Vulnerability Analysis of Social Media Accounts Against Cyber Attacks

Ahamd Farid Aseel[1], Yashar Abri[1]

[1]*M.Sc. Student, Information Technology Engineering, Faculty of Engineering, College of Farabi, University of Tehran*
faridaseel.4all@gmail.com, yasharabri@ut.ac.ir

Abstract

This article examines the vulnerability of social media accounts against cyber attacks. With the increasing number of users on these platforms and the accumulation of sensitive information in user accounts, the security of these networks is facing cyber threats. The article analyzes phishing attacks and brute-force attacks as penetration methods and investigates the weaknesses of social media networks against these attacks. Additionally, social engineering, as a deception-based and psychological attack on individuals within social networks, is analyzed. Through a questionnaire, users' attitudes and behaviors regarding security measures are evaluated. The results indicate that some users use strong passwords but do not change them regularly, and users' awareness of security practices is inadequate. The security of social media accounts is of utmost importance, and this article emphasizes that increasing users' and administrators' awareness of cyber threats and countermeasures is crucial to strengthening the security of these platforms. The information presented in this article can contribute to enhancing the security of accounts and protecting users' personal information against cyber attacks.

Keywords: *Cyber Attacks, Social Networks, Phishing, Brute Force, Penetration.*

1 Introduction

In the world of digital communications and the widespread adoption of social networks, individuals increasingly utilize these platforms for communication, information sharing, and social interactions. However, with the continuous expansion of user numbers on these networks and the accumulation of sensitive information and user credentials in their accounts, the issue of security and vulnerabilities has become one of the most critical and prevalent concerns. Furthermore, as technology advances and cyber threats escalate, social networks are constantly facing various types of attacks. Attacks such as phishing, brute force, and social engineering are among the methods exploited by malicious actors to infiltrate user accounts and misuse sensitive information [1]. The main

objective of this scientific article is to examine the vulnerability of social media accounts against cyber-attacks. To achieve this goal, we delve into the analysis of phishing and brute force attacks as two important penetration methods on user accounts, evaluating the security weaknesses of these networks against such attacks. Additionally, we investigate and analyze social engineering as an attack based on deception and psychological manipulation of individuals. Through a comprehensive and reliable questionnaire, we assess users' attitudes and behaviors regarding security measures on social networks. This article emphasizes that users' awareness of cyber threats and countermeasures is key to strengthening the security of social media accounts and safeguarding their personal and confidential information. Given the increasing significance of social networks in modern society and their prominent role in human interactions, we hope that this article contributes to enhancing users' and administrators' awareness of information security and their accounts, ultimately leading to an overall improvement in the security of these platforms.

2 Hack

Hacking is a computer crime that involves using social media websites to gain unauthorized access to computers or digital devices. Cybercriminals can employ various attack methods to gain access to the targeted users' digital devices [2]. They send emails or messages to users of social media sites, and when the user clicks on a suspicious link, the hackers gain unauthorized access to information through hacking [3]. Two types of attacks are commonly used by cybercriminals: targeted attacks and opportunistic attacks. In targeted attacks, hackers use specific tools to attack a particular target, while opportunistic attacks utilize viruses and worms. This type of attack is especially carried out by hackers, spammers, and cybercriminals [4].

2.1 Phishing

Phishing refers to a type of cyber attack where the goal is to gain access to sensitive and important user information through deception and forgery and exploit it for malicious purposes. In this type of attack, attackers encourage users to provide sensitive information such as usernames, passwords, banking details, and similar information by sending deceptive messages or fake websites [4]. Social networks as the primary target of phishing attacks: Given the large number of users and the various personal information shared on social networks, these platforms are considered the primary target of phishing attacks. Attackers typically attempt to persuade users to enter their sensitive information on various pages by sending deceptive links or pages [5]. Consequences of phishing attacks on social networks: Phishing attacks result in the misuse of users' sensitive information. Attackers may use the obtained information for targeting, fraud, identity theft, and other malicious activities [6].

2.2 Combation Phishing

1. Awareness and Education:

   Raising awareness among users about different phishing attacks and educating them on methods to detect deceptive messages and pages can significantly improve the security of their accounts.

2. Detection of Suspicious Links:

   Using tools and software that detect suspicious links and inform users to refrain from accessing suspicious pages [5].

3. Verifying Website Identities:

   Users should carefully verify the identity of websites and only enter sensitive information on official and reputable pages.

4. Software Updates:

   Regularly updating software and operating systems to patch vulnerabilities and potential security weaknesses [7].

2.3 Brute Force

In a brute force attack, the attacker attempts to gain access to the target user's account by using automated methods and extensive trial and error. The attacker tries all possible combinations to discover the user's password. If the account's password is weak and easily predictable, the attacker can easily penetrate the desired account and access the user's personal information, images, and content. Brute force attack is one of the most commonly used methods to infiltrate systems and user accounts and has been employed extensively in the past. From a technical perspective, this attack takes two main forms: brute force attack, which involves trying different combinations word by word, and dictionary-based brute force attack, which uses a list of words to guess the password [8].

2.4 Combatting Brute Force

To prevent brute force attacks, users should use strong and complex passwords that include a combination of uppercase and lowercase letters, numbers, and symbols. Additionally, enabling security features such as two-factor authentication can significantly enhance the security of user accounts. Given the increasing importance of social networks and the information stored in user accounts, it is essential for users and administrators of these networks to be aware of the vulnerabilities and threats posed by brute force attacks and take necessary actions to strengthen the security of these platforms [9].

2.5 Social Engineering

Social engineering is one of the most complex and popular methods of attacking the security of social networks. In this method, the attacker utilizes psychological tricks and social knowledge to prompt users to provide sensitive information and their credentials. With the increasing use of social networks and the importance of personal information in these environments, social engineering has become one of the biggest security threats in these networks [10].

As a deception-based attack, social engineering seeks to persuade individuals to perform inappropriate actions and disclose their sensitive information by exploiting their motivations, needs, and fears. Common social engineering techniques include phishing emails, enticing messages, and unknown phone calls, with the aim of extracting personal information and gaining access to user accounts [11].

To prevent social engineering attacks, users should consider the following:

- Do not trust unfamiliar and suspiciously sent information.
- Avoid sharing sensitive information and personal credentials with unknown individuals.
- Enable two-factor authentication and other security features in user accounts.
- Ensure the validity and reliability of received website sources and messages.

3 Methods

In this study, a questionnaire was used as a tool for data collection. This questionnaire consists of ten main questions presented with options A, B, and C for participants to respond to. The responses to this questionnaire were completed by individuals from the Persian-speaking community in various countries, including Australia, Iran, Afghanistan, and some European countries. The participants in this questionnaire include individuals with different educational levels, including Ph.D., Master's, Bachelor's, and lower levels. Furthermore, the design and collection of responses were conducted online.

In this research, responses from 80 participants were obtained. The questionnaire was distributed randomly among users of social networks such as Facebook, Instagram, and Telegram. After data collection, statistical analysis was performed, and the results were interpreted statistically. The questionnaire used in this paper is available in appendix 1 .

4 Results

The results showed that 53.3% of users always use strong passwords (including uppercase and lowercase letters, numbers, and symbols) for their accounts, and 46.7% do use this

type of password, but not always. Additionally, 80% of users update their passwords regularly, but not consistently, while 13.3% never change their passwords.

Regarding sharing sensitive information, 20% of users always share sensitive information, and 40% do so cautiously, while 40% do not share sensitive information at all.

The results indicate that 40% of users always check attachments before opening them, 26.7% do so cautiously, and 33.3% ignore this step.

Regarding the use of security apps and extensions, 13.3% of users always use them, 26.7% use them cautiously, and 60% do not use these tools at all.

Results show that 47.6% of users have experienced phishing or attempted unauthorized access to their social media accounts, while 26.7% of users have not experienced such attacks. Additionally, 26.7% of users are not familiar with phishing and lack sufficient awareness.

Regarding actions taken after experiencing phishing, the results indicate that 53.3% of users reported the incidents and took necessary measures to protect their accounts, while 46.7% of users did not take any actions.

Regarding awareness of security measures related to social media accounts, 53.3% of users have sufficient awareness, while 46.7% lack sufficient awareness.

Regarding the use of public social networks or public accounts for communication and sharing personal information, 46.7% of users use these networks, while 53.3% do not use them.

Regarding awareness of cyber threats and ways to counter them, 20% of users have sufficient awareness, while 80% lack sufficient awareness. These results indicate the need for promoting cybersecurity awareness and increasing users' knowledge about cyber threats.

5 Conclusion

In conclusion, the results indicate that a significant portion of users still lack sufficient awareness regarding cyber threats and ways to counter them. Therefore, increasing user awareness about cyber threats and protective measures on social media platforms requires further efforts from organizations and security-related entities.

By implementing necessary changes in user behavior and attitudes and promoting the importance of security for social media accounts, a considerable improvement in the security of these platforms and a reduction in security breaches and abuses can be achieved. As an initial study, these findings can serve as a motivational factor for conducting further research and taking more practical actions to enhance the security of user accounts on social media platforms.

References

[1] S. Y. A. A. M. subhi R. M. Zeebaree, "Social Media Networks Security Threats, Risks and Recommendation: A Case", in International Journal of Innovation, Creativity and Change. www.ijicc.net, 2020.

[2] A. Power, "What is social media?", British Journal of Midwifery, vol. 22, pp. 896-897, 2014.

[3] J. C. Bertot, P. T. Jaeger, and D. Hansen, "The impact of polices on government social media usage: Issues, challenges, and recommendations", Government information quarterly, vol. 29, pp. 30-40, 2012.

[4] S. Norden, "How the internet has changed the face of crime", 1554411 M.S., Florida Gulf Coast University, Ann Arbor, 2013.

[5] C. Konradt, A. Schilling, and B. Werners, "Phishing: An economic analysis of cybercrime perpetrators", Computers & Security, vol. 58, pp. 39-46, 5, 2016.

[6] K. J. Mitchell, D. Finkelhor, L. M. Jones, and J. Wolak, "Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization", Journal of Adolescent Health, vol. 47, pp. 183-190, 2010.

[7] M. Omar Saeed Al, "Threats and Anti-threats Strategies for Social Networking Websites", International Journal of Computer Networks & Communications, vol. 5, pp. 53-61, 2013

[8] Jan Vykopal. A Flow-Level Taxonomy and Prevalence of Brute Force Attacks. In Advances in Computing and Communications, pages 666–675, Kochi, India, 2011. Springer.

[9] A. P. a. M. T. Enrico Franchi, "Information and Password Attacks on Social Networks", in JITR, Italy, 2015.

[10] F. Mouton, L. Leenen, and H. S. Venter, "Social engineering attack examples, templates and scenarios", Computers & Security, vol. 59, pp. 186- 209, 6, 2016.

[11] E. U. Osuagwu, G. A. Chukwudebe, T. Salihu, and V. N. Chukwudebe, "Mitigating social engineering for improved cybersecurity", in Cyberspace (CYBERAbuja), 2015 International Conference on, 2015, pp. 91-100.

Appendix

sample questionnaire: Below is a sample questionnaire used in this article.

1. Do you use a strong password (including uppercase and lowercase letters, numbers, and symbols) for your social media accounts?
A.Yes, always
B.Yes, but not always
C.No, I don't use one at all

2. Is your password for social media accounts up to date and changed periodically?
A.Yes, I regularly change my password
B.Yes, but not regularly
C.No, I never change the password

3. Do you share sensitive information (such as personal information, phone number, home address, etc.) in your social media posts and profile?
Yes, always
Yes, but with caution
No, I don't share sensitive information

4. Do you review attachments you receive on social media (such as files, links, etc.) before opening them?
A.Yes, always
B.Yes, but with caution
C.No, they are ignored

5. Do you use security-related apps and extensions to protect your social media accounts?
A.Yes, always
B.Yes, but with caution
C.No, I don't use them at all

6. Have you ever experienced phishing or attempts to infiltrate your social media accounts?
A.Yes, I have experienced it
B.No, I have never experienced it
C.I don't know what phishing is

7. If you have experienced phishing or intrusion attempts, have you reported it and taken necessary actions to protect your account?
A.Yes
B.No

8. Do you have sufficient knowledge of security measures related to social media account protection?
A.Yes
B.No

9. Do you use public social networks or public accounts for communication and sharing personal information?
A.Yes
B.No

10. Are you knowledgeable about cyber threats and ways to combat them?
A.Yes
B.No