Bang of Social Engineering in Social Networking Sites

Shilpi Sharma, J.S. Sodhi and Saksham Gulati

Abstract This research paper is a brief study on social engineering that explores the internet awareness among males and females of different age groups. In our study, we have researched on how an individual shares his/her identity and sensitive information which directly or indirectly affects them on social networking sites. This information can be user's personal identification traits, their photos, visited places, etc. The parameters chosen for influence of social engineering in social networking sites are passwords, share ability, and awareness. This research briefly explains how people between age group of 13–40 years share their information over the web and their awareness of netiquettes. This information is then conclusively used to calculate average amount of sensitive information which can be extracted through social engineering for different age groups of males and females.

Keywords Social networking site · Social engineering · Share ability · Awareness · Passwords · Victim

1 Introduction

In today's world where technology is the necessity in everybody's life, social engineering is emerging as vital vicinity in social networking sites. Different services are available for individuals, enterprises, and organizations that have implemented variety of features in social networking sites. These sites provide a perfect platform for hackers and attackers. Information posted and shared by users are always under threat.

Shilpi Sharma (✉) · Saksham Gulati
ASET, Amity University, Noida, India
e-mail: ssharma22@amity.edu

Saksham Gulati
e-mail: saksham.gulati28@gmail.com

J.S. Sodhi
AKC Data Systems Pvt. Ltd., Amity University, Noida, India
e-mail: jssodhi@amity.edu

S.C. Satapathy et al. (eds.), *Proceedings of the International Congress on Information and Communication Technology*, Advances in Intelligent Systems and Computing 438, DOI 10.1007/978-981-10-0767-5_36

Social Engineering, in information security refers to as psychological manipulation of human mind to extract sensitive information [1]. It is an art of deceiving the victim fetching sensitive information that can benefit the hacker or cracker [2, 3]. Social engineering is a widely used technique for extracting information from people to process, counter and plot a structured cyber attack. It is an approach that helps to crack the personal data of unknown users, to find their weaknesses or strengths for an organized crime. In 2011, a survey was conducted by Dimension Research in U.S, Canada, Australia, U.K, Germany, and New Zealand on IT professionals and concluded that 48 % are victims of social engineering attacks in social networking sites [4].

It has been found that the most significant security risks are associated with social engineering [5]. With the changing threat scenario in cyber space [6], hacking skills of hackers are becoming sophisticated and difficult to track. Social networking sites are progressively accessed by users of different age groups from teenagers to old people and the irony is users by pass their concern toward information security [7, 8]. Furthermore, information on social networking sites is accessed automatically by social engineering bots by providing data in machine readable form. The most common ways of social engineering includes distribution of adware's, uploading explicit content as advertisement, distribution of malware through ads, prank calls, surfing through web, fake emails, uploading of false information, etc.

Our paper explores the implications of age and gender in social engineering to fetch the password and know about the awareness of respondents, while sharing information in social networking sites. In our evaluation, we test our approach on gender and age of users on social networking sites using three basic measures, i.e., passwords, share ability, and awareness. As maturity comes with age and experiences in both the genders, our primary dataset is categorized into high, medium, and low level. It presents the variations in password of males and females of different age groups and awareness of sharing information over the internet [9, 10]. Social engineering is the biggest threat both at internal as well as external level for any company or an individual [11]. Thus, social engineering can be made easy by making them vulnerable to cyber crimes.

The rest of the paper is organized as follows: Sect. 2 summarizes research related to social engineering in social networking sites, Sect. 3 describes the methodology and result of concept implementation is outlined in Sect. 4. In Sect. 5, we draw conclusions from our findings and propose future research.

2 Related Work

Social engineering attacks are not only well known in practice but also in literature [12, 13]. Instead of pointing toward vulnerabilities in technical systems, the social engineering targets the weaknesses of people. Research on privacy implications of social networking sites has been discussed in a number of publications. The most

widely used social engineering techniques include social surfing, dumpster diving and shoulder surfing. These techniques are used by hackers on everyday basis to gather information about the victim [14]. Password guessing is a common way to crack passwords as no major risk is associated with it [15, 16]. Password guessing is mostly a psychological act where technology or softwares are not the primary factor [17]. The main motive of social engineering is to crack sensitive information of a victim as passwords related information holds the top priority [15–17].

Social engineering is totally dependent on an individual's personality [17]. A survey states that people with unstable personality can be manipulated easily for extracting information through them [15]. And people with strong personality do not share their sensitive information easily and mentioned social engineering as an internal threat [18]. Generally, individuals choose password based on their traits and if an attacker understands an individual thoroughly then sensitive information can be easily extracted [19]. Thus, it also provides the importance of training given to every user to prevent information against social engineering [20].

Social engineering comes as a message in the form of request that requires victims to accept or respond [21]. The attacker creates multiple fake profiles that impersonate with victims friend, relatives, or a famous person in social networking sites. Although many organizations control security threats but sometimes fails to recognize the dangers associated with social engineering attacks [7].

3 Research Methodology

The basic idea of research methodology states that "every mind can be tricked and manipulated" [4, 9]. The statement indicates that the most secure system in this world can be cracked through human hacking or social engineering [19]. For the study of awareness and sharing passwords, 400 samples with equal number of males and females are chosen and they are studied for a particular interval [23]. All their online social activities are recorded as a part of research to collect primary data. Their passwords were gathered and classified into three categories easy, medium, or difficult to crack [22]. To capture the potential personnel awareness and share ability, we include age and gender in the survey. Age and gender has been studied to come across the social engineering threats and effectiveness of internet security [23, 24].

4 Results

The sample size of our research was 400 which comprises of 200 males and 200 females to define their authenticity and security while creating passwords. This study is conducted on three social networking sites—Instagram, Facebook, and

LinkedIn. LinkedIn mostly have professional profiles hence high-quality data was shared while Instagram had profuse database of personal photographs. Facebook was significant to link the accounts with assured authenticity of data.

4.1 Password

Password is a basic login criterion to access any account in social networking sites. They are the most important credentials for logins and must be secured properly. Passwords must contain both upper and lower case characters along with special characters to make it strong. In our research, a study has been conducted among males and females of different age groups which have been categorized into two defined age groups with 13–20 years and 21–35 years.

The chart shows the level of difficulty, in terms of complexity of passwords:

(1) Difficult: The passwords which have a combination of uppercase and lowercase alphabets along with special characters and have no usual meaning in any language are classified as difficult. Such passwords are difficult to crack, guess, or even shoulder surf [25].
(2) Medium: These passwords generally contain both uppercase and lowercase alphabets with special characters. However, they can be easily guessed or cracked because they are either close to predefined dictionary word or have a meaning related to something that user generally talks about.
(3) Easy: These passwords are very easy to guess as they generally have no mixing of uppercase and lowercase alphabets. Also, the passwords are short in length and carry a meaning closely related or associated to users.

Figure 1 shows that maximum users lying in male category have password of medium level. This interprets that password lacks combination of uppercase and lowercase characters along with special characters that makes it easy to crack using predefined dictionary. This category mostly comprise of teenagers who use internet on regular basis. As female use easy passwords, it concludes that the respondents are not concerned about the password leakage due to lack of knowledge about cyber crimes.

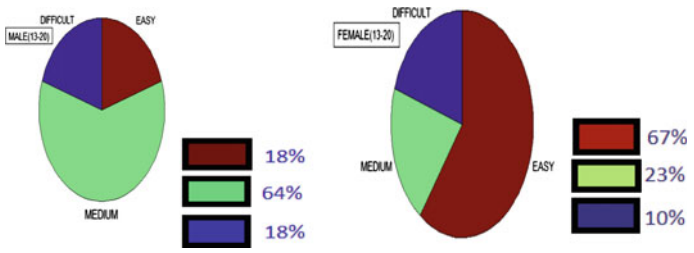

Fig. 1 Pie-chart showing male and female response for age group 13–20 years for password

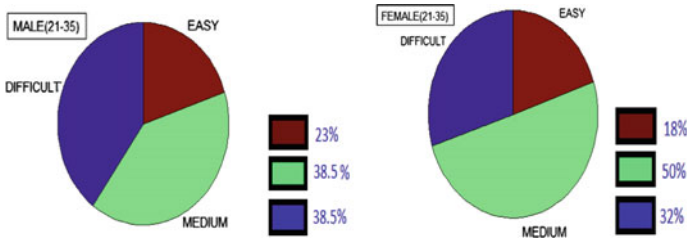

Fig. 2 Pie chart showing response of males and females of age 21–35 for password

Figure 2 explores a general change toward males and females in age group of 21–35 as they have shifted or inclined to a more secure password. The figure represents shifts from easy to difficult level of passwords. It can be clearly concluded from the result that age is proportional to the maturity of mind. Hence social engineering of a person in minor age group is easier.

Thus, the result shows that male from age group 21–35 creates more difficult passwords than females. And females store easy passwords that changes drastically as per age groups which develops with maturity and experience.

4.2 Share Ability

Data share ability is the measure of data that one shares on social networking sites through which a user can be classified as a potential victim to hacker.

Different levels of share ability with respect to age and gender are categorized as

(1) High: Too much sensitive data is shared on social networking sites which can be used against the user that can be unsafe. This includes phone number, address, private photos, daily movements, etc.
(2) Medium: The data or information shared by user is as per the requirement of social networking sites so, not much data is shared.
(3) Low: People lying in this category share very less amount of data. Only a few pictures are uploaded with no personal information. People in this category generally do not show much interest in social networking sites.

Figure 3, represents the amount of data shared by males and females of different age groups.

Moreover, males and females of age group 21–35 show that they share very high amount of data on internet (Fig. 4).

Here we found that as per the demand of social networking site, people shares good amount of personal data. Males of age group 13–20 generally shares more information. Also, change in age group data directly influences share ability. With growing age, users gain experience of cyber world and cyber crimes that influence data share ability in both males and females.

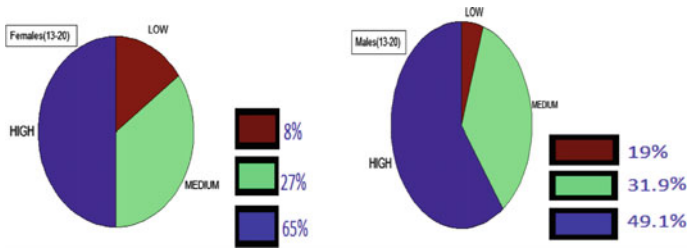

Fig. 3 Pie chart showing share ability of female and male of age group 13–21

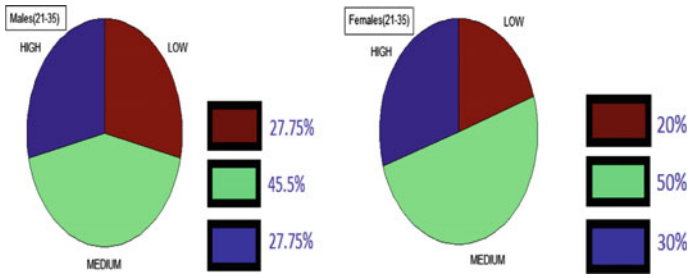

Fig. 4 Pie chart showing share ability of male and female of age group 21–35

4.3 Awareness

Awareness can be defined as a measure of knowledge about the crimes related to internet. A responsive user knows about the consequences of uploading sensitive information on social networking sites and can easily identify how to protect information leakage within the social networks. Also, user may share his photos and phone number on Facebook and restrict it to be viewed by few only.

Based on different levels of awareness with age and gender are categorized as:

(1) High: This category generally contains technically sound engineers and professionals or prompt users of social networking site. People lying in this category share very high amount of sensitive information but they know how to protect it.
(2) Medium: People of this category have some idea about private security on social networking site. They never use high profile security system like two-way authentication nor do they reply to requests over email to showcase their profile.
(3) Low: People of this category do not have much idea about the usage of their sensitive information by providers or third parties of social networking sites. These persons generally send and accepts friend request to and by unknown people (Figs. 5 and 6).

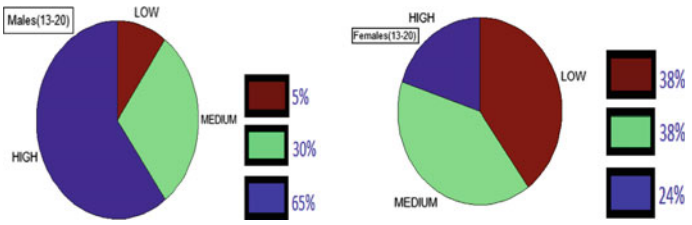

Fig. 5 Pie chart showing awareness of male and female of age group 13–20

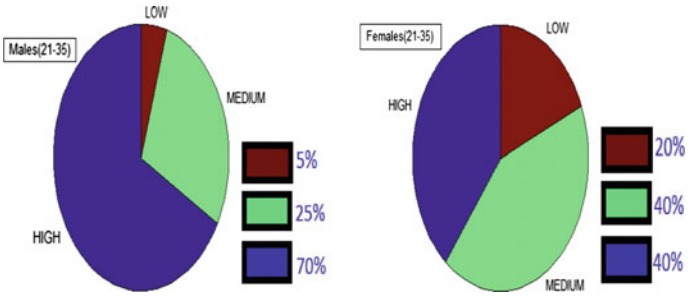

Fig. 6 Pie chart showing awareness of male and female of age group 21–35

The result shows that males are generally aware about the cyber crimes. A huge amount of data is shared over the internet and becomes a necessity to provide security otherwise the user will be trapped as a victim toward cyber crime. High awareness includes good knowledge of privacy over social networking sites that include hiding photos from anonymous, two token authentication and secondary email to reset passwords. It has been observed that most people in age group 21–35 of both genders had enough knowledge about cyber crimes. And females of age group 13–20 had limited knowledge about cyber crimes as compared to males of same age group.

So, it is pragmatic that males have high awareness among internet crimes and knows how to hide their private data or safeguard themselves from being a victim. A good variation was found in female category in terms of awareness with age.

5 Conclusions and Future Work

Social engineering can be used to exploit any human vulnerability either emotional or psychological and our study clearly shows that females are weaker as compared to the males. It was found during the study that females are emotionally weak as compared to males which often results in wrong decisions. Also females share more information and apply comparatively weaker passwords, hence it concludes that

females in general are easy target for social engineering. As deducted from the survey, it can also be concluded that males are more cautious than females of same or different age groups. They are more aware of the consequences of cyber crimes. With age comes the maturity and awareness about cyber experiences. So seniors keep track of their passwords.

Social engineering is a never ending threat to Information. Social engineering can only be prevented by means of experience since there is no formal professional training defined for the same. More of the training or knowledge is required for females of every age group. The user should be trained and made aware of social engineering threats inclusive of the factors that may cause serious attacks.

Practical training including psychology sessions are some of the best ways to train professionals against social engineering.

References

1. Irani, Danesh, Marco Balduzzi, Davide Balzarotti, Engin Kirda, and Calton Pu. "Reverse social engineering attacks in online social networks." In Detection of intrusions and malware, and vulnerability assessment, pp. 55–74, Springer Berlin Heidelberg (2011).
2. Mitnick, Kevin D., and William L. Simon.: The art of deception: Controlling the human element of security. John Wiley & Sons (2011).
3. Huber, Markus, Stewart Kowalski, Marcus Nohlberg, and Simon Tjoa.: Towards automating social engineering using social networking sites. In: Computational Science and Engineering, vol. 3, pp. 117–124. IEEE (2009).
4. Algarni, Abdulmohsen, Yue Xu, and Thomas Chan.: Social Engineering in Social Networking Sites: The Art of Impersonation. In: Services Computing, pp. 797–804. IEEE. (2014).
5. Hadnagy, Christopher.: Social engineering: The art of human hacking. John Wiley & Sons (2010).
6. Thakral A., Rakesh N. and Gupta A.: Area Prone to Cyber Attacks., vol. 39, pp 40. CSI Communications (2015).
7. Sharma, S., & Sodhi., J. S.: Social Network Analysis & Information Disclosure: A Case Study. International Journal of Computer, Electrical, Automation, Control and Information Engineering vol: 9, pp. 567–575. WASET (2015).
8. Long, J. No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing. Syngress. (2011).
9. Graves, K. CEH: Official Certified Ethical Hacker Review Guide: Exam 312–50. John Wiley & Sons. (2007).
10. Uebelacker, S., & Quiel, S. The social engineering personality framework. In: Socio-Technical Aspects in Security and Trust (STAST), pp. 24–30. IEEE. (2014).
11. Greitzer, Frank L., Jeremy R. Strozer, Sholom Cohen, Andrew P. Moore, David Mundie, and Jennifer Cowley.: Analysis of Unintentional Insider Threats Deriving from Social Engineering Exploits. In: Security and Privacy Workshops (SPW), pp. 236–250. IEEE. (2014).
12. Stringhini, G., Kruegel, C., & Vigna, G.: Detecting spammers on social networks. In: 26th Annual Computer Security Applications Conference pp. 1–9. ACM. (2010).
13. Webb, S., Caverlee, J., & Pu, C.: Social Honeypots: Making Friends With A Spammer Near You. In: CEAS. (2008).
14. http://resources.infosecinstitute.com/cyber-kill-chain-is-a-great-idea-but-is-it-something-your-company-can-implement/.

15. Kumar, N.: Password in practice: An usability survey. Journal of Global Research in Computer Science, vol. 2(5), pp.107–112. (2011).
16. Medlin, B. D., & Cazier, J. A.: An empirical investigation: Health care employee passwords and their crack times in relationship to hipaa security standards. International Journal of Healthcare Information Systems and Informatics (IJHISI), vol. 2(3), pp. 39–48. (2007).
17. Meadows, D. Thinking in Systems: A Primer, Chelsea Green Publishing, (2008).
18. Parrish Jr, J. L., Bailey, J. L., & Courtney, J. F. A Personality Based Model for Determining Susceptibility to Phishing Attacks. Little Rock: University of Arkansas. (2009).
19. Cappelli, D. M., Moore, A. P., & Trzeciak, R. F.: The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes, Addison-Wesley. (2012).
20. Kuo, C., Romanosky, S., & Cranor, L. F.: Human selection of mnemonic phrase-based passwords. In: 2nd symposium on Usable privacy and security, pp. 67–78. ACM. (2006).
21. Sterman, J. D.: Business dynamics: systems thinking and modeling for a complex world, vol. 19. Boston: Irwin/McGraw-Hill. (2000).
22. Algarni, A., Xu, Y., Chan, T., & Tian, Y. C.: Toward understanding social engineering. In: 8th International Conference on Legal, Security and Privacy Issues in IT Law, (Critical Analysis and Legal Reasoning, pp. 279–300, The International Association of IT Lawyers (IAITL). (2013).
23. Medlin, B. D., Cazier, J. A., & Foulk, D. P.: Analyzing the vulnerability of US hospitals to social engineering attacks: how many of your employees would share their password? International Journal of Information Security and Privacy (IJISP), 2(3), pp. 71–83. (2008).
24. Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J.: Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions. In: SIGCHI Conference on Human Factors in Computing Systems, pp. 373–382. ACM. (2010).
25. Workman, M. Wisecrackers.: A theory-grounded investigation of phishing and pretext social engineering threats to information security. Journal of the American Society for Information Science and Technology, vol. 59(4), pp. 662–674. (2008).