Journal of Cybersecurity Education, Research and Practice

Volume 2019 | Number 2 Article 4

2019

Sit Back, Relax, And Tell Me All Your Secrets

Sarah Kirk
Middle Georgia State University, sarah.kirk@mga.edu

Daniel Foreman
Middle Georgia State University, daniel.foreman@mga.edu

Cody Lee
Middle Georgia State University, cody.lee@mga.edu

Shannon W. Beasley
Middle Georgia State University, shannon.beasley@mga.edu

Sit Back, Relax, And Tell Me All Your Secrets

Abstract

The goal of this research is to describe an active learning opportunity that was conducted as a community service offering through our Center for Cybersecurity Education and Applied Research (CCEAR). As a secondary goal, the participants sought to gain real world experience by applying techniques and concepts studied in security classes. A local insurance company tasked the CCEAR with assembling a team of students to conduct penetration testing (including social engineering exploits) against company personnel. The endeavor allowed the insurance company to obtain information that would assess the effectiveness of employee training with regard to preventing the divulgence of sensitive information. The team of students assembled organized, planned and executed all penetration testing. This academic opportunity allowed the students to build experience transacting the social engineering while laying the groundwork for future projects that will allow additional students to build and expand the process outlined in this study.

Keywords

penetration testing, social engineering

INTRODUCTION

In the case of network and information security, individuals entrusted with securing the digital assets of a business look for ways to guarantee that their networks and intellectual property are protected as promised to stakeholders. Oftentimes, the best way to test the strength and fitness of a proposed system is to subject the solution to scrutiny and potential failure. A dynamic approach to assessing strengths and weaknesses takes the form of penetration testing. An initial step to penetration testing focused on by the assembled group of students is social engineering. This paper describes a small-scale penetration exercise designed and carried out as part of an independent study by a group of information technology students.

Social engineering endeavors attempt to exploit human nature to gain access or obtain sensitive information. A knowledgeable social engineer can easily capitalize on a basic human characteristic: the tendency to extend trust when provided plausible information. While this characteristic is not the only feature of human nature exploited by social engineers, it does provide a good starting point for building a relationship between the social engineer and the chosen target. In the case of the team assembled for this this project, the students began to create a script and practice a social exchange of dialog between actors portraying the roles of perpetrator and victim. This practice served to smooth the delivery of the perpetrator and identify potential sticking points in the exchange (Meinert, 2016).

Employee behavior can be viewed as the result of personal traits, organizational culture, and outside influence resulting in repeatable patterns of action – the key is for the perpetrator to identify and exploit available weaknesses (Rogers, 2005). A common flaw in many business organizations is the fact that management fails to properly address the human element when implementing information security protocols and procedures (Knowles, 2002). It is with this knowledge in mind that a local insurance company asked the Center for Cybersecurity Education and Applied Research (CCEAR) at Middle Georgia State University to assemble a team of three students that would be allowed to conduct social engineering exploits and penetration testing against the company's employees.

Since the project was begun through the CCEAR, the agreement specifying that penetration testing including social engineering in the physical, telephone, and remote environments of the company were permitted as long as there was no disclosure of results to anyone outside the company for a period of two years following the testing and no disclosure of sensitive information to anyone outside the company. Additionally, any required Institutional Review Board (IRB) applications and university requirements were met an outlined in the project as presented to the assembled team and its supervising faculty member. Subsequently, the assembled students were required to agree to the rules and stipulations for conducting the activity as specified by the supervising faculty member, the university, the CCEAR, and the insurance company to be studied.

PENETRATION TESTING / SOCIAL ENGINEERING

"Penetration testing is a comprehensive method to test the complete, integrated, operational, and trusted computing base that consists of hardware, software, and people" (McGraw, 2006). Testing identifies weak links that can be exploited in a company or corporation. Discovering the presence of security vulnerabilities can aid in preparing a plan to fend off attacks, which is an invaluable tool in securing information. The advantages of testing include: soliciting third party

opinions, identifying potential vulnerabilities, and determining the cyber defense capabilities of an entity. While testing is an excellent tool in modern security, there are several disadvantages to utilizing this technique (Furtuna, 2015). First, it can be difficult or expensive to find a knowledgeable, reputable, and discreet administrator to conduct the penetration testing. After all, the tester will receive access to sensitive information or trade secrets.

While many skills are need for penetration testing, a social engineer specifically needs to have critical thinking skills that allow the individual to adapt and modify the way that they are approaching the situation as events unfold (Hurley, 2007). In some cases, this can take the form of presence of mind to escape the situation when exposure or detection is imminent. Thinking outside the box and a willingness to try new things will add to the performance of the engineer when things are proceeding favorably or poorly.

Penetration testing can produce noted advantages, but it is worth considering the potential costs in terms of lasting effects that are produced within the organizational culture. Once an exploit has been perpetrated, even for improvement purposes, the employee – manager relationship is irrevocably altered. If employees choose to view penetration testing as a breach of trust, management may be viewed as an adversarial force akin to "big brother" (Clark, Kokko, & White, 2012). If management determines this potential risk is acceptable, the perpetrators will go through multiple steps and processes to transact penetration testing. These steps can include but are not limited to: planning and preparation, information gathering and analysis, vulnerability detection, penetration attempt, analysis and reporting, and cleaning up (SANS, 2002).

Perpetrators must follow a code of ethics as they will be potentially handling sensitive information of a business or its employees. Without a strong personal code of ethics, nothing prevents the tester from taking the information from the exploited company and potentially selling it to the highest bidder. Companies must take into account the reputation of the perpetrators that they hire in order to remain protected from unethical behavior. At a minimum, the potential penetration testers should be vetted using the same or more stringent criteria as a company employee trusted with sensitive information.

Social engineering is the attempt to acquire secure information by performing different psychological and social manipulation attacks on the human element (Cisco). A social engineering exploit is a socially immersive type of attack due to the fact that it is not limited by the accepted requirements of honesty or integrity found in typical business interactions. The direction of the manipulated conversation can be changed and continue as long as the attacker wants, if the attacker is receiving valuable information or the conversation can be ended if exposure is imminent. The attackers perform extensive research before an exploit. Then the attackers plan accordingly to realize improved success rates for extracting information from the target. Social engineering can be accomplished by using different methods through various outlets.

Obtaining sensitive information can occur via the telephone communication (direct or overheard), computer-based exchanges such as e-mail, phishing, or hacking, dumpster diving, shoulder surfing, reverse social engineering, and persuasion. The types of attacks vary depending upon the perceived weakness to be exploited), the location of the attack, and the targeted individual. "In order to gather information, the attacker will have to gain the trust of his future targets" (Greavu-Serban & Serban, 2014). Once a target's trust is secured, the attack can be carried out via the outlets explained earlier. By using the telephone, the attacker can impersonate a fellow employee or technician. Once the initial introduction is established, the caller may ask open ended

questions that would leave the employee to answer in a way that could be used as useful information.

Technology-based attacks involve exploiting software vulnerabilities or installing malicious code onto the target's computer that will subsequently be used to retrieve sensitive data. These types of attacks can be carried out in different ways using an assortment of delivery mechanisms and triggers (Cisco). The means of delivery could range from delivery by e-mail attachment or some form of electronic link clicked by a user to physical introduction in the form of inserting or tricking the target into inserting some storage device with malicious code that automatically executes.

Dumpster diving is the act of rifling through an organization's trash to obtain information that could be used by the attacker to help compromise security or establish the credibility of the attacker (Harnish, 2015). The trash could contain access codes, passwords, or other seemingly innocent information that could be used to make the attacker seem like they are more credible while carrying out an attack to gain access to the network. In extreme cases, the sensitive information may be in the trash itself if an employee failed to dispose of the information properly.

Shoulder surfing is a direct observation technique by looking over someone's shoulder or by the means of using magnification from farther distances to gain access to sensitive information (Tari, Ozok, & Holden, 2006). This exploit can take a wide range of approaches. In a simple case, an attacker observes a victim that is typing sensitive information in a manner that allows direct observation. The shoulder surfing ruse becomes more elaborate when the perpetrator observes from a distance or surveils the victim to gather a schedule or routine that supports a more direct observation.

Reverse social engineering is a technique in which the attacker convinces the target that they have an issue that needs to be remedied, and that the attacker has the ability to fix the issue (Gragg, 2003). With the false sense of power that the attacker creates, they can provide a sense of urgency as a way to promote the significance of the fabricated issue at hand, this urgency is created through convincing the target that they must act quickly or there will be dire consequences.

In most exploits, it is helpful to the attacker if the victim perceives that there is a sense of urgency requiring immediate action. The need for quick action prevents the victim from taking time to rationally consider their behavior or choose the correct actions. If the need for action is necessitated by a threat of personal cost to the victim, the motivation for action is even stronger. For example, in the case of phishing exploits, the fear of exposing sensitive information or financial loss triggers victim action or compliance. In business settings, fear of punishment or dismissal can be used as a strong motivator to trigger action.

Professional behavior is best described as the demeanor and attitude portrayed by an individual while in the workplace. While attitudes can vary across a profession, "end users are said to be 'the weakest link' in information systems (IS) security management in the workplace. They often knowingly engage in certain insecure uses of IS and violate security policies without malicious intentions" (Guo, Yuan, Archer, & Connelly, 2011). The variation in attitudes and acceptable professional behavior can be explained by examining the different work environments and backgrounds of employees.

Employee behavior is best described as how an employee reacts to a particular situation within the workplace. Several factors can influence an employee's behavior: the organizational culture,

job responsibilities, and workplace communication (Jain, 2015). The managers and leaders above and beside an employee can greatly influence an employee's work behavior just by how they interact on a professional level (Management Study Guide, 2016; Mohanta, 2015). However, if a "transformational leader promotes exploring novel ways of getting things done, to test fresh products, processes and services, or in other words, to abandon old ways of doing things and provide way-outs for new ones" (Jain, 2015). This action may lead to a new feeling of self-empowerment which can be exploited by a social engineer.

Since each employee is different, there are differences in the way each person will behave and how they react to different situations within the workplace. Employers see some commonalities within their employees. Some embrace change while others fear it, and some will be productive under close supervision while others are not. The reality is that some workers are extremely motivated and learn new tasks more effectively than others (Meinert, 2016).

ASSEMBLING THE TEAM

During the spring semester of 2016, a group of three students were selected to take part in a project that allowed them to test their knowledge of social engineering and penetration testing. The team conducted penetration testing on behalf of a real-world business entity. The students were selected for the project based on willingness to participate, expressed interest within the field of cybersecurity, demonstrated professional behavior and aptitude in security classes, and availability to carry out the testing.

The expressed goal of the testing was to extract as much information as possible from insurance company employees without unduly disrupting normal business activities or publicly exposing the data of customers. The project began in the summer of 2016 when the three students were tasked with a month-long research assignment. Students first explored the available academic literature related to social engineering, penetration testing, and security training. Following the literature reviews, students led an extensive research and practice that was based around mock exploits. Then the team developed a flow chart or script to outline the conversation of telephone calls that would be used for social engineering.

THE SCRIPT

Since each situation is different, the students developed a guide for creating the conversation in real time when talking to each employee. The script was very simple and only offered fake credentialing twice before terminating the call if neither was accepted. This prevented creating a situation that put employees in a state of alert. The decision logic employed can be seen in fig. 1.

The authors attempted several tactics to extract personal or sensitive information from the target employee. The authors were fueled with information collected from various reconnaissance techniques. This allowed the researchers to draw conclusions about the susceptibility of employees and customers when subjected to a potential exploit and how they would react to certain scenarios that solicited their personal information. All results were documented following the attempt for group analysis at a later time.

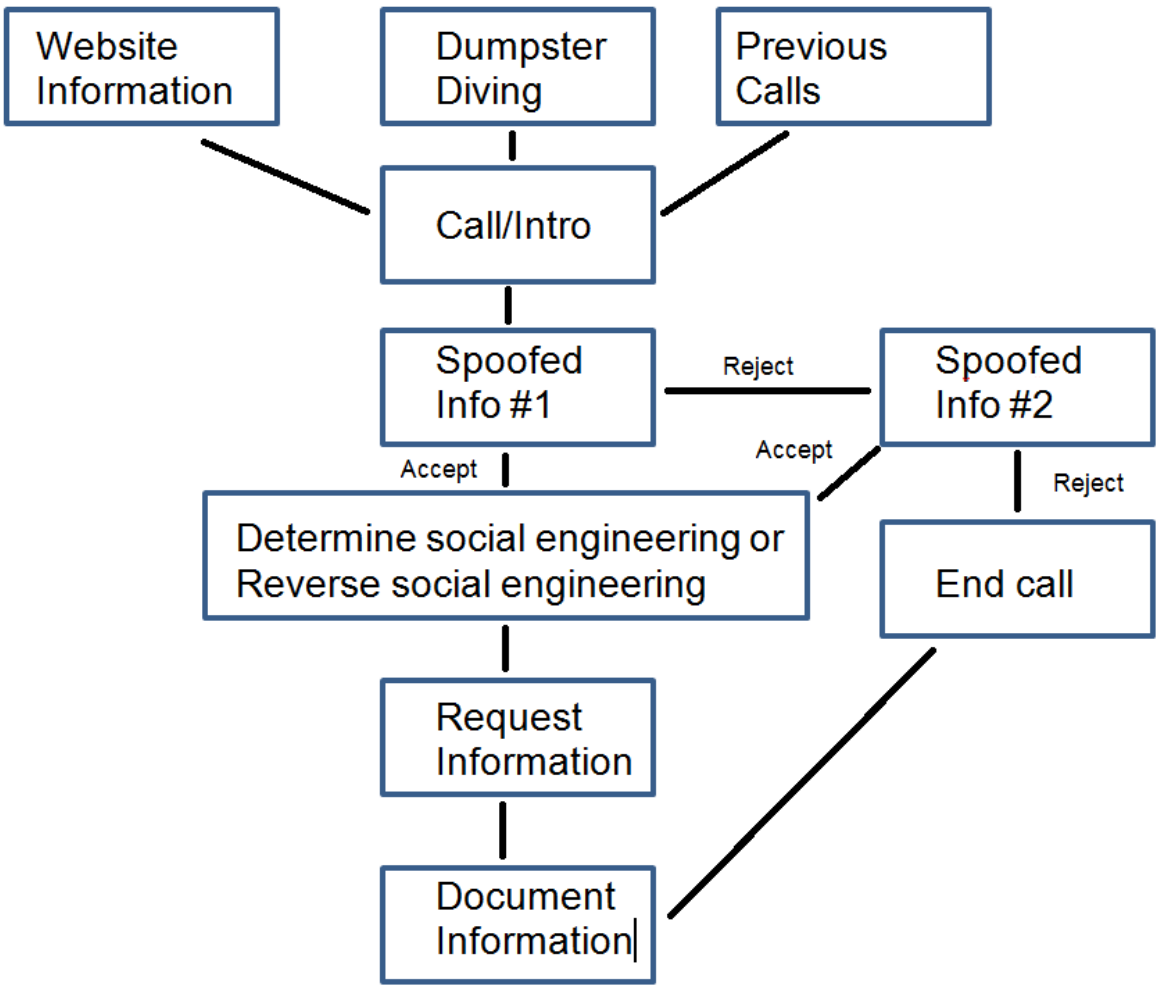

Figure 1. Decision logic used to create script for conversation during phone call.

THE ACTUAL TESTING

Through the process of dumpster diving, information was discovered that was determined to be of a sensitive nature. Specifically, information was obtained in the form of official state Uniform Motor Vehicle accident reports, credit card statements, check requests for sponsorships, and records containing other private data. All of these documents were used to formulate a plan to determine the best way to carry out the social engineering process. These documents gave insider information detailing the transaction of business within the company, which in turn, led to a point of ingress for penetrating the entity. Each report found in the dumpster was used to create a specific script in order to carry out the task needed to acquire particular information.

Telephone conversations were utilized as an avenue to carry out penetration testing. The process began with the check requests for sponsorships to determine if the employees could be persuaded to resend the checks into another account. To remain consistent and build credibility, a script was followed by perpetrators when interacting with the targets. Upon calling a target, careful consideration was given to the speech patterns and topics discussed in order to formulate a plan to

gain the trust of the target during the execution of the exploit. This consideration took the form of mimicking the accent, phrasing, speech pattern, and timber of the target. An alias was established for each exploit by using appropriate information to establish credibility. After presenting initial credentials, the perpetrator then had to construct the remainder of their identity as needed during the conversation transacting the exploit.

The target then asked how he/she could be of assistance. Casual conversation was made to establish a rapport with the target. Then upon acceptance, the perpetrator asked if the check had been sent out. In one case, the target was confused upon the request and wanted to know which employee was originally contacted about receiving the check. It was then clarified that the original phone call was made by a different caller. This action set up the sponsorship and that the original caller was not able to check up on the status of the payment. The perpetrator then stated that they were instructed to follow up on the payment, which was not received. The perpetrator stated that they did not have any additional information except what was on the paper in front of her. The perpetrator then offered a subtle plea for help from her new friend in resolving the situation. The target was then temporarily left to further discuss the status of the check with someone else that would know. After finding out the information, the target returned to the phone to inform the perpetrator that the check had been placed in the mail; additionally, the target stated that the check should be arriving within the next several days. Additionally, the target stated that if there were any further questions, the perpetrator should re-initiate contact with the target. The perpetrator then attempted to have the money placed into another account, but the target stated that the money was not able to be moved into another account. However, the most significant aspect of the experiment was that the target's trust was able to be gained, which is significant because this is an indication that a certain level of penetration had been successfully achieved.

The credit card statement was used to create a focused exploit that targeted an individual employee at the business entity. The entity was initially called and the perpetrator was asked to speak to the employee. After waiting a couple of hours for the target to return from lunch, there was another attempt at calling the target. This time, an answering service picked up in which the target's name was stated and the call went straight to the target's desk. The perpetrator alleged that fraudulent charges had been made on the target's card. The target reacted with surprise at the claims. In terms of penetration testing, this is a key or critical juncture in the process: when the target is off balance from the shock experienced by the information revealed by the attacker. This moment of shock or possible panic is the key moment for a perpetrator to strike. At this time, the target is most vulnerable and likely to act without regard for information security. This is when the perpetrator sets in to become the hero and alleviate stress by proposing to help remove the threat. Seizing this opportunity, the perpetrator asked questions to verify the identity of the target and various pieces of information found on the statement. Specifically, the information that the perpetrator attempted to obtain was the 16-digit credit card number, the expiration date of the card, and the CVV/CVC code located on the back of the card. The perpetrator explained that these questions were necessary to protect the target, and then quickly shifted the conversation to the alleged charges. It is worth noting that the perpetrator already had access to the 16-digit credit card number and used it to establish credibility in order to obtain the other two pieces of information that they did not already possess.

The target stated that they were unable to recall the exact credit card number at that moment as well as the other pieces of information that the perpetrator sought. The target then asked if it would be acceptable to contact the bank after they left their place of employment later that evening to

confirm this information. The perpetrator accepted this proposal as it was clear that no further information could be obtained in this exploit and offered a phone number and contact information the target could use. While this may sound like a dead-end, responding in this fashion to a reasonable request further establishes credibility and potentially furthers the exploit. Ultimately, it was an unsuccessful attempt to get the employee to verify the credit card number since an additional call did not occur, but it was enough to verify that the target was the person on the statement. This exploit would be considered reverse social engineering. The difference being that it involves an establishment of trust between perpetrator and target. After the trust is established, the personal information is then requested from the target. This differs from normal social engineering because instead of applying an outside pressure such as a time-based sense of urgency, this method attempts to gain the trust of the target in a calm and collected manner so the target is more relaxed, willing to help, and feels as though they are in control of the situation. This method works because "the attacker creates a situation where they must help the target individual and then pose as some people who the target will recognize as individuals who can both solve the target's problem and receive privileged information" (Krombholz, Hobel, Huber, & Weippl, 2013).

Overall, the testing seemed to work well on some cases but was less successful for other cases. This is to be expected. It is worth noting that each exploit has a very low expectation of success, but each exploit launched at a single entity provides information that makes subsequent exploits against targets of the same entity potentially more effective. Overall, penetration testing should be viewed as a numbers game. From the perpetrator's standpoint, only one or two cases need to yield fruit in order to justify the expenditure of effort. In our example, the intended targets seemed to be very knowledgeable of what to look for in an exploit. No harm was done with the gathered information nor were there any discrepancies when talking with the intended targets.

The business world is supported with the use of technology which is protected by the latest versions of technology-based security solutions such as firewalls, antivirus software, and others to protect information. Attackers want to utilize the path with the least amount of resistance. In order to prevent successful social engineering exploits, employees must be thoroughly trained to avoid falling prey to social engineering attacks. Training consists of a variety of different methods including: employment training, educational videos, third party programs, and online skill assessments. Once trained, an employee must be tested and periodically re-trained to maintain and assess skill levels. Employers have multiple tools for testing as well, be it pen and paper tests, online questionnaires, third party programs, or even mock social engineering tests. However, it is important to note that as employees have been subjected to social engineering attempts in the past, it becomes a less effective mechanism for testing their knowledge using a social engineering attack.

CONCLUSION / RECOMMENDATIONS

This experience has proven that the human element is usually the unknown factor when it comes to the security of any company or personal information. There are a few lessons that one can learn from reading about these test results. Arguably, there are lessons that can be learned from both sides of the testing. Both the local business and the perpetrators themselves can carry with them valuable knowledge from this test in order to help each party in the future. From the local business perspective, holes and vulnerabilities are visible within the physical and cyber-security. The overall procedure highlights the degree to which employees with the company can be tricked or coerced into divulging sensitive information.

In general, the employees exceeded expectations of what the perpetrators thought would happen. In other words, the employees curved the perpetrators' predictions. The perpetrators were very rarely given information from an employee themselves. However, the perpetrators were able to uncover client information that could be crucial in the release of this sensitive information. As an example, dumpster diving was the medium in which the perpetrators were able to retrieve the sensitive information. The perpetrators found numerous records of client information, ranging from claims to records of payment, which included account names and numbers. With what the perpetrators were able to gather from this test, the perpetrators were able to conclude that while the employees did well on the front-end when asked specific questions about clients and their information, the back-end was lacking in such a way to where they weren't discarding of unused personal information accordingly.

In addition, the physical security of the building seemed to be lack as well to the extent of locking outside doors. A tester was able to enter the building and physically plant a harmful program within a healthy number of computers. The overall learning opportunities that the business can retrieve from this are to ramp up the physical security of the building and to properly dispose of any unwanted or unused client information. A simple way to improve the physical security of the building is by simply installing a key-card access system on all outside doors. With this proposed idea, the risk of anyone entering the building through any outside door will decrease dramatically. This is just one of many ways the business can improve their physical security.

A very simple way to improve their disposed client information from being used by another party is to simply put it through a paper shredder. Paper shredding unwanted and unused client information will make it very difficult for anyone to find the information that they need. On the other hand, the perpetrators themselves can take valuable knowledge from this test as well. With them doing the testing themselves, they already have a working knowledge of what to do and not to do within a business regarding sensitive information. Through the testing, they will know what to look out for and identify a scam easily because they'll know most of the common tricks that scammers will use.

While both sides will gain valuable knowledge from this test, it is safe to assume that both parties wish they could do something differently to help improve their chances of winning, so to speak. It can be argued that the business wish they could have been able to spot a non-worker within the building. This is where the key-card access system would have played a significant role. It is safe to say that the business would like to start over and upgrade their security system in order to prevent such an attack. Even though the employees did well overall, it wouldn't hurt the business to assure that every employee is properly educated and informed of the different ways that other people can obtain client information. With these slight changes, the chances of information being exposed and any other harm to the business will be drastically reduced. On the other side of the coin, there is reason to believe that the perpetrators would have done some things differently in retrospect. For instance, the social engineers of the test would like to have gained more knowledge prior to testing. To clarify, the social engineers would like to have known more ways and methods of trying to extort personal or client information from the employees. They believe that more knowledge of the different methods of social engineering would have helped the success rate of gaining personal or client information. Overall, extensive research and more practice of the different social engineering methods are believed to have wielded more promising results if they had more experience. The social engineers recognize this test as a valuable learning experience and will take to heart the results of the test. Therefore, they will incorporate this new knowledge

and apply it with future endeavors and future tests.

REFERENCES

Cisco. Protect Against Social Engineering, Security-Aware Culture Helps Neutralize Social-Engineering Threats. http://www.cisco.com/c/en/us/about/security-center/protect-against-social-engineering.html

Clark, T., Kokko, H., & White, S. J. (2012). Trust: An essential element of leaders and managers. *American Journal of Health-System Pharmacy, 69(11),* 928-930. doi:10.2146/ajhp110516

Conducting a Penetration Test on an Organization. (2002). SANS Institute. Retrieved April 12, 2017.

Furtuna, A. (2015, January 15) 5 Benefits of a penetration test. Retrieved April 12, 2017.

Gragg, D. (2003). A multi-level defense against social engineering. SANS Reading Room, March, 13.

GREAVU-ŞERBAN, V., & ŞERBAN, O. (2014). Social Engineering a General Approach. *Informatica Economica, 18(2),* 5-14. doi:10.12948/issn14531305/18.2.2014.01

Guo, K. H., Yuan, Y., Archer, N. P., & Connelly, C. E. (2011). Understanding nonmalicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems, 28(2),* 203-236.

Harnish, R. (2015). Cybersecurity in the World of Social Engineering. Cybersecurity in Our Digital Lives, (2,143).

Hurley, C. (2007). Penetration Tester's Open Source Toolkit. Burlington, MA: Syngress.

Jain, R. (2015). Employee Innovative Behavior: A Conceptual Framework. Indian Journal of Industrial Relations, 51(1), 1-16.

Knowles, R, (2002). The Leadership Dance. Third Edition. Center for Self-organizing leadership.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2013, November). Social engineering attacks on the knowledge worker. In Proceedings of the 6th International Conference on Security of Information and Networks (pp. 28-35). ACM.

McGraw, G. (2006). Software security: building security in (Vol. 1). Addison-Wesley Professional.

Meinert, M. C. (2016). SOCIAL ENGINEERING: The Art of Human Hacking. American Bankers Association. *ABA Banking Journal, 108(3),* 49.

Mohanta, G. C. (2015, January 20). Individual Differences and Its Importance. Slideshare: Leadership and Management. Retrieved August 25, 2016.

MSG: Management Study Guide (2016) Employee Behavior. MSG: Management Study Guide. Retrieved. August 25, 2016.

Rogers, E. M. (2005). Diffusion of innovations. New York: Free Press.

Tari, F., Ozok, A., & Holden, S. H. (2006, July). A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. In Proceedings of the second symposium on Usable privacy and security (pp. 56-66). ACM.