Journal of Knowledge-Research Studies

Behaviors Related to Security and Privacy of Social Network Users: A Study of Threats Based on Social Engineering

Khadije Akar[1], Mohammad Reza Kiani[2], Mahmood Sangari[3]

Received: January, 11, 2025; Revised: May, 5, 2025
Accepted: May, 10, 2025; Published: September, 1, 2025

Abstract

Purpose: The vast volume of data and information circulating in social networks, combined with their popularity and extensive use, exposes these platforms to numerous security risks. Consequently, user security and privacy have become among the most critical issues in in today's digital landscape. Many factors influence users' security and privacy behaviors on social networks. This study investigates the role of individual factors in shaping behaviors related to the security and privacy of social network users.

Methodology: This descriptive-survey research employed a researcher-designed questionnaire administered to a sample of 375 students at the University of Birjand . The questionnaire's validity was confirmed by expert judgment, and its reliability was verified using Cronbach's alpha coefficient ($\alpha = 0.876$).

Findings: The average levels of behaviors associated with the social engineering factors of authority and loneliness were within the optimal range. However, the mean score for the celebrity variable was significantly higher than the optimal level, while normalization and attention-grabbing events acored significantly below the desired level. In addition, , the average levels of behaviors related to the social engineering methods of phishing, forgery, and identity theft was significantly higher than the optimal level, whereas bait links, fake website offers, and online romance scams were within the acceptable range. Demographic analysis revealed that female students scored higher than male students across all variables, and undergraduate students showed higher acores than those at graduate levels .

Conclusion: The behaviors related to social engineering factors (such as celebrity influence, authority, loneliness, attention-grabbing events, and normalization) were generally at a desirable level among students. However, behaviors associated with social engineering methods (including bait links, fraudulent websites, online romance scams, phishing, and identity theft) exceeded the optimal level.

Value: Overall, participants engaged more frequently in behaviors related to social engineering methods than in those related to factors. Although students expressed a strong concern for security and privacy issues, they also acknowledged limited awareness of certain aspects of these topics.

Keywords: ***Social Engineering, Behavior, Security, Privacy, Social Networks***

How to Cite:

Akar, Kh., Kiani, M. R., & Sangari, M. (2025). Behaviors Related to Security and Privacy of Social Network Users: A Study of Threats Based on Social Engineering. *Journal of Knowledge-Research Studies*, 4 (2):132-145

Doi: 10.22034/jkrs.2025.19789

https://jkrs.tabrizu.ac.ir/article_19789_en.html

Article Type: Original Article

©The Author(s) **Publisher: University of Tabriz** **E-ISSN: 2821-045X**

[1] Master of Knowledge and Information Science, Faculty of Education and Psychology, University of Birjand, Birjand, Iran.

[2] Assistant Professor, Department of Knowledge and Information Science, Faculty of Education and Psychology, University of Birjand, Birjand, Iran.

[3] Assistant Professor, Department of Knowledge and Information Science, Faculty of Education and Psychology, University of Birjand, Birjand, Iran (Corresponding Author) msangari@birjand.ac.ir.

Extended Abstract

Introduction: Social engineering fundamentally involves the manipulation of human trust or the deception of individuals to gain access to confidential information, which is then misused for malicious purposes. In the context of social networks, Social engineering has emerged as one of the most significant and growing security concerns. attackers exploit vulnerabilities that arise from interpersonal relationships among users, , taking advantage of human tendencies such as curiosity, empathy, or trust.

Social engineering is considered one of the most common types of threats faced by social media users (Al-Bladi & Weir, 2020). It primarily relies on exploiting human trust or manipulating individuals to disclose sensitive information. Malicious actors and social engineers inflict substantial harm on modern societies by causing the loss of data, financial resources, and other valuable assets belonging to both individuals and organizations (Yasin et al., 2021). In this way, social engineering contributes directly to privacy violations and security breaches on social networks (Zolfahami, 2022).

Methodology: This descriptive survey employed a researcher- designed questionnaire administered to a sample of 375 students from the University of Birjand. Statistical analysis was conducted using both descriptive statistics (mean, standard deviation, tables, and graphs) and inferential statistics, including one-sample t-test, independent t-test, binomial t-test, one-way analysis of variance (ANOVA), and Kruskal-Wallis test. SPSS software was used for data analysis, and the normality of data distribution was confirmed using the Kolmogorov-Smirnov test. The validity of the questionnaire was confirmed through expert review, and its reliability was verified using Cronbach's alpha coefficient ($\alpha = 0.87$)

Findings: In today's world, celebrities play a highly influential role within society. Their popularity often leads to increased public trust, particularly among younger and middle-aged individuals who tend to view them as role models and are influenced by their behavior. However, given the sociocultural conditions in Iran and negative media coverage surrounding celebrities, the findings of this study indicated that, according to respondents, celebrities do not hold a significant role in their decision-making processes regarding security and privacy issues.

The results further revealed that the average level of social engineering behaviors related to security and privacy on social networks was significantly higher than the desirable level. Among these, phishing and identity theft showed notably higher averages. In contrast, the averages for bait links, fraudulent websites, and online romance scams were at the desirable level. Overall, the mean levels of behaviors associated with both social engineering factors and methods were generally within the acceptable or desirable range.

The findings indicated that the average level of social engineering behaviors related to security and privacy in social networks was significantly higher than the optimal level. Specifically, the averages for phishing, forgery, and identity theft were also notably above this level. In contrast, the averages for bait links, fraudulent websites, and online romance scams were within the desirable range. Overall, the mean rate of behaviors assiciated with social engineering factors and methods concerning security and privacy was generally at an acceptable level. Furthermore, the results suggest that students, despite forming emotional connections with various individuals -including those of the opposite sex- on social networks, have not shown

Journal of Knowledge-Research Studies

Journal of Knowledge-Research Studies (JKRS)

Vol 4

Issue 2

Serial Number 12

Journal of Knowledge-Research Studies (JKRS)

Vol 4

Issue 2

Serial Number 12

reduced sensitivity toward their own security. Instead, they have remained vigilant against potential exploitation by malicious actors.

The mean values of all variables –namely social engineering factors, social engineering methods, and overall social engineering – were slightly higher among the female participants compared to the male group. In other words, women demonstrated a higher average level of social engineering behaviors related to security and privacy.

To examine mean differences among participants categorized by education level, a one-way analysis of variance (ANOVA) was conducted. The results revealed that the means of the variables differed across the three educational groups (Bachelor's, Master's, and Doctorate). Further analysis of these differences showed that for the variables related to social engineering methods and overall social engineering , the differences were statistically significant, with the Bachelor's group showing the highest mean scores. However, for the variable of social engineering factors, the difference among the groups was not statistically significant.

The findings indicated that the overall level of engagement in behaviors related to social engineering factors associated with security and privacy in social networks was at a desirable level. Specifically, the mean scores for the variables of authority and loneliness were within the desirable range. However, the mean score for the celebrity variable was significantly higher than the desirable level, while the mean scores for the normalization and attention-seeking variables were significantly lower than the desirable level.

Table 1. Results of One-Sample t-Test for Variables Related to Social Engineering Factors

Variable	Mean	Standard Deviation	Desired Level	Mean Difference	T	DF	Significance Level
Social Engineering(overall)	19.74	3.172	20	0.259-	1.581-	373	0.115
Celebrities	3.70	1.037	4	0.302-	5.636-	374	0.0001
Authority	3.96	0.999	4	0.043-	0.827-	374	.409
Loneliness	4.07	1.164	4	0.072	1.197	374	0.0001
Normalization	3.77	1.033	4	0.232-	4.351-	374	0.0001
Events of Interest	4.26	0.953	4	0.256	5.204	374	0.0001

Conclusion: The findings revealed that the level of behaviors related to social engineering factors among students –such as those associated with celebrities, authority, loneliness, attention-grabbing events, and normalization- was generally at a desirable level. However, the level of behaviors related to social engineering methods, including bait links, fraudulent websites, online romance scams, phishing, and identity theft, was found to be above the desirable level.

In conclusion, it is recommended to organize training programs aimed at fully familiarizing users with the threats and risks present in social networks, as well as with effective strategies to counter them through practical behavioral measures. Moreover, it is important to consistently publicize, across all forms of media, real cases of individuals who have suffered significant harm within these spaces and the legal penalties imposed on those who violate privacy. Additionally, given that men

are generally more prone to risk-taking behaviors and tend to underestimate dangers, it is crucial to provide them with targeted education on security issues in social networks, emphasizing self-protection against such threats. Finally, a series of specialized training courses should be developed for undergraduate students -who largely belong to the 1980s generation- to enhance their understanding of various techniques and practices related to the virtual environment, with which they may be less familiar.

Value: Although students placed great importance on issues related to security and privacy, they acknowledged that their actual awareness and understanding of many of these topics were lower than expected.

Keywords: ***Social Engineering, Behavior, Security, Privacy, Social Networks***

Journal of Knowledge-Research Studies (JKRS)

Vol 4

Issue 2

Serial Number 12

References

Al Hasib, A. (2009). Threats of online social networks. *IJCSNS International Journal of Computer Science and Network Security*, *9*(11), 288-93.

Alabdulatif, A., Alturise, F. (2020). Awareness of data privacy on social networks by students at Qassim University. *International Journal of Advanced Computer Research*, *10*(50), 194. http://dx.doi.org/10.19101/IJACR.2020.1048094.

Albladi, S. M., & Weir, G. R. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, *8*(1), 1-24. https://doi.org/10.1186/s13673-018-0128-7.

Albladi, S. M., & Weir, G. R. (2020). Predicting individuals' vulnerability to social engineering in social networks. *Cybersecurity*, *3*(1), 1-19. https://doi.org/10.1186/s42400-020-00047-5.

Al-Omoush, K. S., Garrido, R., & Cañero, J. (2023). The impact of government use of social media and social media contradictions on trust in government and citizens' attitudes in times of crisis. *Journal of Business Research*, *159*, 113748. https://doi.org/10.1016/j.jbusres.2023.113748.

Badami, M. A. , Meghdadi, M. M. & Pilevar, M. (2022). Investigating the Impact of Cyberspace on the Abuse of the Right to Raise a Child with Emphasis on Religious Education. *Legal Research*, *21*(50), 457-494. doi: 10.48300/jlr.2021.279730.1619 [In Persian]

Bhattacharya, M., Roy, S., Chattopadhyay, S., Das, A. K., & Shetty, S. (2023). A comprehensive survey on online social networks security and privacy issues: Threats, machine learning- based solutions, and open challenges. *Security and Privacy*, *6*(1), e275. https://doi.org/10.1002/spy2.275.

Cárcamo-Ulloa, L., Cárdenas-Neira, C., Scheihing-García, E., Sáez-Trumper, D., Vernier, M., & Blaña-Romero, C. (2023). On Politics and Pandemic: How Do Chilean Media Talk about Disinformation and Fake News in Their Social Networks?. *Societies*, *13*(2), 25. https://doi.org/10.3390/soc13020025.

Chee, R. M., Capper, T. S., & Muurlink, O. T. (2023). The impact of social media influencers on pregnancy, birth, and early parenting experiences: A systematic review. *Midwifery*, *120*, 103623. https://doi.org/10.1016/j.midw.2023.103623.

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical practice and epidemiology in mental health: CP & EMH*, *16*, 24-35. https://doi.org/10.2174%2F1745017902016010024.

Cross, C., & Layt, R. (2022). "I suspect that the pictures are stolen": Romance fraud, identity crime, and responding to suspicions of inauthentic identities. *Social Science Computer Review*, *40*(4), 955-973. https://doi.org/10.1177/0894439321999311.

Ehsanifar, M., & Rezvanian, M. (2016). The role of users' behavior in feeling the security of social networks. Annual Research Conference in Humanities and Social Studies, Tehran. [In Persian]

Eslami, E., Mousavi, S. H., & Alikhah, F. (2019). virtual celebrities; Familiar strangers in the age of social media. *Cultural Studies and Communication, 16*(59), 45-74. https://doi.org/10.22034/jcsc.2019.35296 [In Persian]

Fadhil, H. S. (2023). Social Engineering Attacks Techniques. *Int. J. Progress. Res. Eng. Manag. Sci. International Journal Of Engineering And Computer ScienceIJPREMS,3*(1) , 18-20. DOI:10.18535/ijecs/v6i1.09

Fatemi Nia, M. A., Heydari, M, ., & Tabankhet, H. (1400). Social penetration coefficient of celebrities and social factors affecting it in Rasht city. *Communication Research, 28*(108), 39-67. [In Persian]

Gee, D. (2016). *Rethinking Security: A discussion paper.* Ammerdown Group.

Gu, X., Chen, F., Yang, X., Chen, H., Wang, Y., Hou, J., ... & Wang, Y. (2023). Evolutionary trend and network structure characteristics of publicity information dissemination about waste separation by different opinion leaders. *Resources, Conservation and Recycling*, *194*, 106991. https://doi.org/10.1016/j.resconrec.2023.106991

Hood, M., Creed, P. A., & Mills, B. J. (2018). Loneliness and online friendships in emerging adults. *Personality and Individual Differences*, *133*, 96-102. https://doi.org/10.1016/j.paid.2017.03.045

Hossein Pour, J., & Mesrkhani, Q. (2017). The role of virtual social networks on the public security of its users. *Police order and security, 11* (2), 659-611. [In Persian]

Hosseini Senu, S. A., & Mazaheri, E. (2017). The effect of privacy, security and perceived trust on information sharing behavior in mobile social networks: the moderating role of gender. *Journal of Information Processing and Management, 93*(6), 235-213. doi: 10.35050/JIPM010.2018.009 [In Persian]

Hu, X., Hu, D., Zheng, S., Li, W., Chen, F., Shu, Z., & Wang, L. (2018). How people share digital images in social networks: a questionnaire-based study of privacy decisions and access control. *Multimedia Tools and Applications*, *77*(14), 18163-18185. https://doi.org/10.1007/s11042-017-4402-x.

Jafarpour Hadi Kiashari, R., Kabuli, M.H., & Shahcheraghi, A. (2022). Analyzing the effect of objective and subjective elements on the sense of "privacy" in the architectural space. *Eastern Art and Civilization, 10*(38), 17-28. doi: 10.22034/jaco.2022.364304.1264 [In Persian]

Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. *Complex & Intelligent Systems*, *7*(5), 2157-2177. https://doi.org/10.1007/s40747-021-00409-7.

Jalali, Z. , Kianpour, M. & Aqababaei, E. (2017). sociological study of factors influencing attitude towards personal privacy in social networks (the case of young Facebook users in Isfahan). *Strategic Research on Social Problems*, *6*(1), 17-28. doi: 10.22108/ssoss.2017.21281 [In Persian]

Kanampiu, M. (2018). *A Study of Security and Privacy in Online Social Networks Using Social Network Analysis and Human Factors Perspectives* (Doctoral dissertation, North Carolina Agricultural and Technical State University).

Kemp, S., & Erades Pérez, N. (2023). Consumer Fraud against Older Adults in Digital Society: Examining Victimization and Its Impact. *Environmental Research and Public Health*, *20*(7), 5404. https://doi.org/10.3390/ijerph20075404

López, C., Hartmann, P., & Apaolaza, V. (2019). Gratifications on social networking sites: The role of secondary school students' individual differences in loneliness. *Educational Computing Research*, *57*(1), 58-82. https://doi.org/10.1177/0735633117743917

Mittal, N. (2023). User Perceptions of Privacy and Security in Online Social Networks. *Innovative Science and Research Technology,1*(8), 91-94. DOI **:** https://doi.org/10.5281/zenodo.7547576

Nawaz, N. A., Ishaq, K., Farooq, U., Khalil, A., Rasheed, S., Abid, A., & Rosdi, F. (2023). A comprehensive review of security threats and solutions for the online social networks industry. *PeerJ Computer Science*, *9*, e1143. DOI:10.7717/peerj-cs.1143

Okokpujie, K., Kennedy, C. G., Nnodu, K., & Noma-Osaghae, E. (2023). Cybersecurity Awareness: Investigating Students' Susceptibility to Phishing Attacks for Sustainable Safe Email Usage in Academic Environment (A Case Study of a Nigerian Leading University). *Sustainable Development & Planning*, *18*(1), 255-263. https://doi.org/10.18280/ijsdp.180127

Paki, Z. S., Sani, S., & Diri, G. I. (2022). Connection to the use of free Android apps in Kebbi State, Nigeria. *Social Sciences*, *5*(3), 144-154. https://doi.org/10.52326/jss.utm.2022.5(3).11.

Pour Naqdi, B. (2017). Security opportunities and threats in virtual social networks for students. *Strategic Researches of Iran's Social Issues*, *1*(2), 37-71. doi: 10.22108/ssoss.2018.103434.1062 [In Persian]

Rahmatizadeh, A .,Karimzadegan Moghadam, D., & Vahdat, D. (1400). Reliability and the difference between the moral behavior of honesty in speech and the inner intention of people in social networks. *Ethics in Science and Technology*, *16*(3), 97-104. dor: 20.1001.1.22517634.1400.16.3.13.0 [In Persian]

Rehman, S. U., Manickam, S., & Al-Charchafchi, A. (2023). Privacy calculus model for online social networks: a study of Facebook users in a Malaysian university. *Education and Information Technologies*, *28*(6), 7205-7223. DOI:10.1007/s10639-022-11459-w

Rhodes, S. C. (2022). Filter bubbles, echo chambers, and fake news: How social media conditions individuals to be less critical of political misinformation. *Political Communication*, *39*(1), 1-22. https://doi.org/10.1080/10584609.2021.1910887.

Rochlitz, M., Schoors, K. J., & Zakharov, N. (*2023, April 29*). *Can Authoritarian Propaganda Compete with the Opposition on Social Media?* Experimental Evidence from Russia. Experimental Evidence from Russia. http://dx.doi.org/10.2139/ssrn.4433145.

Sart, G., & Sezgin, F. H. (2022, November 7-9). The effect of internet addiction on social and emotional loneliness in university students. In *ICERI2022 Proceedings* (pp. 6420-6426). IATED. https://doi.org/10.21125/iceri.2022.1599**.**

Steiert, D. (2019). *Privacy preservation in mobile social networks* (Doctoral dissertation, University of Missouri--Columbia).

Van der Schyff, K., & Flowerday, S. (2021). Mediating effects of information security awareness. *Computers & Security*, *106*, 102313. https://doi.org/10.1016/j.cose.2021.102313.

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283-297. https://doi.org/10.1016/j.chb.2017.10.007.

Wang, Q. (2020). *Towards the Understanding of Private Content–Content-based Privacy Assessment and Protection in Social Networks* (Doctoral dissertation, University of Kansas).

White, G., & Leontyeva, A. (2023). Tweet Your Heart Out: The personality correlates and affective consequences of social media use on close relationships and psychological health. *Mental Health and Social Behaviour*, *5*(1), 75, 177. https://doi.org/10.33790/jmhsb1100177.

Yasin, A., Fatima, R., Liu, L., Wang, J., Ali, R., & Wei, Z. (2021). Understanding and deciphering of social engineering attack scenarios. *Security and Privacy*, *4*(4), e161. https://doi.org/10.1002/spy2.161.

Ye, S., Ho, K. K., & Zerbe, A. (2021). The effects of social media usage on loneliness and well-being: analysing friendship connections of Facebook, Twitter and Instagram. *Information Discovery and Delivery*, *49*(2), 136-150. https://doi.org/10.1108/IDD-08-2020-0091.

Journal of Knowledge-Research Studies

Journal of Knowledge-Research Studies (JKRS)

Vol 4

Issue 2

Serial Number 12

Yi, Y., Zhu, N., He, J., Jurcut, A. D., Ma, X., & Luo, Y. (2023). A privacy-dependent condition-based privacy-preserving information sharing scheme in online social networks. *Computer Communications*, *200*, 149-160. https://doi.org/10.1016/j.comcom.2023.01.010.

Yoro, R. E., Aghware, F. O., Akazue, M. I., Ibor, A. E., & Ojugo, A. A. (2023). Evidence of personality traits on phishing attack menace among selected university undergraduates in Nigerian. *Electrical and Computer Engineering (IJECE)*, *13*(2), 1943-1953. https://doi.org/10.11591/ijece.v13i2.pp1943-1953

Yoro, R. E., Aghware, F. O., Malasowe, B. O., Nwankwo, O., & Ojugo, A. A. (2023). Assessing contributor features to phishing susceptibility amongst students of petroleum resources varsity in Nigeria. *Electrical and Computer Engineering (IJECE)*, *13*(2), 1922-1931. https://doi.org/10.1177/0894439321999311.

Zhang, Z., Jing, J., Wang, X., Choo, K. K. R., & Gupta, B. B. (2020). A crowdsourcing method for online social networks security assessment based on human-centric computing. *Human-centric Computing and Information Sciences*, *10*(1), 23. https://doi.org/10.1186/s13673-020-00230-0.

Zulfahmi, M., Elsandi, A., Apriliansyah, A., Anggreainy, M. S., Iskandar, K., & Karim, S. (2023). Privacy protection strategies on social media. *Procedia Computer Science*, *216*, 471-478. https://doi.org/10.1016/j.procs.2022.12.159

Journal of Knowledge-Research Studies (JKRS)

Vol 4

Issue 2

Serial Number 12