real or an invented scenario (the pretext) to increase the chance that a targeted victim will divulge information or perform actions that would be unlikely in ordinary circumstances. A sophisticated example of pretexting is reverse social engineering, which was described above in the context of non-electronic social engineering scams. When applied to electronic (online) interactions, reverse social engineering has proven to be a very effective computer-based exploit.

Salient Characteristics	Typical Information Requested	Potential Consequences/ Outcome
Appeal • usually good news or bad news • sense of urgency • sensitive or confidential matter • impersonating known sender **Desired response** • provide specific information • update personal/account information • click on link in email message • open an attachment **Suspicious indicators** • generic greetings • suspicious context • poor grammar or spelling • strange or unusual sender • incorrect information • illegitimate embedded URLs	• account information • user name • password and PIN • credit card number • Social Security number • bank account number • bank routing number • email address • telephone number • other personal information	• financial loss • identity theft • personal, confidential, or proprietary information stolen • intellectual property stolen • computer compromised, malware or virus implanted • data, software, and/or hardware assets manipulated or destroyed • personal or organizational embarrassment • political gain • denial of service

Table 1: Social Engineering Characteristics **[29]**

Phishing/spear phishing—an exploit generally defined as a phisher impersonating a trusted third party to gain access to private data. Typically, the phisher sends an email that appears to come from a legitimate business or individual (e.g., a bank, credit card company, or fellow employee) requesting verification of information and warning of dire consequence if it is not provided. The email usually contains a link to a fraudulent web page that appears legitimate—sometimes with company logos and content—and requests private information (e.g., Social Security number, bank account number, banking PIN). Social engineering, and particularly phishing, has become more sophisticated over time: attackers learn which techniques are most effective and alter their strategies accordingly **[26,27].** An example is spear phishing, in which the attacker initially gathers personal information about the target victim and uses it to tailor the phishing scheme, which increases the probability of success **[28].** As seen in Table I, the information sought and potential outcomes are, not surprisingly, much the same as the targeted information and consequences in cyber-attacks generally, although the methods of attack differ somewhat, especially regarding salient characteristics in the first column of the table. These characteristics inform our approach to describing social engineering incidents and identifying patterns in these attacks **[29].**

Counter Measures

Following are some measures that individuals and companies should take to minimize the risk of these attacks:

- Never divulge personal information via phone or on unsecure websites.
- Do not click on links, download files, or open email attachments from unknown senders.
- Be sure to make online transactions only on websites that use the https protocol. Look for a sign that indicates that the site is secure (e.g., a padlock on the address bar).
- Beware of phone phishing; never provide personal information over the phone if you receive a call. Beware of emails that ask the user to contact a specific phone number to update user's information as well.
- Beware of links to web forms that request personal information, even if the email appears to come from a legitimate source. Phishing websites are often exact replicas of legitimate websites.
- Adopt proper defence systems such as spam filters, anti-virus software, and a firewall, and keep all systems updated.
- For a social network user, it's fundamental to trust no one and reveal only a limited amount of information. Never post personal information, such as a vacation schedule and home photos. Never click on links and videos from unknown origin and never download uncertified applications **[30].**

What can your company do to prevent being victimized by these types of attacks?

- Humans need to be trained – they are the weakest link. Companies should employ, at minimum, a bi-annual training geared towards each user group (end-users, IT staff, managers, etc.) so that everyone is aware of the latest attacks.
- Employees should be tested by having an outside party conduct a social engineering test. These kinds of tests help keep the employee on their toes and more likely to avoid the attacks.
- Since these attacks are on the rise, a number of new defences have been developed. AppRiver is a great Spam and Virus email filter that can block a large number of phishing exploits before they even reach the internal servers. If they happen to get through, an endpoint protection system that can block the latest malware is probably your best bet at stopping the attack**[31].**

II. Discussion

Social engineering is one of the most ongoing threats that's lurking constantly over the network security system. The SE attackers prey on the weakness of human nature and use manipulation to breech the security system. Since hacking a high tech security system is difficult it is one of the most effective of all cyber-crimes. The high success rate is due to lack of awareness among people, and controlling human nature is near to an impossible task. People are prone to manipulation tricks. Since there is no direct technical method to detect and prevent SE attacks, this makes it one of the most severe threats to the individuals as well as the companies.

The only way to curb such ongoing epidemic of SE, is by spreading awareness among individuals to not fall for such tricks. The organization can reduce the impact of Social Engineering attacks by implementing a comprehensive information security strategy. Such strategy would include measures ranging from publishing a well written security policy, implementing ongoing security awareness and education programs, following through with auditing programs to monitor policy compliance, installing security devices to prevent unauthorized physical access and buying insurance against security attacks**[32].**But SE is indeed a very serious threat and has caused great damage to individuals as well as organizations and measures are needed to keep these attacks at check.

III. Conclusion

Through this review paper we can conclude that how much strong a company's security is, there is always a loophole of manipulation since human trust is a liable factor. Social engineers manipulate their victims into giving their personal information and bank details as humans can be manipulated easily due to their tendency to trust, which can be taken a great advantage of by these attackers. A social engineer need not be an expert on networks or security. The attackers either fool the victims or get the information without the victim's knowledge. Social engineers are nothing but con mans. Controlling human nature is near to an impossible task. Therefore, alongside advance techniques to curb various cyber-crimes, we also need to consider the human factor which is liability to the security because it's not possible to just create a system without any human participation. This human factor is the weakest link in security which can be secured not by one-time training but only by an ongoing process of amelioration. There is no direct solution to this impending threat that constantly lurking over the security system. The only solution is to spread awareness among individuals so that they do not fall prey to these attackers. A lot of harm has already been caused because of them. This is one of the most effective and undetectable cyber-crime.

References

[1]. Huber M., Kowalski S., Nohlberg M., Tjoa S., "Towards Automating Social Engineering Using Social Networking Sites," Computational Science and Engineering, 2009, Volume: 3, Digital Object Identifier: 10.1109/CSE.2009.205, Publication Year: 2009, Page(s): 117 – 124.

[2]. Xin (Robert) Luo,Richard Brody, Alessandro Seazzu, Stephen Burd, "Social Engineering: The Neglected Human Factor for Information Security Management", Information Resources Management Journal, 24(3), 1-8, July-September 2011

[3]. Mitnick, K., & Simon, W. (2002). The Art of Deception: Controlling the Human Element of Security. New York, NY: John Wiley & Sons.

[4]. 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.

[5]. 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.

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

[7]. 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.

[8]. Monique Bezuidenhout, Francois Mouton, H.S. Venter, "Social Engineering Attack Detection Model: SEADM,"DOI:10.1109/ISSA.2010.5588500 , Source: IEEE Xplore , Conference: Information Security for South Africa (ISSA), 2010

[9]. Mataracioglu, T., 2009. Social Engineering: Attack and Protection Methods. TUBITAK BILGEM Cyber Security Institute – Course Notes.

[10]. Mitnick, K.D. and Simon, W.L., 2002. The Art of Deception. Indianapolis: Wiley Publishing

[11]. Arslantas, M.B., 2004. Methods Used in Internet Crime. MEB Head Office of Information Technologies. Available from: http://egitek.meb.gov.tr/EgitekHaber/EgitekHaber/s75/bılsım sucları.htm

[12]. Hasan, M., Prajapati, N., Vohara, S., 2010. Case Study on Social Engineering Techniques for Persuasion. International Journal on Applications of Graph Theory in Wireless Ad Hoc Networks and Sensor Networks.

[13]. Slatalla, M., Quittner, J., 1995. Masters of Deception: The Gang that Ruled Cyberspace. New York: Harper Collins.

[14]. Voyager, 1994. Janitor Privileges, 2600: The Hackers' Quarterly

[15]. TolgaMataracioglu, SevgiOzkan, Ray Hackney, "Towards a Security Lifecycle Model against Social Engineering Attacks : SLM-SEA," Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, Illinois, August 15-17, 2013.

[16]. Mitnick, Kevin. "How to Hack People." BBC News Online, October 14, 2002. URL: http://news.bbc.co.uk/1/hi/technology/2320121.stm (Aug 12, 2003)

[17]. The Art of Deception by Kevin D. Mitnick, William L. Simon and Steve Wozniak, ISBN 0-471-23712-4

[18]. Peltier, T. (2006). Social Engineering: Concepts and Solutions. Information System Security, 15(5), 13–21. doi:10.1201/1086.106589 8X/46353.15.4.20060901/95427.3

[19]. Rusch, J. (1999). The Social EngineeringofInternetFraud. Paper presented at the INET'99 Conference, San Jose, CA.

[20]. Allen, M. (2006). SocialEngineering: AMeanstoViolateaComputerSystem. Bethesda, MD: SANS Institute.

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

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

[23]. 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.

[24]. Harl. "The Psychology of Social Engineering." Text of Harl's talk at Access All Areas III, 05/07/97. URL: http://www.vampi.users1.50megs.com/social.html

[25]. Stevens, George. "Enhancing Defenses against Social Engineering". GIAC Practical Repository. URL: http://www.giac.org/practical/gsec/George_Stevens_GSEC.pdf (Aug 12, 2003).

[26]. Downs, JS, MB Holbrook, & LF Cranor. "Decision Strategies and Susceptibility to Phishing." Symposium On Usable Privacy and Security (SOUPS), July 12-14, 2006, Pittsburgh, PA, USA.

[27]. Downs, JS, M Holbrook, and LF Cranor. "Behavioral response to phishing risk." (Institute for Software Research, Paper 35), APWG eCrime Researchers Summit, Pittsburgh, PA, October 4-5, 2007.

[28]. O'Brien, T.L. "Gone spear-phishin'." The New York Times (4 December 2005) http://www.nytimes.com/2005/12/04/business/yourmoney/04spear.html?pagewanted=1&ei=5088&en=2f313fc4b55b47bf&ex=1291352400&partner=rssnyt&emc=rss&_r=0

[29]. Frank L. Greitzer, Jeremy R. Strozer, Sholom Cohen, Andrew P. Moore, David Mundie and Jennifer Cowley," Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits", DOI: 10.1109/SPW.2014.39 Conference: 2014 IEEE Security and Privacy Workshops, Workshop on Research in Insider Threat, At Oakland, California

[30]. Social Engineering Attacks: Common Techniques & How to Prevent an Attack, by Pierluigi Paganini. https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
[31]. Social Engineering Attacks: Common Techniques & How to Prevent an Attack, by Paul Kubler. https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack
[32]. "The Threat of Social Engineering and Your Defense Against It" by Radha Gulati, GIAC Security Essentials (GSEC) Certification Practical AssignmentVersion 1.4b – Option 1