

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

Khadije Akar¹, Mohammad Reza Kiani², Mahmood Sangari³

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 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 scored 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 scores 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://doi.org/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](#)

The paper is an open access and licensed under the Creative Commons CC BY NC license.



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).



Journal of
Knowledge-Research
Studies (JKRS)

Vol 4

Issue 2

Serial Number 12

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 associated 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

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*

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>.



**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

- 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 ScienceIJPREAMS*,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/ijstdp.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](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. doi: 10.1001.1.22517634.1400.16.3.13.0 [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 (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



رفتارهای مرتبط با امنیت و حریم خصوصی کاربران شبکه‌های اجتماعی: بررسی تهدیدات

مبثنی بر مهندسی اجتماعی

خدیدجه آکار^۱، محمدرضا کیانی^۲، محمود سنگری^۳*

۱. کارشناس ارشد، علم اطلاعات و دانش‌شناسی، دانشکده علوم تربیتی و روانشناسی، دانشگاه بیرجند، بیرجند، ایران.

۲. استادیار، گروه علم اطلاعات و دانش‌شناسی، دانشکده علوم تربیتی و روانشناسی، دانشگاه بیرجند، بیرجند، ایران.

۳. استادیار، گروه علم اطلاعات و دانش‌شناسی، دانشکده علوم تربیتی و روانشناسی، دانشگاه بیرجند، بیرجند، ایران (نویسنده مسئول) msangari@birjand.ac.ir

تاریخ بازنگری: ۱۵ اردیبهشت ۱۴۰۴

تاریخ دریافت: ۲۲ دی ۱۴۰۳

تاریخ انتشار: ۱۰ شهریور ۱۴۰۴

تاریخ پذیرش: ۲۰ اردیبهشت ۱۴۰۴

چکیده

هدف: حجم عظیم داده‌ها و اطلاعات در حال گردش در شبکه‌های اجتماعی در کنار محبوبیت و گستردگی استفاده از آن‌ها، این شبکه‌ها را در معرض خطرات امنیتی متعددی قرار می‌دهد. بنابراین امروزه امنیت و حریم خصوصی کاربران به یکی از مهم‌ترین مسائل در شبکه‌های اجتماعی تبدیل شده است. عوامل زیادی بر روی امنیت و حریم خصوصی کاربران در شبکه‌های اجتماعی اثرگذارند که این پژوهش از آن میان، به بررسی نقش عوامل مهندسی اجتماعی در رفتارهای مرتبط با امنیت و حریم خصوصی کاربران در شبکه‌های اجتماعی پرداخته است.

روش‌شناسی: روش این پژوهش کاربردی، توصیفی (از نوع پیمایشی) بود. گردآوری داده‌ها با استفاده از پرسش‌نامه محقق ساخته و در نمونه‌ای به حجم ۳۷۵ نفر از جامعه دانشجویان کارشناسی و کارشناسی ارشد و دکتری دانشگاه بیرجند و به روش نمونه‌گیری تصادفی طبقه‌بندی نسبتی انجام شد. روایی پرسش‌نامه با تأیید متخصصان موضوعی و اساتید حاصل و برای آزمون پایایی از آزمون آلفای کرونباخ (۰/۸۷۶) استفاده شد.

یافته‌ها: میانگین میزان انجام رفتارهای مربوط به عوامل مهندسی اجتماعی اقتدار و تنهایی در حد مطلوب اما میانگین متغیر سلبی به‌طور معناداری بیشتر از حد مطلوب و میانگین متغیرهای عادی‌انگاری و وقایع موردتوجه به‌طور معناداری کمتر از حد مطلوب بود. همچنین میانگین میزان انجام رفتارهای مربوط به روش‌های مهندسی اجتماعی فیه‌شنگ و جعل و سرقت هویت به‌طور معناداری بیشتر از حد مطلوب بود؛ اما میانگین متغیرهای لینک طعمه، ارائه وب‌سایت‌های تقلبی و کلاه‌برداری‌های عاشقانه آنلاین در حد مطلوب بود. علاوه بر این بررسی متغیرهای جمعیت شناختی نشان داد که در همه متغیرهای موردبررسی بانوان نمره بالاتری از آقایان دریافت کردند. همچنین نمره دانشجویان کارشناسی از دو مقطع بالاتر از خودشان، در همه متغیرها بیشتر بود.

نتایج: نمونه انتخاب‌شده این پژوهش رفتارهای مربوط به روش‌های مهندسی اجتماعی مرتبط با امنیت و حریم خصوصی را بیشتر از رفتارهای مربوط به عوامل مهندسی اجتماعی در شبکه‌های اجتماعی انجام می‌دادند؛ اما به‌طور کلی میزان انجام رفتارهای مرتبط با مهندسی اجتماعی مربوط به امنیت و حریم خصوصی در حد مطلوب بود.

اصالت و ارزش: این پژوهش با رویکردی نوآورانه، برای نخستین بار نقش عوامل مهندسی اجتماعی را در شکل‌گیری رفتارهای امنیتی و حریم خصوصی کاربران شبکه‌های اجتماعی بررسی کرده است. تمرکز بر ابعاد روان‌شناختی و رفتاری کاربران، این مطالعه را از تحقیقات فنی پیشین متمایز می‌سازد. نتایج آن می‌تواند مبنایی کاربردی برای طراحی آموزش‌ها و سیاست‌های ارتقای سواد امنیتی در میان دانشجویان و کاربران شبکه‌های اجتماعی فراهم آورد.

کلیدواژه‌ها: مهندسی اجتماعی، رفتار، امنیت، حریم خصوصی، شبکه‌های اجتماعی.

چگونه به این مقاله استناد کنیم؟

آکار، خدیدجه؛ کیانی، محمدرضا؛ سنگری، محمود (۱۴۰۴). رفتارهای مرتبط با امنیت و حریم خصوصی کاربران شبکه‌های

اجتماعی: بررسی تهدیدات مبثنی بر مهندسی اجتماعی. نشریه مطالعات دانش پژوهی، ۴ (۲): ۱۴۵-۱۳۲

Doi: [10.22034/jkrs.2025.19789](https://doi.org/10.22034/jkrs.2025.19789)

URL: https://jkrs.tabrizu.ac.ir/article_19789.html

نوع مقاله: مقاله پژوهشی

ناشر: دانشگاه تبریز

شاپا الکترونیکی: 2821-045X

© نویسندگان



این مقاله به صورت دسترسی باز و با لایسنس CC BY NC کرییتیو کامنز قابل استفاده است.

شبکه‌های اجتماعی آنلاین، رسانه‌های جدید و نوینی هستند که در ساختارهای اجتماعی، فرهنگی، اقتصادی و سیاسی جوامع تغییراتی ایجاد کرده‌اند. این شبکه‌ها نه تنها قواعد و قوانین حاکم بر ارتباط و تعامل میان انسان‌ها، بلکه تفکر و نگرش ما را نسبت به خود، دیگران و جهان تغییر داده‌اند. با رشد سریع فناوری، شبکه‌های اجتماعی آنلاین در دهه جاری محبوبیت زیادی پیدا کرده‌اند (جین و همکاران^۱، ۲۰۲۱). شبکه‌های اجتماعی این امکان را به فرد می‌دهد تا با طیف وسیعی از افراد در ارتباط باشند و علایق خود را در همه زمینه‌ها با آن‌ها به اشتراک بگذارد (کانامپیو^۲، ۲۰۱۸). درحالی که کاربران می‌توانند با استفاده از خدمات از مزایای بسیاری برخوردار شوند، درعین حال با افزایش استفاده از شبکه‌های اجتماعی نگرانی‌های زیادی در مورد امنیت و حفظ حریم خصوصی اطلاعات خود دارند (رحمان و همکاران^۳، ۲۰۲۲؛ میتال^۴، ۲۰۲۳؛ نواز و همکاران^۵، ۲۰۲۳). تا به امروز، شبکه‌های اجتماعی آنلاین، مانند فیس‌بوک، توییتر، و سایر شبکه‌های اجتماعی، به‌طور قابل توجهی مورد حمله قرار گرفته و پیامدهای قابل توجهی داشته است. در پی رسوایی نقض اطلاعات فیس‌بوک، کاربران متوجه شدند که داده‌های شخصی آن‌ها چقدر آسیب‌پذیر است و چقدر کورکورانه به شبکه‌های اجتماعی آنلاین اعتماد می‌کنند (وانگ^۶، ۲۰۲۰). بر اساس چنین رویدادهایی می‌توان گفت شبکه‌های اجتماعی بهترین ابزار برای مهاجمان مخرب برای ارتکاب جرائم سایبری هستند و امنیت^۷ و حریم خصوصی^۸ یکی از مهم‌ترین مسائل در شبکه‌های اجتماعی آنلاین است که مورد توجه نهادهای امنیتی قرار گرفته است (نواز و همکاران، ۲۰۲۳). از ابتدای زندگی بشر، امنیت یکی از دغدغه‌های اصلی انسان‌ها بوده است به‌طوری که با نابودی آن آرامش خاطر انسان از بین می‌رود و تشویش، اضطراب و ناآرامی جای آن را می‌گیرد (حسین پور و مصرخانی، ۱۳۹۷). امنیت با الهام از ریشه لاتین کلمه «se + cura»، به معنای عاری از ترس یا اضطراب است (گی^۹، ۲۰۱۶) و از اینکه اطلاعات کاربر در دسترس افراد غیرمجاز و سوء استفاده آنان قرار بگیرد محافظت می‌کند. از طرفی دیگر حریم خصوصی را به‌عنوان محافظت از اطلاعات شخصی در برابر سوء استفاده توسط دیگران و تنها اجازه دادن به برخی از نهادهای مجاز برای دسترسی به اطلاعات شخصی می‌دانند. برخی حریم خصوصی را به‌عنوان مجموعه‌ای از سیاست‌ها توصیف می‌کند که سیستم‌ها را مجبور می‌کند از

۱. Jain & et al.

۲. Kanampiu

۳. Rehman & et al.

۴. Mittal

۵. Nawaz & et al.

۶. Wang

۷. Security

۸. Privacy

۹. Gee





اطلاعات خصوصی محافظت کنند (البدلطیف و آلتوریس^۱، ۲۰۲۰). حال برای مقابله با این تهدیدات باید دانست که چه عواملی بر روی امنیت و حریم خصوصی در شبکه‌های اجتماعی تأثیر می‌گذارد. طبق پژوهش‌های متعددی (یاسین و همکاران^۲، ۲۰۲۱؛ کانامپو، ۲۰۱۸) که در این حوزه انجام شده است عوامل زیادی (از جمله عوامل انسانی، فردی، معنوی، اجتماعی، مادی، رفتارهای مهندسی اجتماعی^۳ و ...) تأثیر گذارند؛ اما عامل مهمی که پژوهش حاضر بر روی آن تمرکز دارد عامل رفتارهای مهندسی اجتماعی است و شامل عوامل (سلبریتی‌ها^۴، اقتدار^۵، تنهایی^۶، عادی‌انگاری^۷ و وقایع، رویدادها و پیام‌های مورد توجه عموم مردم) و روش‌ها (لینک طعمه، ارائه وب‌سایت‌های تقلبی، کلاه‌برداری عاشقانه آنلاین، فیشینگ^۸، جعل هویت^۹ و سرقت هویت^{۱۰}) می‌شود. مهندسی اجتماعی یکی از رایج‌ترین انواع تهدیداتی است که ممکن است کاربران شبکه‌های اجتماعی با آن مواجه شوند (البلادی و ویر^{۱۱}، ۲۰۲۰) و در واقع سوء استفاده از اطمینان و یا فریب عوامل انسانی به جهت دسترسی به اطلاعات محرمانه و در مرحله بعد سوء استفاده از این اطلاعات است. کلاه‌برداران مخرب و مهندسان اجتماعی آسیب‌های زیادی را به جامعه مدرن وارد می‌کنند، زیرا منجر به ازدست‌رفتن داده‌ها، اطلاعات، پول و بسیاری موارد دیگر برای افراد و شرکت‌ها شده است (یاسین و همکاران، ۲۰۲۱) و به عبارتی منجر به نقض حریم خصوصی کاربران در شبکه‌های اجتماعی می‌شود (ذوالفهمی^{۱۲}، ۲۰۲۲). یک مهاجم مهندسی اجتماعی در شبکه‌های اجتماعی از آسیب‌پذیری‌های روابط بین فردی بین کاربران سوء استفاده می‌کند. از جمله آسیب‌پذیری‌ها می‌توان به توسل به غرور، جلب توجه به سلبریتی، توسل به اقتدار و توسل به طمع و جعل هویت اشاره کرد (کانامپو، ۲۰۱۸). سستی در تنظیمات حریم خصوصی یکی از این آسیب‌پذیری‌ها است (البلادی و ویر، ۲۰۲۰). برای مقابله با این تهدیدات نیاز به شناسایی تکنیک‌هایی است که افراد با به‌کاربردن آن‌ها در مقابل این تهدیدات ایمن شوند. بیشتر کارهای تحقیقاتی عمدتاً بر شناسایی تکنیک‌هایی متمرکز شده‌اند که مهندسان اجتماعی برای انجام حملات خود از آن‌ها استفاده می‌کنند. از جمله این تکنیک‌ها آموزش کاربران آنلاین در مورد

۱. Alabdulatif & Alturise

۲. Yasin & et al.

۳. social engineering

۴. Celebrities

۵. Authority

۶. Loneliness

۷. Normalization

۸. Phishing

۹. impersonation

۱۰. identity theft

۱۱. Albladi & Weir

۱۲. Zulfahmi & et al.



انواع حملات مهندسی اجتماعی و آموزش به آنها برای کنترل توزیع اطلاعات شخصی حساس و هویت دیجیتال خود است (یاسین و همکاران، ۲۰۲۱).

بر اساس آنچه ذکر شد، اهمیت روزافزون شبکه‌های اجتماعی مورد تأکید همه محققان است و رفتارهای مرتبط با امنیت و حریم خصوصی در این بستر در حال گسترش از اهمیت ویژه‌ای برخوردار است و در این میان بیشترین تأکید مطالعات بر روی عامل مهندسی اجتماعی بوده است؛ لذا در این پژوهش به مطالعه این موارد پرداخته شده است و به دنبال آن بوده تا دریابد که آیا کاربران عامل‌های مهندسی اجتماعی را در رفتارهای خود انجام داده‌اند؟ علاوه بر این آیا کاربران روش‌های مهندسی اجتماعی را در رفتارهای خود انجام داده‌اند؟ و در نهایت نقش متغیرهای جمعیت شناختی در این رابطه چقدر بوده است؟

۲- روش‌شناسی پژوهش

این پژوهش کاربردی و توصیفی در نمونه‌ای به حجم ۳۷۵ نفر از جامعه دانشجویان دانشگاه بیرجند به روش نمونه‌گیری تصادفی طبقه‌بندی نسبتی انجام شد. جامعه مورد مطالعه دانشجویان دانشگاه بیرجند (۱۰۵۳۴ نفر) بودند. ۱۸۳ نفر از شرکت‌کنندگان زن و ۱۹۲ نفر مرد بودند. ۲۳۷ دانشجو در مقطع کارشناسی، ۱۱۰ دانشجو در مقطع کارشناسی ارشد و ۲۸ دانشجو در مقطع دکتری مشغول به تحصیل بودند. لازم به توضیح است طبقات نمونه بر اساس مقطع تحصیلی محاسبه شد. داده‌های پژوهش با استفاده از پرسش‌نامه محقق ساخته گردآوری شد. پرسش‌نامه شامل ۱۰ گویه است و از طیف لیکرت در آن استفاده شد (از ۱ به معنای کاملاً مخالفم تا ۵ به معنای کاملاً موافقم نمره‌گذاری شد). پرسش‌نامه از دو بخش تشکیل شده بود که مبنای آن برآوردن هدف‌ها و پاسخ به سؤالات پژوهش است. بخش اول در مورد عوامل مهندسی اجتماعی و بخش دوم در مورد روش‌های مهندسی اجتماعی بود.

تجزیه و تحلیل داده‌های آماری این پژوهش با استفاده از روش‌های آمار توصیفی (میانگین، انحراف معیار، جداول و نمودارها) و آمار استنباطی (شامل آزمون‌های تی تک نمونه، تی مستقل، دوجمله‌ای، تحلیل واریانس یک طرفه و کروسکال والیس) صورت گرفت. نرم‌افزار مورد استفاده برای تحلیل‌های آماری، اس‌پی‌اس‌اس بود. ضمناً نرمال بودن توزیع داده‌ها با استفاده از آزمون کولموگروف-اسمیرنوف مورد تأیید قرار گرفت.

۳- یافته‌ها

سؤال اول: میزان انجام رفتارهای مرتبط با عوامل مهندسی اجتماعی مربوط به امنیت و حریم خصوصی در شبکه‌های اجتماعی توسط کاربران چقدر است؟

یافته‌ها نشان داد که میانگین میزان انجام رفتارهای مربوط به عوامل مهندسی اجتماعی مرتبط با امنیت و حریم خصوصی در شبکه‌های اجتماعی در حد مطلوب بود. میانگین متغیرهای اقتدار و

تنهایی در حد مطلوب؛ اما میانگین متغیر سلبیتی به طور معناداری بیشتر از حد مطلوب و میانگین متغیرهای عادی انگاری و وقایع مورد توجه به طور معناداری کمتر از حد مطلوب بود.

جدول ۱. نتایج آزمون مقایسه میانگین میزان انجام عوامل مهندسی اجتماعی مربوط به امنیت و حریم

خصوصی در شبکه‌های اجتماعی

متغیر	میانگین	انحراف معیار	حد مطلوب	تفاوت میانگین	T	Df	سطح معناداری
عوامل مهندسی اجتماعی	۱۹/۷۴	۳/۱۷۲	۲۰	-۰/۲۵۹	-۱/۵۸۱	۳۷۳	۰/۱۱۵
سلبیتی	۳/۷۰	۱/۰۳۷	۴	-۰/۳۰۲	-۵/۶۳۶	۳۷۴	۰/۰۰۰۱
اقتدار	۳/۹۶	۰/۹۹۹	۴	-۰/۰۴۳	-۰/۸۲۷	۳۷۴	۰/۴۰۹
تنهایی	۴/۰۷	۱/۱۶۴	۴	۰/۰۷۲	۱/۱۹۷	۳۷۴	۰/۲۳۲
عادی انگاری	۳/۷۷	۱/۰۳۳	۴	-۰/۲۳۲	-۴/۳۵۱	۳۷۴	۰/۰۰۰۱
وقایع مورد توجه	۴/۲۶	۰/۹۵۳	۴	۰/۲۵۶	۵/۲۰۴	۳۷۴	۰/۰۰۰۱



نشریه مطالعات دانش پژوهی

صفحه ۱۳۶ |

دوره ۴، شماره ۲

پیاپی ۱۲

اولین عامل از عوامل مهندسی اجتماعی متغیر سلبیتی بود. طبق پژوهش‌های فاطمی نیا و همکاران (۱۴۰۰)؛ گو و همکاران^۱ (۲۰۲۳)؛ اسلامی و همکاران (۱۳۹۹)؛ چه و همکاران^۲ (۲۰۲۳) باتوجه به دنیای امروزه که سلبیتی‌ها نقش بسیار پررنگی در میان مردم یک جامعه دارند و از آنجایی که از محبوبیت خاصی در میان مردم برخوردارند، طبیعتاً اعتماد افراد به آن‌ها چندین برابر می‌شود و بسیاری از جوانان و حتی قشر میان‌سال، آن‌ها را الگوی زندگی خود قرار می‌دهند و تأثیر گذارند. لیکن با توجه به شرایط جامعه ایران و تبلیغات منفی رسانه‌ای در مورد سلبیتی‌ها نتایج نشان داد که بر اساس اظهارات پاسخگویان، این افراد چندان جایگاهی در تصمیم‌گیری‌های مرتبط با امنیت و حریم خصوصی پاسخگویان این مطالعه نداشته‌اند.

عامل بعدی که به آن اشاره می‌کنیم عامل تنهایی است. پژوهش‌های زیادی به و همکاران^۳ (۲۰۲۱)، لویز و همکاران^۴ (۲۰۱۹)، هود و همکاران^۵ (۲۰۱۸)، وایت و لئونتیوا^۶ (۲۰۲۳)، سارت و سزگین^۷ (۲۰۲۲) به نتایجی مشابه با نتایج این پژوهش دست یافته‌اند. طبق نتایج پژوهش‌های ذکر شده، با توجه به پیشرفت روزافزون فناوری و استفاده زیاد کاربران از شبکه‌های اجتماعی و تغییر سبک زندگی افراد و سوق پیدا کردن خانواده‌ها به تک‌فرزندگی به جای چند فرزندگی، ارتباطات مجازی پررنگ‌تر از ارتباطات حضوری شده و افراد برای پر کردن این خلأ و تنهایی،

1 . Gu & et al.

2 . Chee & et al.

3 . Ye & et al.

4 . López & et al.

5 . Hood & et al.

6 . White & Leontyeva

7 . Sart & Sezgin



بیشتر وقت خود را با شبکه‌های اجتماعی گذرانده و دوستان مجازی زیادی رو جایگزین دوستان حقیقی کرده‌اند.

اقتدار عامل دیگری بود که در این پژوهش به آن پرداخته شد. طبق پژوهش‌های صورت گرفته اولوآ^۱ (۲۰۲۳)، روچلیتز و همکاران^۲ (۲۰۲۳)، رودز^۳ (۲۰۲۱)، آل اوموش و همکاران^۴ (۲۰۲۳) دانشجویانی که پیام‌های منابع و مراجع شناخته‌شده مانند نهادهای دولتی را بدون بررسی دقیق می‌پذیرند محدود است. همچنان که پژوهش روچلیتز و همکاران نشان داد این نوع تبلیغات بر روی مصرف‌کنندگان اطلاعات آنلاین تأثیر چندانی ندارد. عامل مرتبط با مهندسی اجتماعی بعدی در مورد وقایع مورد توجه است. متأسفانه در این مورد پژوهش مرتبطی یافت نشد و نتایج پژوهش حاضر می‌تواند به‌نوعی ورود به این مقوله تلقی شود.

و اما عامل بعدی دیگر، عادی انگاری است. تنها پژوهش در این زمینه مطالعه واندر اسپچیف و فلووردی^۵ (۲۰۲۱) است. آن‌ها معتقدند که آگاهی از امنیت اطلاعات به‌عنوان یک واسطه غیرمستقیم بین باز بودن و قصد بررسی تنظیمات حریم خصوصی عمل می‌کند. این نشان می‌دهد که با افزایش باز بودن کاربران نسبت به تهدیدات مربوط به حریم خصوصی (از طریق اخبار و رویدادهای حریم خصوصی)، قصد آن‌ها برای بررسی تنظیمات حریم خصوصی افزایش می‌یابد. همان‌طور که مشاهده شد نتیجه پژوهش ذکر شده با نتیجه پژوهش حاضر همسواست و استفاده زیاد دانشجویان از شبکه‌های اجتماعی باعث نشده که دقت آن‌ها نسبت به مسائل امنیتی کم شود بلکه برعکس هرچه بیشتر به شبکه‌های اجتماعی خود مراجعه می‌کنند دقت آن‌ها نسبت به مسائل امنیتی بالاتر می‌رود.

سؤال دوم: میزان انجام رفتارهای مرتبط با روش‌های مهندسی اجتماعی مربوط به امنیت و حریم خصوصی در شبکه‌های اجتماعی توسط کاربران چقدر است؟
یافته‌ها نشان داد که میانگین میزان انجام رفتارهای مربوط به روش‌های مهندسی اجتماعی مرتبط با امنیت و حریم خصوصی در شبکه‌های اجتماعی به‌طور معناداری بیشتر از حد مطلوب و میانگین متغیرهای فیشینگ و جعل و سرقت هویت به‌طور معناداری بیشتر از حد مطلوب بود؛ اما میانگین متغیرهای لینک طعمه، ارائه وب‌سایت‌های تقلبی و کلاه‌برداری‌های عاشقانه آنلاین در حد مطلوب بود و در نهایت میانگین میزان انجام رفتارهای مرتبط با عوامل و روش‌های مهندسی اجتماعی مربوط به امنیت و حریم خصوصی به‌طور کلی در حد مطلوب بود.

1 . Ulloa & et al.

2 . Rochlitz

3 . Rhodes

4 . Al-Omoush

5 . Van der Schyff & Flowerday

جدول ۲. نتایج آزمون مقایسه میانگین میزان انجام روش‌های مهندسی اجتماعی مربوط به امنیت و حریم خصوصی در شبکه‌های اجتماعی

متغیر	میانگین	انحراف معیار	حد مطلوب	تفاوت میانگین	T	Df	سطح معناداری
روش‌های مهندسی اجتماعی	۲۰/۷۷	۳/۹۱۸	۲۰	۰/۷۷۰	۳/۸۰۱	۳۷۳	۰/۰۰۰۱
لینک طعمه	۴/۰۳	۱/۱۰۶	۴	۰/۰۳۲	۰/۵۶۰	۳۷۴	۰/۵۷۶
ارائه وبسایت‌های تقلبی	۴/۱۲	۱/۰۷۶	۴	۰/۱۲۰	۲/۱۶۳	۳۷۳	۰/۰۳۱
کلاهبرداری‌های عاشقانه آنلاین	۴/۱۱	۱/۰۰۲	۴	۰/۱۱۲	۲/۱۶۵	۳۷۴	۰/۰۳۱
فیشینگ	۴/۱۸	۱/۰۰۵	۴	۰/۱۸۱	۳/۴۹۴	۳۷۴	۰/۰۰۰۱
جعل و سرقت هویت	۴/۳۲	۰/۹۷۶	۴	۰/۳۲۳	۶/۴۰۵	۳۷۴	۰/۰۰۰۱
مهندسی اجتماعی (عوامل و روش‌ها)	۴۰/۵۰	۶/۲۲۳	۴۰	۰/۵۰۹	۱/۵۸۱	۳۷۲	۰/۱۱۵



اولین روشی که به آن اشاره کردیم ارائه وبسایت‌های تقلبی بود. جین و همکاران (۲۰۲۱) معتقدند کاربران باید هنگام ارسال هرگونه رسانه یا اطلاعات در سایت‌های شبکه‌های اجتماعی هوشیار باشند. هنگام بازدید از یک وبسایت باید یو آر ال را بررسی کنید. این عادات می‌تواند تا حدی به کاربر کمک کند تا در برابر حملات سایبری مختلف در رسانه‌های اجتماعی محافظت شود. آنچه از تحلیل این پژوهش استنباط می‌شود این بود که دانشجویان به‌عنوان قشر آگاه جامعه تا حد مطلوبی طعمه وبسایت‌های تقلبی نشده‌اند.

تنها پژوهش ناهم‌سو با پژوهش حاضر، متعلق به ذوالفهمی و همکاران (۲۰۲۳) بود که دریافتند اکثر مردم تجربه کلیک کردن روی یک لینک مشکوک را دارند. راه‌های زیادی برای نقض حریم خصوصی افراد وجود دارد، مانند ارسال لینک طعمه به کاربر، ارائه وبسایت‌های تقلبی برای به دست آوردن جزئیات ورود به سیستم با توجه به روش‌های متفاوتی که جنسیت‌های مختلف از رسانه‌های اجتماعی استفاده می‌کنند.

کلاهبرداری عاشقانه آنلاین روش بعدی است. پژوهش‌های زیادی از قبیل رحمتی زاده و همکاران (۱۴۰۰)، کولوپچیا (۲۰۲۰)، کراس و لایت (۲۰۲۱)، بادامی و همکاران (۱۴۰۱)، پکی و همکاران^۱ (۲۰۲۲) به نتایج مشابه با نتایج این پژوهش دست یافته‌اند. طبق یافته‌های پژوهش پکی و همکاران (۲۰۲۲) ۵۵/۲۶ درصد از کاربران گزارش دادند که پیام‌های کلاهبرداری دریافت کرده‌اند که می‌تواند به استفاده آن‌ها از برنامه‌های رایگان مرتبط باشد، در حالی که ۳۲/۴۵ درصد از آن‌ها درواقع توسط کلاهبرداران کلاهبرداری شده‌اند و اپلیکیشن‌های رایگان رسانه‌های اجتماعی همراه با ویژگی‌های اعتبار ورود کاربران می‌توانند مسئول نرخ بالای پیام‌های کلاهبرداری باشند که پاسخ‌دهندگان به‌طور منظم دریافت می‌کنند.

۱ . Paki & et al.



طبق شواهد نتایج پژوهش‌های انجام‌شده هم‌سو با نتایج پژوهش حاضر است و دانشجویان از طریق ارتباط عاطفی که با افراد مختلف و بعضاً جنس مخالف در شبکه‌های اجتماعی برقرار کرده‌اند باعث نشده که حساسیت‌شان نسبت به مسائل امنیتی خودشان کم شود و در این زمینه مراقب سوء استفاده افراد مغرض بوده‌اند. همچنین کراس و لایت (۲۰۲۱) به این نتیجه رسیدند که بسیاری از شاکیان از جستجوی اینترنتی برای تأیید یا رد سوء ظن خود در مورد شریک زندگی خود استفاده کردند. این در بسیاری از موارد نتایج مستدلی به همراه داشت و تأیید کرد که هویت مجرم واقعی نبود. در انجام این کار، استدلال می‌کند که اگر چه برای قربانیان کلاهبرداری عاشقانه مؤثر است، اما پاسخ‌ها می‌تواند آسیب‌های مداومی را که توسط مجرمان به خطر افتاده است را تشدید کند.

همان‌طور که مشاهده شد تمامی نتایج حاکی از آن است که دانشجویان از طریق ارتباط عاطفی که با افراد مختلف و بعضاً جنس مخالف در شبکه‌های اجتماعی برقرار کرده‌اند باعث نشده که حساسیت‌شان نسبت به مسائل امنیتی خودشان کم شود و در این زمینه مراقب سوء استفاده افراد مغرض بوده‌اند.

فیشینگ روش بعدی مورد مطالعه این پژوهش بود. یافته‌های یورو و همکارانش (۲۰۲۳) نشان داد که ۴۷ درصد از شرکت‌کنندگان طعمه فیشینگ شده بودند (به عبارتی بر روی لینک‌های مخرب که در ایمیل‌های ارسال شده به آنان ارائه شده بود کلیک کردند) در حالی که تقریباً ۵۳ درصد از شرکت‌کنندگان طعمه فیشینگ نشده بودند. جالب آنکه دانشجویانی که از حملات فیشینگ بی‌اطلاع بودند، عملکرد بهتری نسبت به دانشجویانی داشتند که از حملات فیشینگ آگاه بودند و یا دانشجویانی که متوجه حملات فیشینگ بودند. اکوکپوجی (۲۰۲۳) به این نتیجه رسید که ۷۰/۶ درصد از دانشجویان مورد بررسی به دلیل ناآگاهی مستعد این نوع حملات فیشینگ هستند. نتایج پژوهش‌های بالا که به صورت تجربی افراد را در معرض فیشینگ قرار داده‌اند نشان داد که بخش زیادی از افراد حتی در بین دانشجویان به عنوان طبقه تحصیل کرده در معرض حملات فیشینگ هستند در عین حالی که از قبل در مورد آن اطلاعات داشته‌اند. شاید این یک هشدار باشد؛ به این معنا که اگر چه آن‌ها خود را در این زمینه آگاه می‌دانند (بر اساس نتایج پژوهش حاضر) ولی در عمل طعمه فیشینگ می‌شوند (پژوهش‌های تجربی).

روش بعدی که به آن اشاره می‌شود جعل هویت و سرقت هویت است. پژوهش‌های متعددی از قبیل جین و همکاران (۲۰۲۱)، الحسیب (۲۰۰۹)، کراس و لایت (۲۰۲۱)، کمپ و پرز^۱ (۲۰۲۳) به نتایجی مشابه با نتایج این پژوهش دست یافته‌اند که به برخی از آن‌ها اشاره می‌شود. طبق یافته‌های جین و همکاران (۲۰۲۱) ۹۱/۶ درصد از نقض اطلاعات کاربران منجر به جعل هویت یا سرقت هویت شده است. همچنین الحسیب (۲۰۰۹) دریافت که اکثر کاربران (به‌ویژه نوجوانان)



به دلیل دست کم گرفتن گستردگی و فعالیت شبکه اجتماعی خود در معرض خطر افشای بیش از حد و تجاوز به حریم خصوصی قرار دارند.

و اما آخرین روشی که به آن می پردازیم روش لینک طعمه است. طبق یافته های ذوالفهمی و همکاران (۲۰۲۳) اکثر مردم تجربه کلیک کردن روی یک لینک مشکوک را دارند. همچنین یافته های جین و همکاران (۲۰۲۱) نشان داد که کاربران باید هنگام ارسال هرگونه رسانه یا اطلاعات در سایت های شبکه های اجتماعی هوشیار باشند. یک رمز عبور قوی باید اتخاذ شود و نباید با کسی به اشتراک گذاشته شود. هنگام بازدید از یک وب سایت باید یو آر ال را بررسی کنید و نباید روی پیوندهای مخرب کلیک کنید. این عادات می تواند تا حدی به کاربر کمک کند تا در برابر حملات سایبری مختلف در رسانه های اجتماعی محافظت شود.

آنچه از نتایج پژوهش ها می توان تحلیل کرد این است که کاربران اگر با لینک جذابی روبرو شدند بدون اینکه از ایمن بودن لینک مطمئن شوند روی آن کلیک کردند و در دام لینک طعمه افتاده اند.

سؤال سوم: متغیرهای جمعیت شناختی (جنسیت، تحصیلات) به چه میزان بر رفتارهای مرتبط با امنیت و حریم خصوصی کاربران در شبکه های اجتماعی اثر گذارند؟

یافته ها نشان دادند که میانگین همه متغیرها شامل عوامل مهندسی اجتماعی، روش های مهندسی اجتماعی، و مهندسی اجتماعی به طور کلی (عوامل و روش ها) در گروه زنان از گروه مردان، مقداری بیشتر است. به عبارتی میزان انجام رفتارهای مهندسی اجتماعی مرتبط با امنیت و حریم خصوصی در بین زنان میانگین بالاتری را به دست آورده است.

جدول ۳. نتایج آزمون مقایسه میزان رفتارهای مرتبط با امنیت و حریم خصوصی کاربران در شبکه های اجتماعی در بین زنان و مردان

متغیر	جنسیت	تعداد	میانگین	انحراف معیار	سطح معناداری آزمون لون	T	سطح معناداری آزمون T
عوامل مهندسی اجتماعی	زن	۱۸۲	۲۰/۲۸	۳/۰۲۵	۰/۰۳۰	۳/۲۴۴	۰/۰۰۱
	مرد	۱۹۲	۱۹/۲۳	۳/۲۲۹			
روش های مهندسی اجتماعی	زن	۱۸۳	۲۱/۵۸	۳/۷۶۲	۰/۶۷۸	۴/۰۱۵	۰/۰۰۰۱
	مرد	۱۹۱	۱۹/۹۹	۳/۹۱۵			
مهندسی اجتماعی (عوامل و روش ها)	زن	۱۸۲	۴۱/۸۵۷	۶/۰۸۸	۰/۴۸۲	۴/۱۷۲	۰/۰۰۰۱
	مرد	۱۹۱	۳۹/۲۲۵	۶/۰۹۲			

برای بررسی تفاوت میانگین بین گروه های آزمودنی ها که بر اساس سطح تحصیلات دسته بندی شده بودند از آزمون تحلیل واریانس یک طرفه استفاده شد. نتایج نشان داد میانگین هیچ یک از متغیرها در سه گروه تحصیلی (کارشناسی، کارشناسی ارشد و دکتری) یکسان نبود و تفاوت هایی

وجود داشت. پس از بررسی معناداری این تفاوت مشخص شد که در متغیرهای روش‌های مهندسی اجتماعی و مهندسی اجتماعی به‌طور کلی (عوامل و روش‌ها) این تفاوت معنادار است و بالاترین میزان میانگین مربوط به گروه کارشناسی بود. اما در متغیر عوامل مهندسی اجتماعی معنادار نبود.



جدول ۴. نتایج آزمون تحلیل واریانس یک‌طرفه متغیرهای پژوهش برحسب تحصیلات

متغیر	تحصیلات	میانگین	انحراف معیار	سطح معناداری لون	آماره F	سطح معناداری آنوا
عوامل مهندسی اجتماعی	کارشناسی	۱۹/۹۴	۲/۸۲۴	۰/۰۰۱	۶/۴۶۱	باتوجه به ناهمگن بودن واریانس‌ها از آزمون کروسکال والیس استفاده شد.
	ارشد	۱۹/۳۱	۳/۷۶۳			
	دکتری	۱۹/۷۹	۳/۳۵۹			
روش‌های مهندسی اجتماعی	کارشناسی	۲۱/۳۱	۳/۶۶۳	۰/۴۳۸	۶/۴۶۱	۰/۰۰۲
	ارشد	۱۹/۷۴	۴/۰۵۲			
	دکتری	۲۰/۲۹	۴/۶۸۱			
مهندسی اجتماعی (عوامل و روش‌ها)	کارشناسی	۴۱/۲۴	۵/۷۱۹	۰/۱۴۹	۴/۸۶۱	۰/۰۰۸
	ارشد	۳۹/۰۴	۶/۸۱۷			
	دکتری	۴۰/۰۸	۶/۹۹۱			

پژوهشی که در مورد متغیر جمعیت شناختی جنسیت در داخل و خارج از کشور و هم‌سو با نتایج پژوهش حاضر انجام گرفته است پژوهش یورو و همکارانش (۲۰۲۳) بوده است، یافته‌های این پژوهش حاکی از آن است که زنان بیشتر از مردان مورد حملات فیشینگ قرار می‌گیرند.

۴- بحث و نتیجه‌گیری

در مورد میزان انجام رفتارهای مربوط به عوامل مهندسی اجتماعی دانشجویان در ارتباط با امنیت و حریم خصوصی (شامل سلبریتی‌ها، اقتدار، تنهایی، وقایع مورد توجه و عادی انگاری) در حد مطلوب و میزان انجام رفتارهای مربوط به روش‌های مهندسی اجتماعی دانشجویان در ارتباط با امنیت و حریم خصوصی (شامل لینک طعمه، ارائه وب‌سایت‌های تقلبی، کلاهبرداری‌های عاشقانه آنلاین، فیشینگ و جعل و سرقت هویت) بیشتر از حد مطلوب بود. دو موضوع مهم در این بخش نیازمند تحلیل است: اول اینکه چرا روش‌های مهندسی اجتماعی در مقایسه با عوامل نمره بالاتری کسب کرده‌اند؟ و دوم چرا وضعیت انجام رفتارهای مربوط به عوامل مهندسی اجتماعی دانشجویان در ارتباط با امنیت و حریم خصوصی به‌طور کلی نمره بالاتری از عوامل فردی مرتبط به آن دریافت کرده‌اند؟ اگرچه پاسخ دقیق نیازمند مطالعات بیشتر است اما در مقام تحلیل شاید بتوان نتایج را به توجه بیشتر رسانه‌ها به روش‌های مهندسی اجتماعی و آگاه‌سازی جامعه در این مورد در مقایسه با عوامل مهندسی اجتماعی مرتبط و عوامل فردی مرتبط با امنیت و حریم خصوصی، مربوط دانست. علاوه بر اینکه ماهیت جنبه‌های مربوط به مهندسی اجتماعی



نسبت به عوامل فردی، بیشتر ادراکی است چنانکه در ذیل سؤال مربوطه گفته شد بر اساس نتایج پژوهش های قبلی، احتمالاً این آگاهی در عمل منتج به رفتار صحیح در مقابل تهدید امنیتی نمی شود. به عبارتی بازهم اهمیت در مقابل انجام رفتار قرار می گیرد.

در پایان پیشنهاد می شود دوره هایی برای آشنایی کامل کاربران با تهدیدات و خطرهای شبکه های اجتماعی و حتی نحوه مقابله با آن ها در رفتار عملی برگزار گردد و از طرفی به طور مستمر در سطح تمامی رسانه ها، افرادی که با آسیب های جدی در این فضاها مواجه شده اند و مجازات های اجرا شده علیه ناقضان حریم خصوصی اعلام شود. همچنین با توجه به اینکه مردان معمولاً ریسک پذیرتر از بانوان هستند و کمتر خطر را جدی می گیرند لذا لازم است تا در قالب برگزاری دوره های آموزشی، مردان را بیشتر از قبل با مسائل امنیتی که در شبکه های اجتماعی با آن روبرو هستند آشنا کرد و بیشتر بر مراقبت از خود در برابر این تهدیدها تأکید کرد؛ و در نهایت یکسری دوره های آموزشی برای دانشجویان دوره کارشناسی که عمدتاً دهه هشتادی هستند در نظر گرفته شود تا بسیاری از تکنیک های مرتبط با فضای مجازی که برای این سنین ممکن است کمتر آشنا باشد مورد آموزش قرار بگیرد.

۵- سپاسگزاری

نویسندگان بر خود فرض می دانند از داوران محترم به دلیل نکات و یادداشت های ارزشمند و اثرگذار در بهبود مقاله حاضر، تشکر و قدردانی نمایند.

۶- منابع و مآخذ

- احسانی فر، محمد؛ و رضوانیان، محمد. (۱۳۹۶، ۵ دی). نقش رفتار کاربران در احساس امنیت شبکه های اجتماعی. پژوهشکده مدیریت و توسعه پژوهشگاه فرهنگ و هنر. <https://civilica.com/doc/708049>
- اسلامی، الهه؛ موسوی، سیدهاشم؛ و علی خواه، فردین. (۱۳۹۹). سلبریتی های مجازی: غریبه های آشنا در عصر رسانه های اجتماعی گونه شناسی زنان مشهور ایرانی در رسانه اینستاگرام. مطالعات فرهنگی و ارتباطات، ۵۹(۱۶)، ۴۵-۷۴. <https://doi.org/10.22034/jcsc.2019.35296>
- بادامی، محمدعلی؛ مقدادی، محمد مهدی؛ و پیله ور، مرضیه. (۱۴۰۱). جایگاه حمایت های حقوقی از کودکان در فضای مجازی با تأکید بر حق تربیت دینی. پژوهش های حقوقی، ۲۱(۵۰)، ۴۹۴-۴۵۷. doi: 10.48300/jlr.2021.279730.1619
- فاطمی نیا، محمدعلی؛ حیدری، مهدی؛ و جوانبخت، حسن. (۱۴۰۰). ضریب نفوذ اجتماعی سلبریتی ها و عوامل اجتماعی مؤثر بر آن در شهر رشت. پژوهش های ارتباطی، ۲۸(۱۰۸)، ۶۷-۳۹. <https://doi.org/10.22082/cr.2021.533889.2211>
- حسین پور، جعفر؛ و مصرخانی، قدیر. (۱۳۹۷). نقش شبکه های اجتماعی مجازی بر امنیت عمومی کاربران آن. نظم و امنیت/انتظامی، ۱۱(۲)، ۱۷۰-۱۵۳.
- حسینی سنو، سید امین؛ و مظاهری، الهام. (۱۳۹۷). تأثیر حریم خصوصی، امنیت و اعتماد ادراک شده بر رفتار به اشتراک گذاری اطلاعات در شبکه های اجتماعی موبایل: نقش تعدیل کننده متغیر جنسیت. پردازش و مدیریت اطلاعات، ۳۴(۱)، ۲۴۵-۲۷۴. doi: 10.35050/JIPM010.2018.009



جعفرپور هادیکیاشری، رضا؛ کابلی، محمدهادی؛ و شاهچراغی، آزاده. (۱۴۰۱). واکاوی میزان اثرگذاری عناصر عینی و ذهنی بر حس «حریم» در فضای معماری. هنر و تمدن شرق، ۱۰ (۳۸)، ۲۸-۱۷. doi: 10.22034/jaco.2022.364304.1264

جلالی، زهرا؛ کیانپور، مسعود؛ و آقابابایی، احسان. (۱۳۹۶). تبیین جامعه‌شناختی مدیریت حریم شخصی کاربران جوان فیس‌بوک شهر اصفهان. پژوهش‌های راهبردی مسائل اجتماعی، ۶ (۱)، ۲۸-۱۷. doi:10.22108/ssoss.2017.21281

پورنقدی، بهزاد. (۱۳۹۷). فرصت‌ها و تهدیدهای امنیت در شبکه‌های اجتماعی مجازی برای دانشجویان. پژوهش‌های راهبردی مسائل اجتماعی، ۷ (۲)، ۹۸-۸۷. doi: 10.22108/ssoss.2018.103434.1062

رحمتی زاده، آریتا؛ کریم زادگان مقدم، داود؛ و وحدت، داود. (۱۴۰۰). اطمینان‌پذیری و تفاوت میان رفتار اخلاقی صداقت در گفتار و نیت درونی افراد در شبکه‌های اجتماعی. اخلاق در علوم و فناوری، ۱۶ (۳)، ۹۷-۱۰۴. doi: 20.1001.1.22517634.1400.16.3.13.0

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. *Advanced Computer Research*, 10(50), 194-205. 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>.

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>.



- Fadhil, H. S. (2023). Social Engineering Attacks Techniques. *Int. J. Progress. Res. Eng. Manag. Sci. International Journal Of Engineering And Computer Science IJPREMS*, 3(1), 18-20. DOI:10.18535/ijecs/v6i1.09
- 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>
- 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>.
- 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>.
- 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
- Okokpuije, 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/ijdsdp.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](https://doi.org/10.52326/jss.utm.2022.5(3).11).
- 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>.

Yi, Y., Zhu, N., He, J., Jurecut, 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. DOI: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>.

