International Journal of Information & Network Security (IJINS)
Vol.1, No.2, June 2012, pp. 45~53
ISSN: 2089-3299

A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model

Anubhav Chitrey, Dharmendra Singh, Monark Bag, Vrijendra Singh
Department of Information Security & Cyber Law
Indian Institute of Information Technology
Allahabad, India

Article Info

Article history:

Received Apr 30th, 2012
Revised May 11th, 2012
Accepted June 03th, 2012

Keywords:

Social Engineering
Phishing
Vishing
Dumpster Diving
Shoulder Surfing

ABSTRACT

The objective of this research is to present and demonstrate an analytical approach towards Social Engineering. A questionnaire was created and a survey was conducted accordingly to determine the understanding of IT practitioners and social networking users based in India. The participants of this survey are either employed with a renowned IT service providing firm or students of top IT colleges. Based on the responses an advanced model of Social Engineering based attacks was developed. The research identified many participating entities in Social Engineering based Attacks and each identified entity of this research is a research area in itself. This model can be used in development of Organization-wide Information Security policy and Information Security Awareness Program.

Corresponding Author:

Anubhav Chitrey,
Department of Information Security & Cyber Law
Indian Institute of Information Technology
Allahabad, India.
Email: anubhavchitrey@gmail.com

1. INTRODUCTION

Social Engineering is the art of exploiting the weakest link of information security systems: the people who are using them [1]. Social Engineering is a method of gathering information and performing attacks against Information and Information Systems. An immense amount of loss has suffered by Organizations and Individuals from these attacks. However Social Engineering as a threat is overlooked because of low awareness and lack of proper training for people. The objective of this research is to present and demonstrate an analytical approach towards Social Engineering and its presence in India. A thorough literature review was performed to formulate a conceptual model of Social Engineering attacks. A questionnaire was conducted to determine the insightful opinions of ninety India based IT practitioners and social networking users, to understand the phenomenon of Social Engineering based attacks. Analysis of the collected responses guided us to construct a more refined model of Social Engineering based attacks. The paper begins with the research objective followed by a presentation of suggested model of these attacks. The opinions of IT practitioners and social networking users based in India, as well as important observations are then presented. The paper ends with the formulation of a more refined model of Social Engineering based attacks.

2. RESEARCH OBJECTIVE AND METHODOLOGY

The objective of this research was defined as – **"Identifying the participating entities and relations between these entities in Social Engineering based attacks".** To fulfill this research objective we

conducted a questionnaire and collected insightful opinions of participants. We put following specific questions –

- **Question-1:** Do you understand the current security issues - especially social engineering? Have you ever faced any Social Engineering based attack?
- **Question-2:** What type of Social Engineering based attacks have you faced and what medium did the attacker use to perform social engineering based attacks on you?
- **Question-3:** What are the motivations and consequences for Social Engineering bases attacks?
- **Questions4:** What are the advancing technology products used by attackers as information gathering tools?
- **Question-5:** Who presents the greatest risk of falling for social engineering based attacks in organizations?
- **Question-6:** What can be done to mitigate Social Engineering based attacks [2] ?
- **Question-7:** What is India's perspective of Social Engineering based attacks [2] ?

A comprehensive questionnaire was conducted to obtain users inputs.

3. INITIAL APPROACH TO SOCIAL ENGINEERING

Social Engineering based Attacks are the most common attack methods adopted by attackers. Exploiting the system and execuritng the malicious code require sound understanding of vulnerabilities present in the system. However, the success rate of such technical attacks have been minimized by using technical controls. Therefore, hackers have now adopted the alternative method – Social Engineering, exploiting the psychological vulnerability present in people and potential technical vulnerabilities of various technologies. Consequently, Social Engineering is now considered as the greatest security threat for people and organizations both.

"Socially-engineered attacks traditionally target people with an implied knowledge or access to sensitive information" [7]. According to a statement from Check Point on the survey "Hackers today leverage a variety of techniques and social networking applications to gather personal and professional information about an individual in order to find the weakest link in the organization" [8]. It is a human-based attack including Dumpster Diving, Shoulder Surfing, Impersonation and Reverse Social Engineering; however it has technological aspects too, including Email Attachment, Trojan horse, Botnet, Online Scams, Vishing and Pop up Applications [2].

4. AFTERMATH

From an interview of Kevin Mitnick, an infamous hacker in the 1980s and 1990s, with the BBC News Online - "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" [12]. The Social Engineering based attacks are costly for people and organizations both, especially large organizations [9]. These attacks are performed in various phases and each phase of the attack requires specific information. For instance, in information gathering phase, information such as organization details including internal documents – organization structure, client details and telephone directories or individual details like date of birth, contact number, address, and marital status and so on. The information gathered is further used in Exploit phase. The level of damage caused by these attacks depends upon purpose of the attack.

Social Engineering based attacks may cause significant loss of CIA. Firstly, loss of confidential information to business rivals or physical damage to assets. Secondly, deprivation of public trust and organization image of organization resulting in business loss because of disclosure of confidential client data such as credit card number to the public. Social Engineering is threat to sensitive financial information of an individual. For instance, phishing mails and pop up advertisements are examples of most common Social Engineering based Attacks against individuals.

5. KEY FINDINGS

To support the proposed model, a questionnaire was conducted and a total of ninety responses were collected. The participants were of different IT domain experts such as IT advisory, software development, security consulting, students and experience. The participants were from various organizations and industries. The questions included in the questionnaire were derived after understanding human psychological vulnerabilities as well as awareness of people in India towards safe and ethical usage of computer and internet applications.

6. THE PROPOSED MODEL

Based on the analysis of the information gathered by questionnaire, the entities included in proposed conceptual model were evaluated. "Organization Security Policy" in the vulnerability section as well as in Safeguard Section came out as one of the most crucial and underestimated component after analysis of the results obtained from questionnaire. Organization security policy is a must to eliminate risks; however the analysis suggests that a weak security policy can lead to the exploitation of organization assets by Social Engineering based attacks. Therefore Security Policy is also considered as a vulnerable entity. "Information Security Awareness and Training Program" emerged as psychological control to overcome psychological vulnerabilities present in human. Answering the questions mentioned at the beginning of this paper –

Question-1: Do you understand the current security issues, especially social engineering? Have you ever faced any Social Engineering based attack? This question was answered after analyzing questionnaire results and literature review. The literature review identified two vulnerable entities in which can directly be exploited by a Social Engineering based attack, including People and Technological Controls. However the questionnaire results analysis suggested that Organization Security Policy is also a major component which is vulnerable to such attacks. Literature review and questionnaire results analysis both agreed upon that People are the weakest link in organization information security. Psychological weakness of people and lack of proper Training and Security Awareness Program are the main causes that Social Engineering based attacks are successful. Literature review suggests that people do not have basic understanding of current security issues – especially Social Engineering. This is supported by 61% of the questionnaire participants. In agreement with the psychological weakness identified in literature review, 90% of the participants accepted that in India, people generally have a higher level of social trust which implies that they are more vulnerable to social engineering based attacks [9].

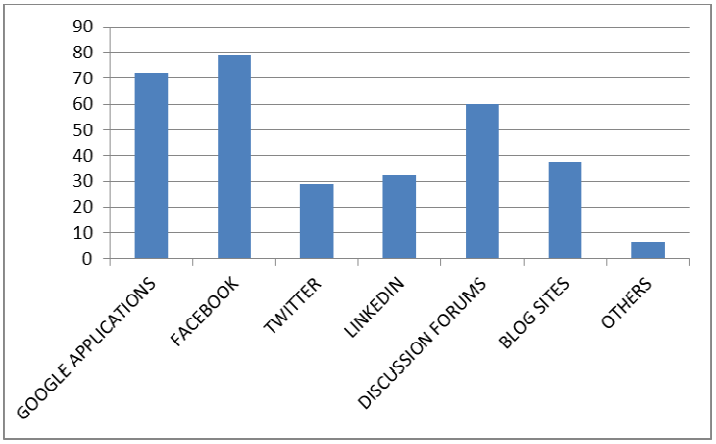


Figure-1: Questionnaire results regarding use of Advancing technology products [11]

The literature review has suggested that there are three major issues related to Technological Controls. Firstly, people think that a lot of technology products have flaws in their security design which are used by an attacker to perform technology-based scams [9]. The questionnaire results show that 79% participants agreed to this. Secondly, 64% people stated that most security technologies are incapable of detecting and preventing social engineering based attacks as social engineering bypasses technical control via manipulating people who are managing them [9]. Additionally, 93% people stated that the advancing technology products such as Google Application, Social Networking Sites, Discussion Forums and Blog Sites are used by social engineers as information gathering tool. As represented in Figure-1, 72% supported use of Google Application, 47% for Social Engineering Sites (79% for Facebook, 29% for Twitter and 32% for LinkedIn), 60% for Discussion Forums and 38% supported for Blog Sites. From the analysis of the results of questionnaire, Organization Security Policy evolved as a major entity which is vulnerable to Social Engineering based attacks. In most cases, people remain unsure about the identity of the requestors or people are unsure if it is proper to grant access to a requestor. This is the reason to put a well-designed, documented

and discussed Organization-wide Security Policy. However, only 10% people think that in India the organizations have a well-defined security strategy and awareness program for their employees for social engineering based attacks [9].

Question-2: What type of Social Engineering based attacks have you faced and what medium did the attacker use to perform social engineering based attacks on you? Social Engineering is a method of influencing, betraying and psychologically manipulating human behavior with or without the use of any Technology. It varies in complexity based on the attack motivation. The Literature review suggests that Social engineering based attacks can be classified into two categories – Human-based and Technology-based. Human-based attacks are totally based on attacker's art of deception and can be conducted either meeting personally or over the telephone. For instance, impersonation, shoulder surfing, dumpster dives and reverse social engineering. Human-based Social Engineering attacks are the most widespread method of deception as voice can easily be masked.

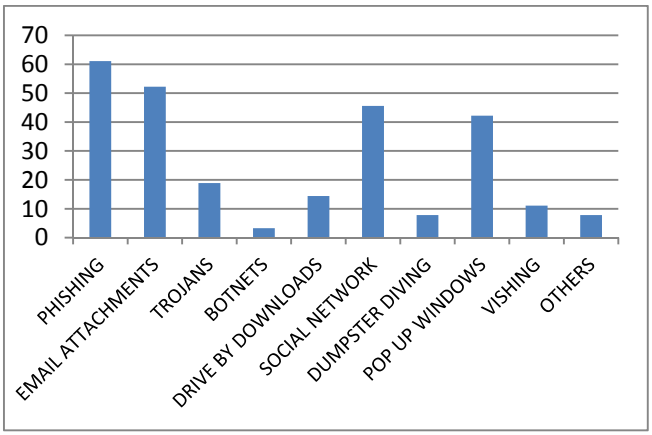


Figure-2: Questionnaire results regarding various attacks used by social engineers [11]

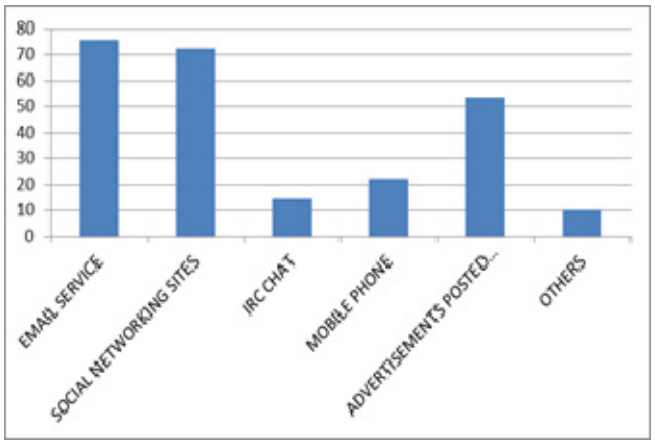


Figure-3: Questionnaire results regarding use of attack medium by social engineers [11]

Technology-based Social Engineering is similar to traditional hacking techniques. The purpose is to deceive people into believing that they are communicating with an authentic computer system through any software or application. The attack methods include Email Attachment, Phishing Mail, Pop-up window, Botnet, Trojan Horse and Social Networking. In agreement with the Literature Review, the analysis of Questionnaire results stated that 61% participants have faced Phishing, 52% have found Email Attachments and 46% have faced attacks through Online social Networking. Other participants have faced attacks through Pop-Up Windows, Vishing, Dumpster Diving, Trojan Horse and Botnets. 76% of the participants agreed upon Email Service to be the most preferable medium to launch attacks while 72% supported Social

Networking, 14% supported IRC Chat Service, 22% supported use of Mobile Phone and 53% supported for Advertisements posted on Websites. The findings are shown in Figure-2 and Figure-3.

Question-3: What are the motivations behind Social Engineering bases attacks? The complexity of Social Engineering based attacks varies based on the motivation. Literature review suggested that Financial Gain motivates attackers the most to launch such attacks. However, only 23% participants supported the literature review. Figure-4 suggests other catalysts of Social Engineering based attacks include Unauthorized Access to Proprietary Information(30%), Competitive Advantage(21%), Revenge(10%) and 11% supported that attackers usually launch such attacks just for fun. Any successful Social Engineering based attack leads to unauthorized disclosure of secrets and a breach of Confidentiality, integrity and Availability.

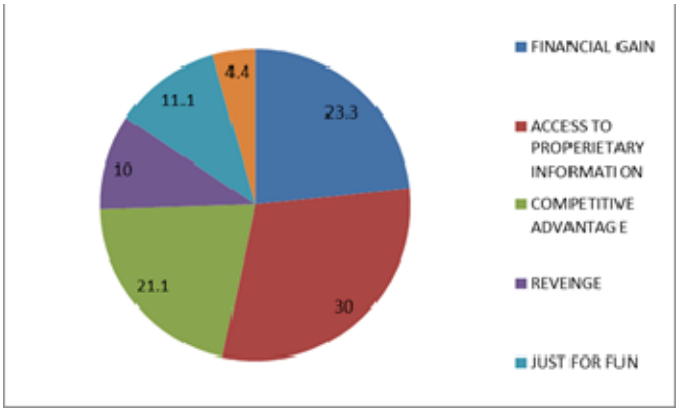


Figure-4: Questionnaire results regarding motivation behind social engineeing attacks [12]

Questions-4: What are the advancing technology products used by attackers as information gathering tools? Today, various technologies are available in public which can be used as an information gathering tool. The Literature review stated that some of these technologies are Google Applications, Online social Networking websites (Facebook, Twitter, and LinkedIn etc.), Discussion Forums and Blog sites. In agreement of the Literature Review, our analysis suggested that 93% people agreed that the advancing technology products such as Google Application, Social Networking Sites, Discussion Forums and Blog Sites are used by social engineers as information gathering tool. 72% supported use of Google Application, 47% for Social Engineering Sites (79% for Facebook, 29% for Twitter and 32% for LinkedIn), 60% for Discussion Forums and 38% supported for Blog Sites.

Question-5: Who presents the greatest risk of falling for social engineering based attacks in organizations?All participants were asked what type of personnel was most likely to susceptible to Social Engineering attacks. New Employees were considered as having the greatest risk of falling social engineering based attacks as 41% participants supported it, followed by Clients(23%) who may be less aware of Social Engineering and Organization Security policy, Partners and Contractors(12%), Top level Management(7%) and IT Professionals(17%) who has access to confidential information as shown in Figure-5. The analysis implied that organizations should conduct a well-designed Information Security Awareness Program and Training for their employees on regular intervals. The new employees should be given special attention during their training. Organization should also educate its clients and partners about Social Engineering.

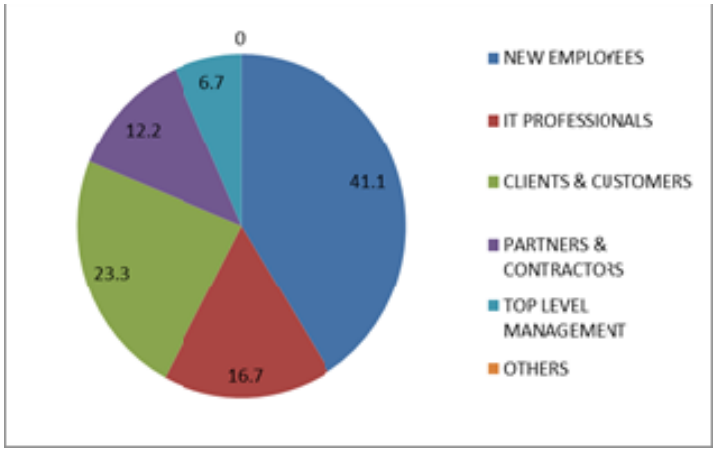


Figure-5: Questionnaire results regarding entities which present greatest risk of falling for social engineeing attacks [12]

Question-6: What can be done to mitigate Social Engineering based attacks [2]? Social Engineering represents multiple dimensions of threats. Therefore a multifaceted solution and defense-in-depth approach is necessary to defend against Social Engineering based attacks. Figure-6 represents the identified layers of a multifaceted defense approach against Social Engineering Based Attacks. The defense-in-depth methodology represents multiple layers of security, including Physical Security, access control, Technical Controls, Security Policy and Information Security Awareness Program. Firstly, Physical security must be implemented properly as many attacks are through gaining physical access. Secondly, Access Controls must be in place to keep unauthorized attacker away and to allow legitimate users only. Organizations should apply different Access Control mechanisms based on type of Social Engineering attack (Human-based and Technology-based). Thirdly, Technical Controls can help to reduce risk of Social Engineering attacks, such as a multifactor based authentication (Something the user knows-password and PIN, Something the user has-ATM Card and Smart Card and Something the user is- biometric characteristic) must be used to prevent unauthorized access and online financial scams. Fourthly, Security Policy is the key element of good defense against Social Engineering based attacks because it separates the uncertainty which is what Social Engineering depends on. The policy should encompass all components which are necessary to protect and must be discussed with all personnel, partners and clients. Ultimately, Security Policy must be assisted by Information Security Awareness Program and Training. The degree of people's vulnerability to social Engineering directly depends on the level of their awareness of such kind of attacks. Therefore People must be educated to Latest Security Threats and Attack Trends to resist Social Engineering based attacks.

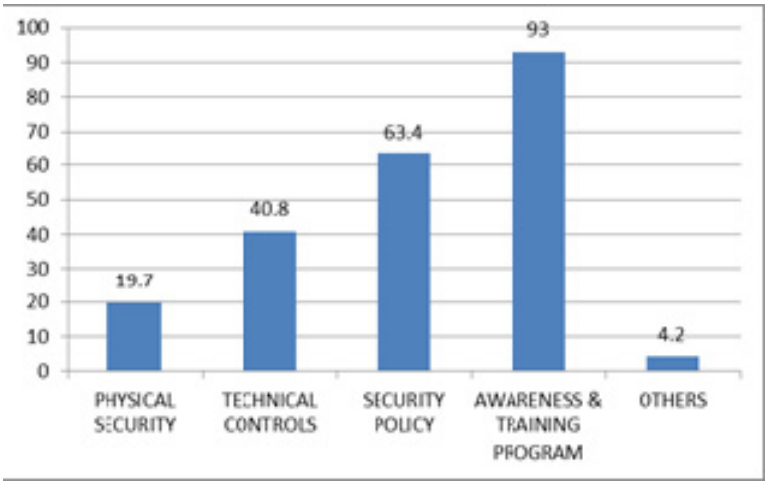


Figure-6: Questionnaire results regarding diffenent safeguards to prevent social engineeing attacks [12]

Question-7: What is India's perspective of Social Engineering based attacks [2]?In general, India contributes the same trend as other countries in terms of Technology and Security Risks associated to its usage. However, Indians do not have sufficient awareness of latest security issues regarding technology usage and their countermeasures. Firstly, according to 61% of the participants, the majority do not have sufficient understanding of Social Engineering based attacks. 52% accepted that they are not fully aware of it, but they know that it can be launched with the personal information shared on internet. 2% of them mentioned that they have heard about it from friends or media and 8% stated that they don't know anything about it. 90% of the participants think that people in India generally have a higher level of social trust which implies that they are more vulnerable to social engineering based attacks. Secondly, with regards to Security Policy and Information Security Awareness Program, only 10% stated that in India the organizations have a well-defined security strategy and awareness program for their employees for social engineering based attacks. Participants commented that the lack of Standards and Compliance in India also have impact on insufficient security strategies within the organizations. Thirdly, the analysis represents the diversity and complexity of Social Engineering based attacks. Participants accepted that a multifaceted security strategy i.e. defense-in-depth, must be used to mitigate the risks associated with Social Engineering. In agreement with the Literature Review, the participants suggested that Physical Security, Access Controls, Technical Controls, Security Policy and Education should also be adopted. The proposed model of Social Engineering based Attacks is shown in Figure-7.

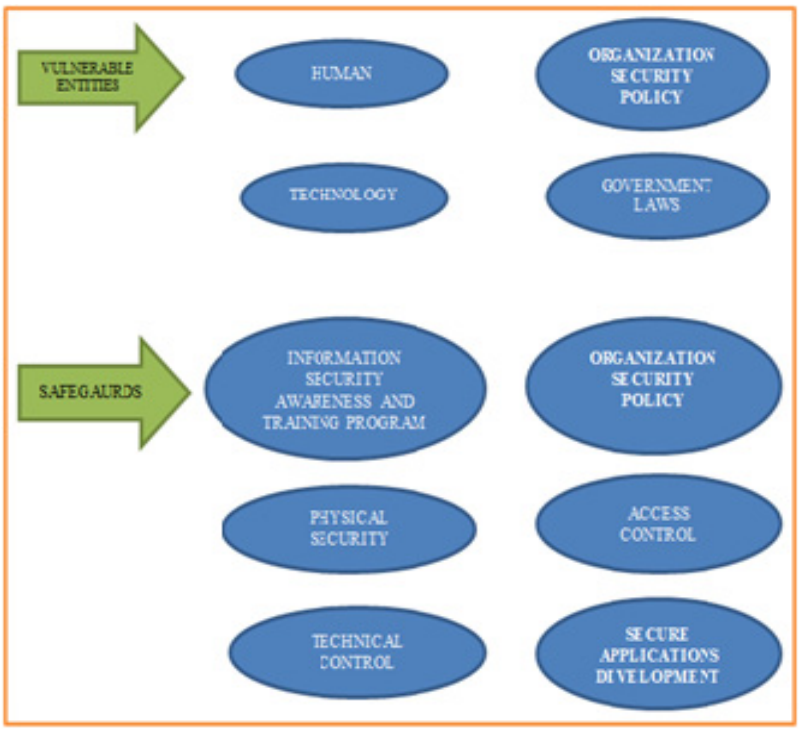


Figure-7: The proposed conceptual model of Social Engineering based attacks based on the result of survey

7. LIMITATIONS AND FUTURE RESEARCH

This study discusses about three aspects of Social Engineering based attacks –
Firstly, it enables the representation of Social Engineering based Attacks via developing a conceptual model to represent the findings.Secondly, it provides a medium to measure the impact of Social Engineering based Attacks over individuals and organizations both. Thirdly, it suggests a diversified approach to develop a security strategy by adopting defense-in-depth methodology to prevent Social Engineering based attacks. There is a research limitation which must be discussed here. The participants of this research were the IT practitioners in India and students who had an interest in Information System Security and Research. As a result, there is a lack of non-IT perspective towards Social.

There are following opportunities of further research on the basis of this research – Firstly, researchers may validate the constructed conceptual model of Social Engineering based Attacks by evaluating the identified entities and a more sophisticated model can be proposed based on this conceptual model. Secondly, this analysis describes the impact and possible safeguards for Social Engineering based attacks. This research can be used to develop an Information Security Awareness Program or design educational applications to educate people how to stay safe against such attacks.

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] Janczewski J. L., Lingyan Fu, "Social Engineering-Based Attacks – Model and New Zealand Perspective", 2010 proceedings, ISBN 978-83-60810-27-9, Page(s): 847 - 853

[3] Stephanie M. White, "Social Engineering," Engineering of Computer-Based Systems, 2003 proceedings, Digital Object Identifier: 10.1109/ECBS.2003.1194807, Page(s): 261 – 267

[4] Laribee L., Barnes D.S., Rowe N.C., Martell C.H., "Analysis and Defensive Tools for Social-Engineering Attacks on Computer Systems," Information Assurance Workshop, 2006 IEEE, Digital Object Identifier: 10.1109/IAW.2006.1652125, Publication Year: 2006, Page(s): 388 -389

[5] Bezuidenhout M., Mouton F., Venter H.S., "Social engineering attack detection model: SEADM." Information Security for South Africa (ISSA), 2010, Digital Object Identifier: 10.1109/ISSA.2010.5588500, Publication Year: 2010, Page(s): 1 – 8

[6] Rabinovitch E., "Staying Protected from Social Engineering," Communications Magazine, IEEE, Volume: 45, Issue: 9, Digital Object Identifier: 10.1109/MCOM.2007.4342845, Publication Year: 2007, Page(s): 20 – 21

[7] Alim S., Abdul-Rahman R., Neagu D., Ridley M., "Data retrieval from online social network profiles for social engineering applications," Internet Technology and Secured Transactions, 2009, ICITST 2009, Publication Year: 2009, Page(s): 1 – 5

[8] Social Engineering: The Basics, By Joan Goodchild, Senior Editor, http://www.csoonline.com/article/514063/social-engineering-the-basics

[9] The Risk of Social Engineering on Information Security: A Survey of IT Professionals - Dimensional Research September 2011, www.checkpoint.com/press/downloads/social-engineering-survey.pdf

[10] Social engineering attacks costly for business, By Joan Goodchild, Senior Editor, http://www.csoonline.com/article/690167/social-engineering-attacks-costly-for-business

[11] Social engineering based attacks – A Survey – Part-1, By Anubhav Chitrey and Dharmendra Singh, http://www.scribd.com/doc/86317607/Social-Engineering-based-Attacks-A-Survey-Part-1

[12] Social engineering based attacks – A Survey – Part-2, By Anubhav Chitrey and Dharmendra Singh, http://www.scribd.com/doc/86317695/Social-Engineering-based-Attacks-A-Survey-Part-2

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

BIOGRAPHY OF AUTHORS

ANUBHAV CHITREY

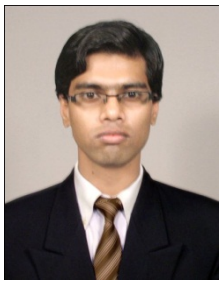
Anubhav Chitrey is a student of Master of Science in Information Security and Cyber Laws from IIIT Allahabad. He possess a Bachelor of Technology in Information Technology. His areas of expertise include IT Risk Management, VAPT, Network security, Web Application Security and ISMS implementation as per ISO 27K standard.

EMAIL – anubhavchitrey@gmail.com

DHARMENDRA SINGH

Dharmendra Singh is a student of Information Security and Cyber Laws at IIIT Allahabad. He did Bachelor of Technology in Computer Science from Bundelkhand University. My areas of interesst are Information Security Research, Network security and Cryptography.

EMAIL – dharms.777@gmail.com



MONARK BAG
Monark Bag is a Lecturer in MBA (IT) and MS (CLIS) Division of Indian Institute of Information Technology, Allahabad. He holds a B.Tech (Computer Science and Engineering), MBA (Information Technology Management) and PhD (Engineering). He is highly engaged in teaching and research. His research interest includes expert system, control chart pattern recognition, quality control, optimization techniques and intrusion detection systems. He has published many papers in reputed journals, conferences and book chapters.
EMAIL – monarkbag@gmail.com

VRIJENDRA SINGH
Vrijendra Singh is a Assistant Professor in MBA (IT) and MS (CLIS) Division of Indian Institute of Information Technology, Allahabad. He holds Ph. D in Computer Science. His Research Interests includes Data Warehousing & Mining, Digital Image Processing, Machine Learning Operations and Enterprise Resource Planning.
EMAIL – vrij@iiita.ac.in