iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** II **Month of publication:** February 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Social Engineering: Attack, Prevention and Framework

Anshul Kumar[1], Nagresh Kumar[2]
[1,2]*Department of Computer Science & Engineering*
Meerut Institute of Engineering and Technology, Meerut, Uttar Pradesh, India

Abstract--Social Engineering is the act of breaking security by manipulating users/individuals into divulging confidential information. It uses psychological tricks to gain trust, rather than technical cracking techniques. Social Engineering includes scams such as obtaining a password by pretending to be an employee, leveraging social media to identify new employees more easily tricked into providing customer information, and any other attempt to breach security by gaining trust. This work contains some of the most current scientific, technical and psychological information on the topic of social engineering today. Our goal is to create framework for the security professional to learn, adopt and embed in their information.
KeyWords: Social Engineering, Phishing, Attacks, Passwords, Awareness.

I. INTRODUCTION

Social engineering is the art of getting people to comply with your wishes. It takes advantage of the psychological aspects of the human mind and the social interaction patterns between people. With this approach a skilled social engineer is able to execute an efficient and cheap compromise of security without having to invest in breaking technological security measures, such as firewalls. A social engineer can also combine technological means to achieve the attack objectives. This includes contacting people by means of communication technology and luring them into executing actions, such as installing malware, which the attacker can use to further compromise the systems. Social engineering is the term that hackers use to describe attempts to obtain information about computer systems through non technical means. Social engineering can be understood as the art of deception. It is the science of getting the people to comply with your wishes. As the social engineering relies on human to human interaction it can be used to target the weakest link of computer security, the human user. It is much easier and cheaper to try to hack the humans than the security systems. Note that social engineering as a concept is much broader, though, and is not solely limited to information security. This is a type of confidence trick for the purpose of vital information gathering. It is a term that describes a non-technical attack that relies on human interaction and tricking people to break normal security procedures. Criminals use social engineering tactics because it is comparatively easier that other attacks.

II. SOCIAL ENGINEERING ATTACKS

A. Human Based Methods

Human based social engineering needs interaction with humans; it means person to person contact and then retrieving the desired information.

1) Impersonation: It is one of the most common social engineering techniques and it takes many forms. Impersonation can occur in person, over the phone or on-line. There are basically seven scenarios where impersonation is used to create a successful social engineering attack.

2) Tech Support: The Social Engineer may pretend to be technical support from one of the organization's software vendors or contractors to gain information. The attacker explains that he is troubleshooting a network problem and has narrowed the problem to a certain computer. He claims to need a user ID and password from that computer to finish tracing the problem. Unless the user has been properly educated in security practices, they will be likely give the "trouble-shooter" the information requested.

3) Roaming The Halls: The attacker may enter the building pretending to be a contractor, client or service personnel. They will often dress in business attire or the appropriate uniform and will often be allowed to roam the halls unnoticed. They can look for passwords stuck on terminals, find important data lying on desks or overhear confidential conversations.

4) Repairman: Most people accept either a telephone repairman or computer technician without suspicion. Acting as a

repairman or technician, the attacker can plant a snooping device or look around for hidden passwords or other critical information all the while appearing to be going through the normal activities associated with their duties.

B. Computer Based Methods

Computer-based social engineering uses computer software that attempts to retrieve the desired information.

1) Pop-Up Windows: A window will appear on the screen telling the user that the network connection has been lost. The user is prompted to reenter their user name and password. A program previously installed by the intruder will then email the information back to a remote site.

2) Instant Messaging/Internet Relay Chat: Users are directed to sites that claim to offer help or more information but are really designed to plant Trojan horse programs on their computers which the hackers later use to gain access to their computers and the networks to which they are connected.

3) E-Mail Attachments: Programs can be hidden in email attachments that can spread viruses or cause damage to computer networks. This includes malicious software such as viruses, worms and Trojan horses. In order to entice users to open the attachments, they are given names that raise curiosity and interest.

4) Email Scams: Email scams are becoming more prevalent. One recent example claims that you have won a trip to the Bahamas and requests "basic information" from the user so that the prize can be awarded. Initially they request relatively harmless information such as name, address and phone number; however, in a subsequent email, credit card information is requested in order to hold your spot on the "free" trip.

5) Chain Letters And Hoaxes: These nuisance emails rely on Social Engineering to continue their spread. While they do not usually cause any physical damage or loss of information, they cause a loss of productivity and also use an organization's valuable network resources.

6) Websites: A common ploy is to offer something free or a chance to win a sweepstakes on a Website. To win the user must enter an email address and a password. Many employees will enter the same password that they use at work, so the Social Engineer now has a valid user name and password to enter an organization's network.

III. PREVENTION OF SOCIAL ENGINEERING ATTACKS:

The following are the defences that can be used to eradicate social engineering attacks:

A. User Awareness And Education

Employee awareness and acceptance of safeguard measures will become our first line of defence in this battle against the attackers. Humans being the weakest link in this attack, they need to be educated about the dangers of social engineering. They need to be trained on what social engineering is and how it can manifest itself in an organization. People need to know the damage done by such thefts on an organization and personal level. These trainings should be a frequent occurrence.

B. Security Policies

The security policy should be well-documented with sets of standards that form a strong foundation of a good security strategy. It should clearly document in simple terms, its scope and contents in each area that it applies to. These policies will be redundant if not enforced and implemented. The users should be following these guidelines for the policies to be effective. Every new user should go through orientation on the security policies that they should follow.

C. Security Audits

Developing and implementing security policies is not enough. There is need to ensure that everyone conforms to the policy. For this reason, there is need to have audits on the usage of the policies. These audits should be done across the board in an organization. It will show who is not following the standards that have been enforced and hence expose vulnerability. Organizations should deploy periodic security vulnerability assessments and penetration tests. This can expose the security loopholes that a social engineer can exploit to attack.

D. Physical Access Authentication

Physical security will help minimize the chance of social engineer to have physical access to the equipment and premises. All employees are needed to have a form of identification card that should be produced at the entrance of the premises. This will ensure that only those persons authorized to be in the facility are granted access. Visitors can be escorted to where they need to go and required to wear a badge so as to identify them as a guest.

E. Incident Documentation And Reporting

When a social engineering attack occurs, the victims should report the incident to the relevant personnel before any active attack is made. For example if a user gives his password to anyone, it is advisable to change the password immediately. This can reduce the impact of an attack.

F. Suspicious Of New Persons

Users must be cautious of unfamiliar individuals and not give out information unless there is a confirmation of their identity. For instance, users that frequently call the technical support must be familiar with the personnel in that department.

G. Employee Background Checks

Industrial espionage and spying can use any possible method available. This is the same for a social engineer. Not all new employees have the goals of the organization at heart. Some people join organization so that they can gather and disclose as much information as possible. It is important for employers to carry out a background research on new employees or would be employees.

IV. METHODOLOGY

A. Online Survey

The basic purpose of online survey is to collect data from targeted users. We have conducted online survey among 114 users to know about the awareness of social engineering attacks in our around world. Following questionnaire is putted against online users:

Question 1. Do you know about Social Engineering?
Question 2. Which social networking sites do you use frequently?
Question 3. Do you ever reply/click/like against any unknown friend request/post/message/video received?
Question 4. If you receive a message to view a file or video on social networking site and from someone within your network, then it is safe to open the attachment?
Question 5. Is it safe to click a link: a link is through a popular website such as Google, Yahoo, Bing:
Question 6. A stranger calls your house and says there is some technical support of your ISP. He/ She says that there is some problem in their Internet connection and needs your password to fix it. Is it safe to provide your password?
Question 7. Do you ever reply against any received unwanted email?
Question 8. Do you ever share your personal information against any unwanted email/ offer through pop-up window/message by your interest etc.?
Question 9. Do you read the terms and condition whenever you registering on any server/website?
Question 10. Do you know that how many login ID and password you have created for different purpose on different website/server till date?
Question 11. Is your all login ID and password are totally different?
Question 12. In how much time interval you change your ID and password?
Question 13. If you receive a phone call or email with notification that you have won the lottery prize in their organization. All that is a processing fee in order to obtain the huge amount of money that they have won. What will you do in that case?
Question 14. You are in your final year of your studies/passed out and looking for a job. You receive a phone call from a recruitment agency. The person calling you and asks you whether you deposit a small amount of money so that they will find a suitable job according to your requirement .What will you do in that case?
Question 15. If you received a call and they introduce themselves that they are part of the Bank where your Bank Account is there. They asked you to answer some questions such as your (Bank Account Number, ATM Number, ATM Password etc .).Then what will you do in that case?
Question 16. Technology based security measures such as firewall, encryption ,antivirus and strong authentication will prevent social engineering fraud?
Question 17. Do you think is it necessary to call a company to verify the identity of its employee if presented with an ID Card?
Question 18. Do any unknown person or individual asks you to donate some money by showing some type of receipt of any

sanstha, orphanage?

B. Experimental Survey

We have conducted experimental survey concern to social engineering threats to know user awareness and response. In experimental survey we have design some attack and target the users to analyse their response.

1) Analysis Of Data Collected Through Online Survey: In this online survey we make a questionnaire and ask questions from users and record their responses.

a) Familiarities about Social Engineering

Sample Size	Employed User	Known about Social Engineering	Unknown about Social Engineering
114	66	34	32

Table 1

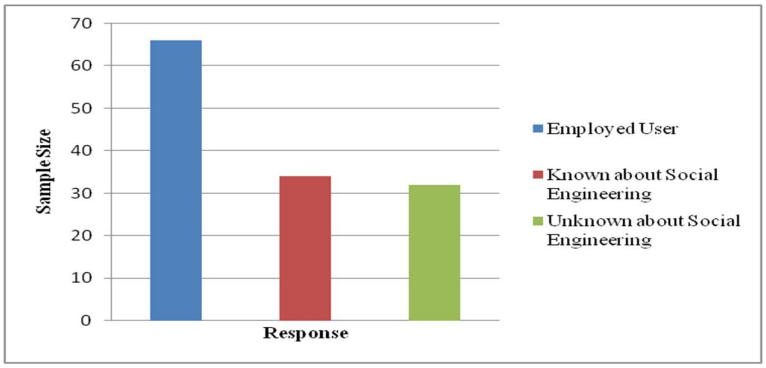


Fig 1

Here we take a sample size of 114 users, out of which 66 are employed users. Out of these 66 employed users 34 of them are known about social engineering and 32 of them are unknown about social engineering.

Sample Size	Unemployed User	Known about Social Engineering	Unknown about Social Engineering
114	48	32	16

Table 2

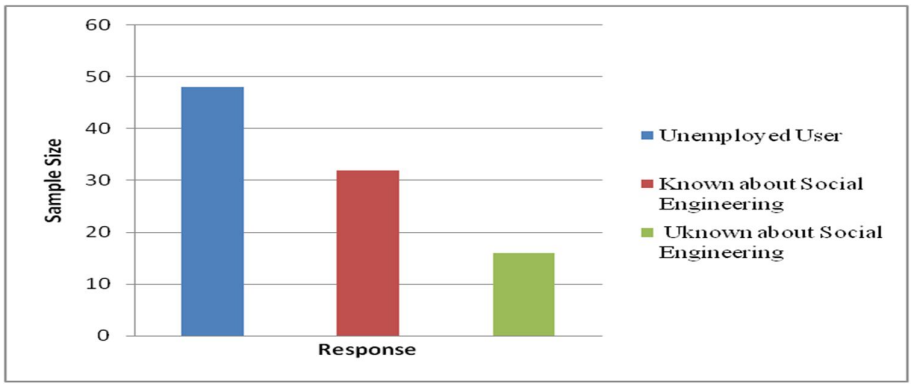


Fig 2

Volume 4 Issue II, February 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Here we take a sample size of 114 users, out of which 48 are unemployed users .Out of these 48 unemployed users 32 of them are aware about social engineering and 16 of them are not aware about social engineering. Users either employed or unemployed have to known about the attacks falls in the category of social engineering.

b) Users Alertness about Their Account

Sample size	Employed User	Users whose id's are diff	Users whose id's are same	Users who remember all id's	Users who don't remember all id's	Users change pwd<5 months	Users change pwd b/w 0.5-1 years	Users change pwd b/w 1-2 years	Users never change pwd
114	66	50	16	42	24	22	16	20	8

Table 3

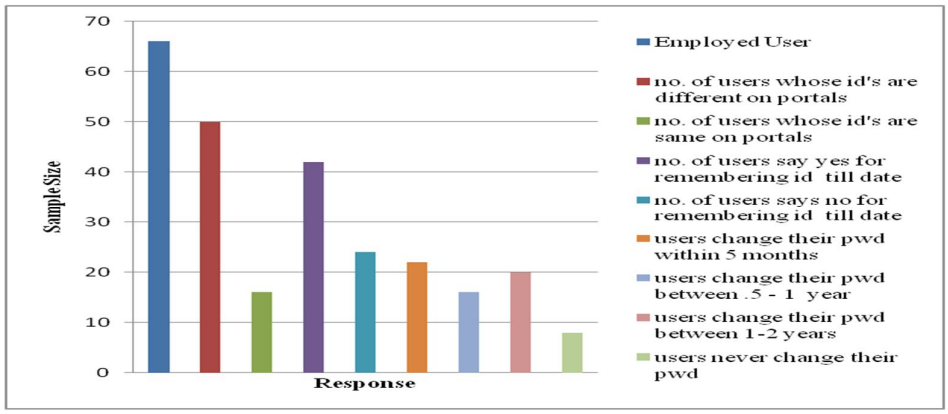


Fig 3

Sample size	Unemployed User	Users whose id's are diff	Users whose id's are same	Users who remember all id's	Users who don't remember all id's	Users change pwd<5 months	Users change pwd b/w 0.5-1 years	Users change pwd b/w 1-2 years	Users never change pwd
114	48	24	24	26	22	12	14	16	6

Table 4

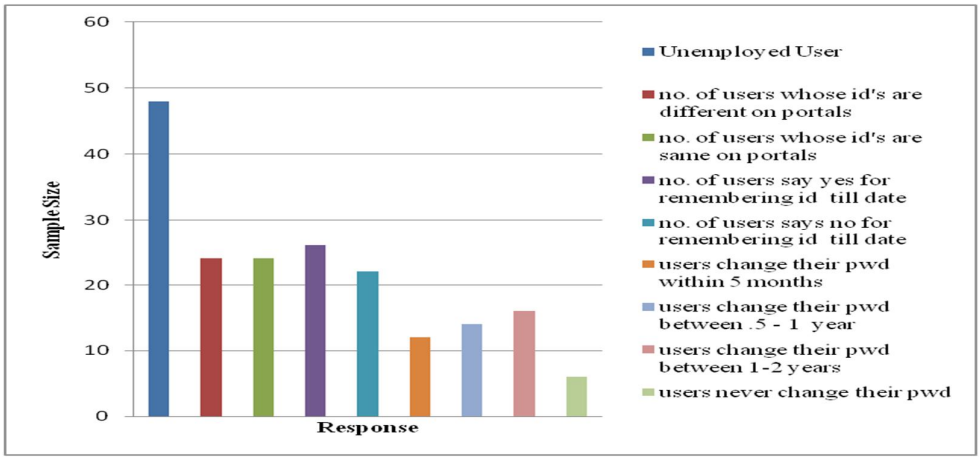


Fig 4

Here we take a sample size of 114 users, out of which 48 are unemployed users. Out of these 48 unemployed users, 24 users of them have multiple id's on different portals,24 of them have same id's on different portal, 26 users of them says yes for remembering id's till date,22 users of them says no for remembering id's till date.12 users of them change their password within five months, 14 users of them says change their password between 0.5 to 1 year, 16 users of them change their password between one year to two year and 6 users of them never change their password. Users either employed or unemployed have to be aware about making account on different portals. User should not use same id's for different logins and never use same password for them. Create unique passwords that that use a combination of words, numbers, symbols, and both upper- and lower-case letters. Don't use easily guessed passwords, such as "password" or "user". Do not choose passwords based upon details that may not be as confidential as you'd expect, such as your birth date, your Social Security or phone number, or names of family members. Don't write your password down anywhere.

2) Analysis Of Data Collected Through Experimental Survey:

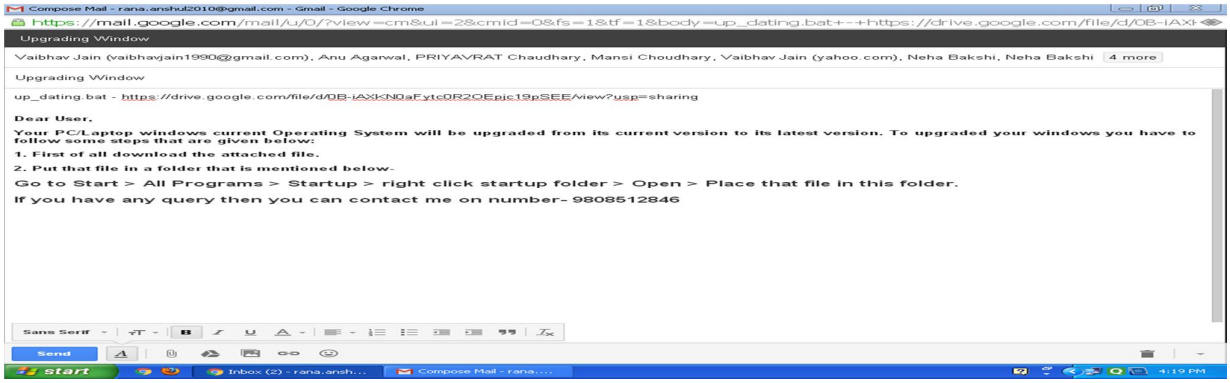


Fig 5

In this scenario we interact with several users and try to cheat them by using some tricks. We offer them to upgrade their operating system from its current version to the new version. And all the users show their interest in this activity. When all of them doing this process as we mentioned above, they all face some problem and contact me regarding their issues. This means that users are not much aware about social engineering attacks. Users who show their interest in computer are not aware about computer related attacks. Users should also aware about these types of attacks also. Even friends can also cheat us. So you should be aware of such types of known peoples and strangers.

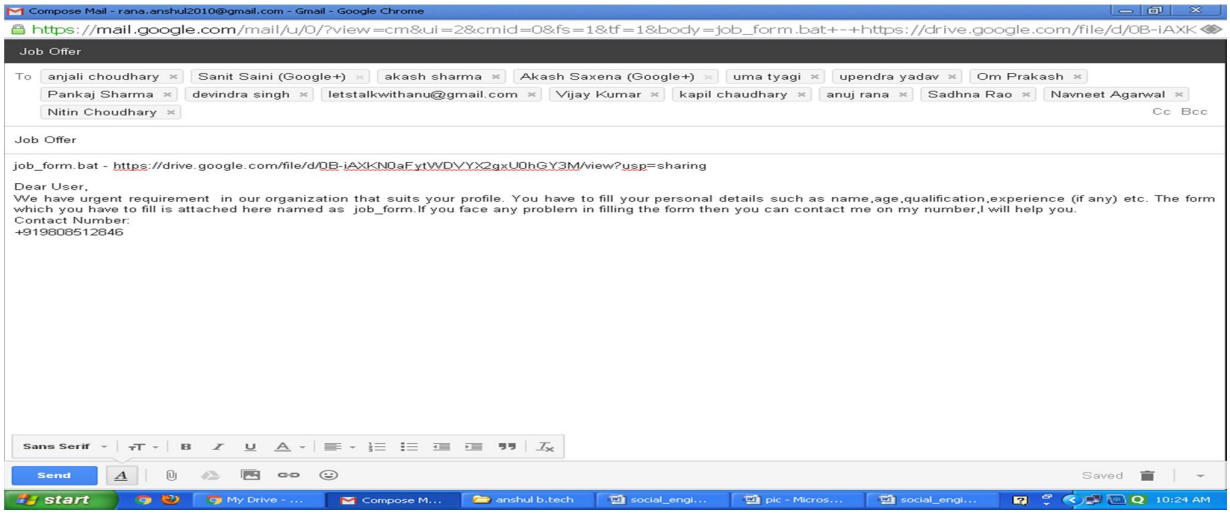


Fig 6

In this scenario we interact with several users and try to cheat them by using some tricks. We offer jobs to several users and all the users show their interest to get job. When all of them doing this process as we mentioned above, they all face some problem and contact me regarding their issues. This means that users are not much aware about social engineering attacks. Users who show their interest in computer are not aware about computer related attacks. Users should also aware about these types of

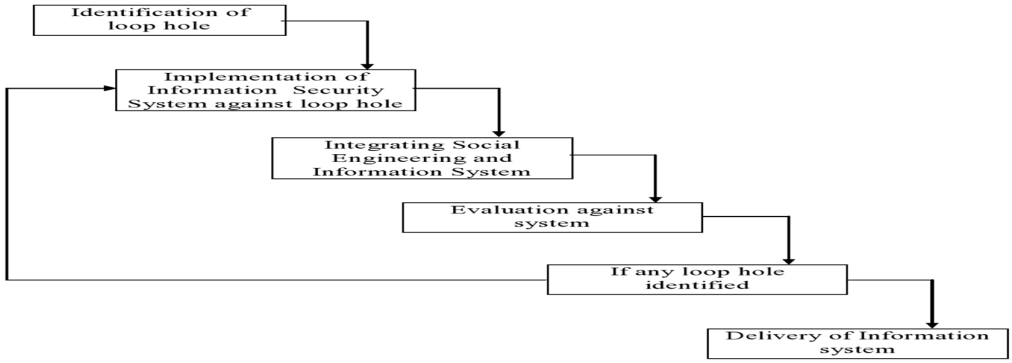
attacks also. Even friends can also cheat us. So you should be aware of such types of known peoples and strangers.

V. FINDINGS

Most of the users/individuals are unknown about Social Engineering.

A computer literate are even the victim of Social Engineering.
Every user can be cheated by knowing their weak points and needs such as job requirement etc.
Users either employed or unemployed do not read any type of document while doing any registration process.
To protect an organization/system, social engineering prevention is a continuous process and it should be integrated with Information System.
Every Software Application/institutional must have a complete guideline about social engineering attacks.

VI. FRAME WORK PROPOSED



A. Identification of Loop Hole

The service provider should be aware about the loop holes of their services provided by them. The common approach towards the inclusion of security within a system is to identify security requirements after the definition of a system. Service provider should consider the security threats their system faces, from the perspective of the sensitive resources within it, the possible access to these resources that potential attackers might wish to gain, the main characteristics of the potential attackers and the type of attack they are likely to carry out.

B. Implementation Of Information System Security Against Loop Hole

Once we understand the sensitive resources and threats, consider the technical security design for the system. The goal of this step is to design a system wide security infrastructure that can enforce the systems security policy in the face of risks identified in the thread model.

C. Integrating Social Engineering And Information System Security

Although Security is an important issue in the development of computerized system. Social engineering, in the context of information security, is the art of manipulating people so they give up confidential information. This is a type of confidence trick for the purpose of vital information gathering. Security of information system has become a well established field. Security is one of the main challenges that developers of information systems face.

D. Evaluation Against System

The introduction of security attack scenarios to test the system's response to potential attacks provides developers the ability to realistically check how the developed system will react to possible security attacks.

E. Delivery Of Information System

Now delivery of the system will be secure, armed and guided against any social engineering attacks.

VII. RESULTS AND DISCUSSION AFTER PROPOSED FRAME WORK

A new frame is drafted and implemented about social engineering attack. We again attack within a small group of individuals and now these individuals are responding in very secure way because of the framework we provided.

Volume 4 Issue II, February 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

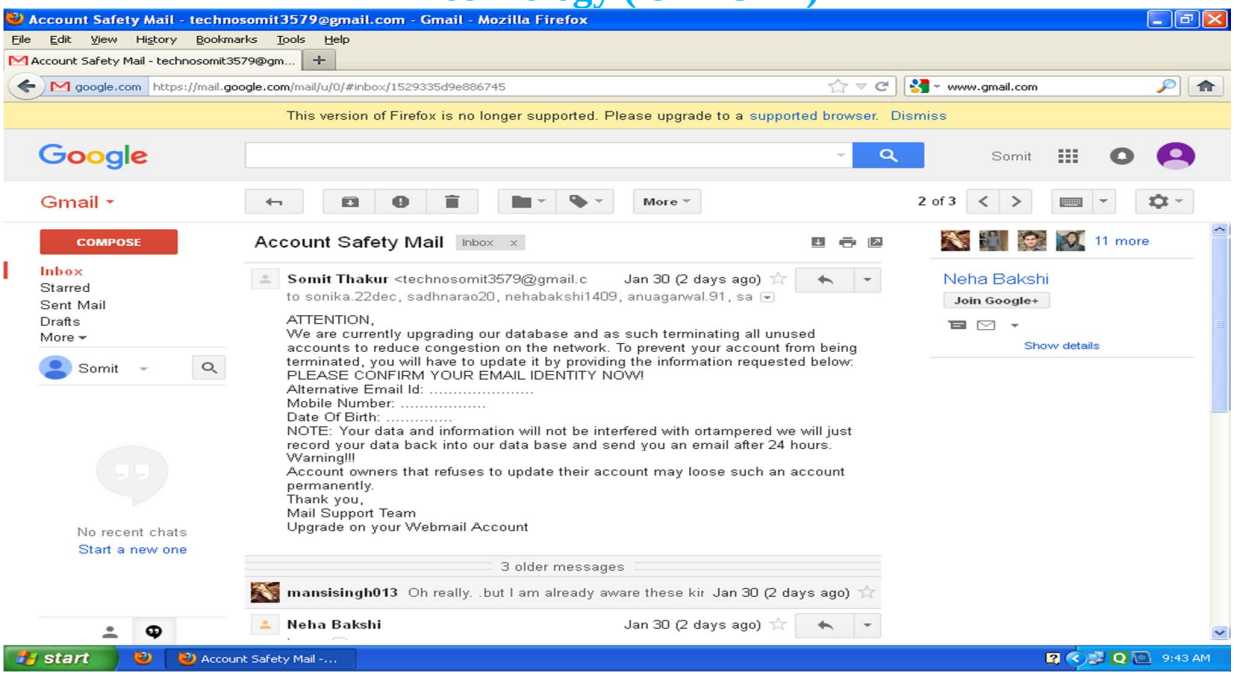


Fig 7

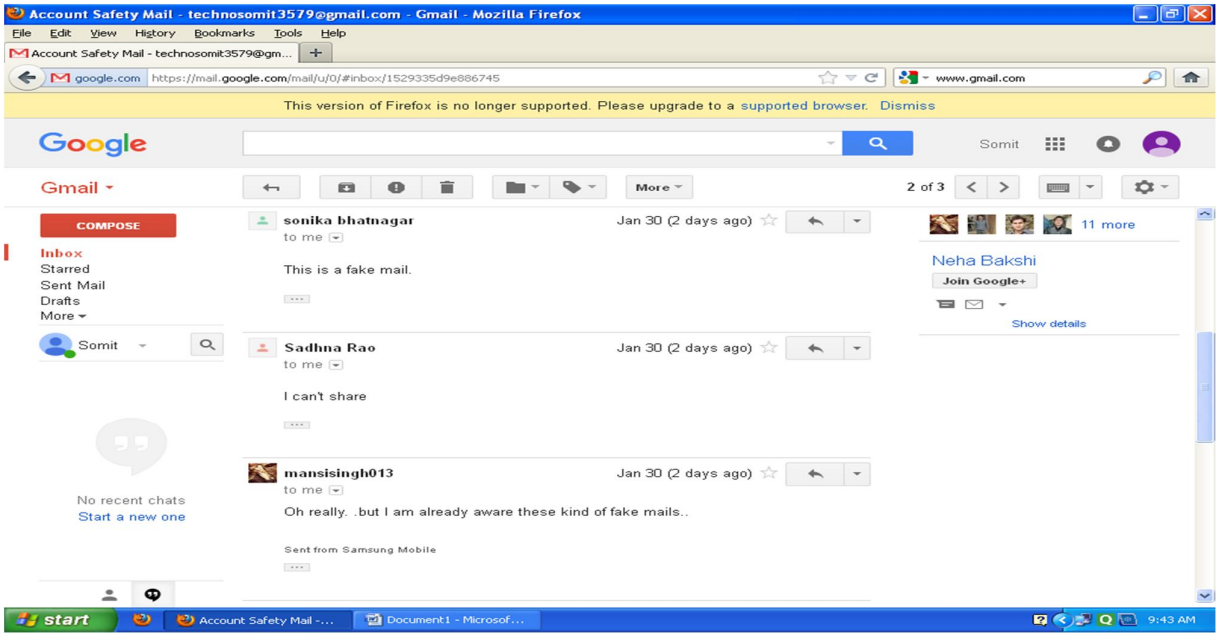


Fig 8

As we have provided a framework to protect users from social engineering attack. Now to test user awareness, we made a fake account on gmail and try to attack on them through mail to different users. Now these users respond in a different way. As we have attack on near about 20 users out of which 14 users does not respond anything. They just ignore that mail. The remaining users replies in a different manner and their responses are recorded in the above images as shown in above fig. This means that after drafted a social engineering attack framework, user are aware of these types of attacks. In present digital world no one can keep away from electronic devices. Now trend of security attacks are completely changed from cryptographic to social engineering. Now users/individuals can never be completely alert.

VIII. CONCLUSION

The goal of every company is to succeed, and the security of information is undoubtedly essential for this success to occur. In an effort for a company to comprehensively protect its information, it must pay careful attention to both technical security

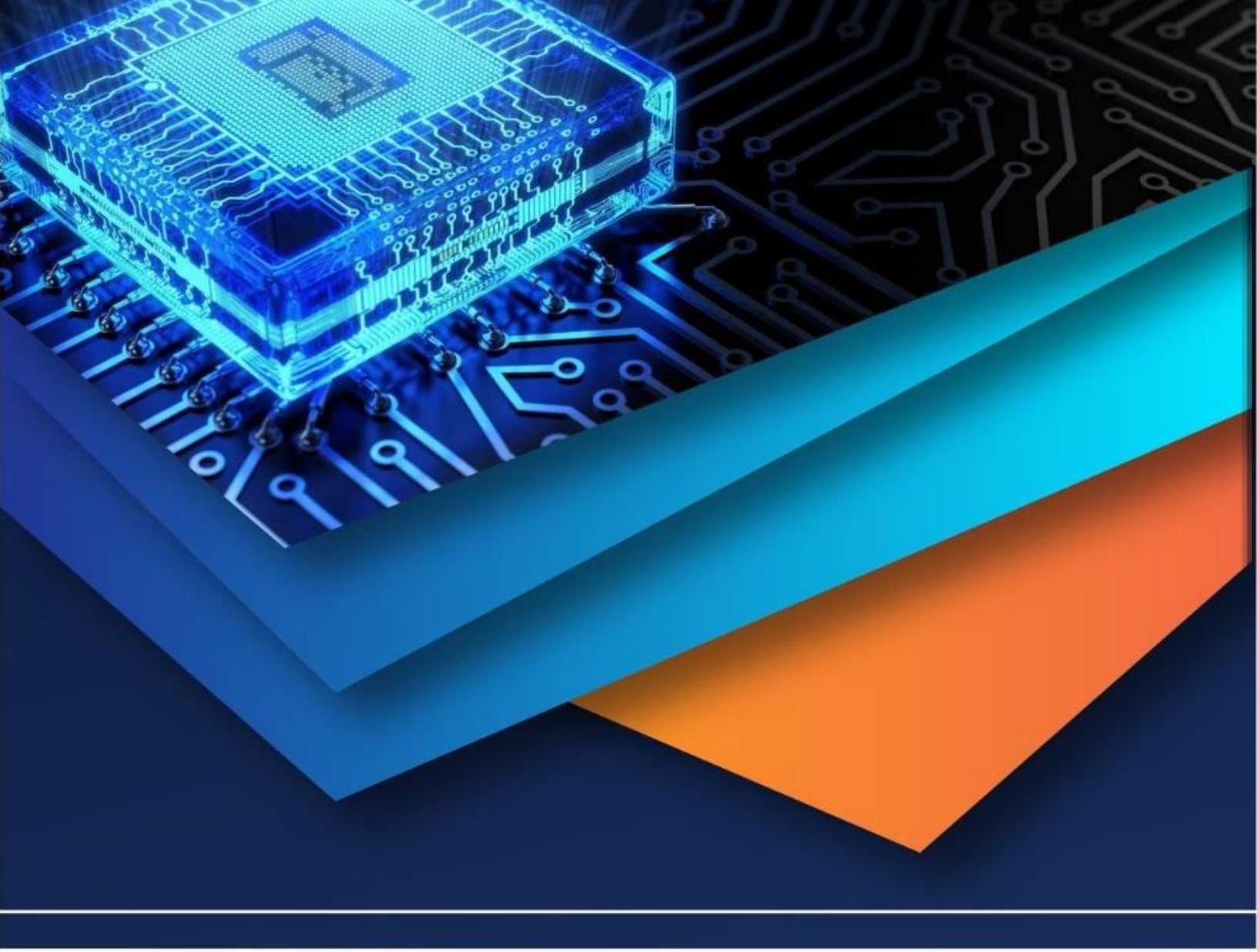
breaches and non-technical forms of hacking like social engineering. Even with the dangers of social media, companies possess the ability to inform their employees of the vast dangers these sites pose to both the individual and the company. Through an effective security awareness training program and extensive audits, a company can ensure that its employees understand the threat that social engineering poses to each employee. When employees collectively recognize potential signs of attacks and take personal responsibility for securing the company's information, the security culture of the company strengthens. When a company effectively equips its employees to protect themselves on social media and to recognize the psychological manipulation of social engineers, the company has completed the first and most important step in countering social engineering attacks. The security risks of social engineering are significant, and organizations must address social-engineering threats as part of an overall risk-management strategy. The best way to mitigate the risk posed by rapidly evolving social-engineering methods is through an organizational commitment to a security-aware culture. Ongoing training will provide employees with the tools they need to recognize and respond to social-engineering threats, and support from the executive staff will create an attitude of ownership and accountability that encourages active participation in the security culture.

IX. FUTURE SCOPE

This is a work in progress, and will continue to be updated as attack methods adapt and change with the times. I feel it contains some of the most current scientific, technical and psychological information on the topic of social engineering today. Our goal is to create a environment for the security professional as a penetration tester or enthusiast to learn and be armed with the most commonly used attack vectors today.

REFERENCES

[1] Kumar Anshul, Chaudhary Mansi, Kumar Nagresh, "Social Engineering Threats and Awareness: A Survey", EJAET Vol 2(11):1-5, 2015.
[2] Megha Gupta and Sameer Agarwal, "A Survey on Social Engineering and the Art of Deception", *International Journal of Information and Education Technology* (*IJIET*), 1 (1), pp. 31 – 35, 2012.
[3] Joseph A Cazier and Christopher M. Botelho, "Social Engineering's Threat to Public Privacy", Proceedings of the 6th Annual Security Conference, , Las Vegas, NV, 2007.
[4] Anubhav Chitrey, Dharmendra Singh and Vrijendra Singh, "A Comprehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model", *International Journal of Information and Network Security*, 1(2), pp. 45 – 53, 2012.
[5] Jeremy R Strozer, Sholom Cohen, AP Moore, David Mundie and Jennifer Cowley, "Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits", IEEE Security and Privacy Workshops, 2014.
[6] Devin Luco, "The Art of Social Engineering: A Research Note", http://anniesearle.com/ 2015.
[7] L J Janczewski and Lingyan (Rene) Fu, "Social Engineering Based Attacks: Model and New Zealand Perspective", Proceedings of the International Multiconference on Computer Science and Information Technology, 2010.
[8] Mahmoud Khonji, Youssef Iraqi, Andrew Jones, "Phishing Detection: A Literature Survey", IEEE Communications Surveys & Tutorials, 15(4), pp. 2091 – 2121, 2013.
[9] R.Chandramouli, "Emerging Social Media Threats: Technology and Policy Perspectives", Cyber Security Summit, 2011.
[10] A Karakasiliotis, M Papadaki and SM Furnell, "Assessing End-User Awareness of Social Engineering and Phishing", Proceedings of the 7th Australian Information Warfare and Security Conference, 2006.
[11] Mosin Hasan, Nilesh Prajapati and Safvan Vohara, "Case Study on Social Engineering Techniques for Persuasion", International journal on applications of graph theory in wireless ad hoc networks and sensor networks, Vol.2, No.2, June 2010.
[12] P. S. Maan and Manish Sharma, "Social Engineering: A Partial Technical Attack", International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012.
[13] Francois Mouton and H.S. Venter, "Social engineering detection model", IEEE, 321-32-10, 2010.
[14] Matthew J. Warren, Shona Leitch, "Social Engineering and its Impact via the Internet", Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, December, 2006.
[15] Sevgi Ozkan and Tolga Mataracioglu, "User Awareness Measurement Through Social Engineering", International Journal of Managing Value and Supply Chains (IJMVSC), Vol. 1, No. 2, December 2010.
[16] Jessica C Flack and Raissa M D'souza, "The Digital Age and the Future of Social Network Science and Engineering", Proceedings of the IEEE , 102, 12, pp.1873 – 1877, 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY