UDC 62-50
DOI: 10.20535/SRIT.2308-8893.2023.4.06

RAISING THE INFORMATION SECURITY AWARENESS AMONG SOCIAL MEDIA USERS IN THE MIDDLE EAST

HEND KHALID ALKAHTANI

Abstract. Social media presents both opportunities and risks for any firm. The Internet has recently made everything possible. Due to its low cost and rapid speed, it is in high demand. Due to the virtual technique of interacting through various social media apps like Instagram, WhatsApp, Twitter, Facebook, etc., people are drawn to social networking. Despite the fact that it offers advantages on both sides, new threats are constantly emerging. Social media usage is widespread, but awareness is low, which makes significant cyberattacks more likely. Numerous threat categories put consumers at risk for cyber security. This research reviewed literature on educating Middle Eastern social media users about information security. Additionally, this research examines various threats made via social media, offers countermeasures, and considers various detection methods.

Keywords: security, security awareness social media, WhatsApp, Twitter, Facebook.

INTRODUCTION

Nowadays, the Internet has become a social environment that includes community, value and norm [1]. Sites like YouTube, Facebook, Twitter, and Instagram have seen a huge increase in the number of users. With the advancement of technology, social network has become pervasive and used like never before. In fact, social media is a collection of websites and applications designed and its goal is to allow people to share the content they want in a fast, efficient, and real-time manner [2]. It is also an online digital communication tool with which you can share links, SMS messages, photos and videos, it can be accessed anytime and anywhere. In fact, there are many social media sites where a large number of people spend a long time using them. Moreover, the number of OSNs is increasing year by year [3].

Facebook was the first social media network in the list of the most popular social networks with a large number of accounts and nearly 2.6 billion monthly active users. It also carries a huge amount of information due to this large number of users [4]. Nevertheless, this wide spread may cause great harm to users' private information because it may facilitate access to and violation of this information, because users cannot choose and specify their own privacy preferences in applica-

tions [5]. This poses significant privacy risks by making users' private data available to applications when they are often not fully aware of the risk of disclosing such information [2]. Moreover, Internet technology inherently leads to security problems, cybercrime, hackers, and intruders. In fact, the characteristics of the Internet reinforce the network structures that may lead to the occurrence of major Internet theft and fraud which is referred to as cybercrime.

Social media users need awareness and knowledge regarding the importance of personal information security, known as Information Security Awareness (ISA). ISA focuses on how an individual is aware of information security policies, rules, and guidelines [6]. Furthermore, ISA can shape individual characteristics to be more interested in revealing self-information in the context of social media. Thus, in this review, we will talk about the level of information security awareness among social media users in the Middle East [1]. Privacy violation is one of the main problems faced by social media users. It presents an ongoing risk to these users.

LITERATURE REVIEW

Due to its extensive use in the most prominent industries including education, healthcare, and entertainment, social media in the Middle East has grown to play a significant role in our lives. The popularity of various online social media platforms like Twitter, YouTube, Facebook and other social networking applications has increased because of this growth in the social networking field [7]. Therefore, the study's literature review will cover the knowledge gap of the significant risk to the personal information post on social media platforms.

The Perspective of Social networking privacy

People in general enjoy exchanging private information with each other, at the same time they have an obvious lack of awareness and knowledge about what might happen if they do so voluntarily or how to stop illegal disclosure of their personal information [8]. Social media's structure encourages its users to contribute willingly by exposing personal information. Users may reveal their personal information if they believe the benefits outweigh the drawbacks.

Social media provides a platform for studying business trends, consumer opinions, trend-setting, and political movements. Online activities that lack enough knowledge and social security and privacy can lead to extreme catastrophes, such as electronic hacking in which personal and private information is required for harmful purposes. Popular social media platforms like Facebook and Twitter, for example, also have their own unique techniques for determining the social characteristics of its users without having to ask them directly [8].

Despite the security measures taken by social media producers and programmers to protect the user information, it is still possible for the personal data to fall into the wrong hands and be exploited. This issue has already occurred in the early months of 2018 known as The Facebook-Cambridge Analytica data scandal, which involved Cambridge Analytica consulting company using millions of Facebook users' personal information without their knowledge or agreement for political advertising [9].

To sum up, threats are growing daily despite the existence of numerous preventative strategies, especially that many social media platforms have the option of making the user's profile available to the public. Moreover, without the user's awareness, attackers and online hackers can have access to the user's private information, as well as analyze and use them at remarkable speeds intending to cause harm.

Information security awareness

Information security awareness is a process that modifies and changes users' attitudes toward safe information standards as well as their values, behaviors, practices, work habits, and organizational culture. Changing these standards and practices helps every user to recognize the information security policies, guidelines, and procedures that should be followed in order to avoid any electronic harassment. Thus, users are required to understand both general and personal information security concepts [10].

Self-disclosure is defined as any knowledge about oneself that is voluntarily and consciously shared with others. Social media users need to be familiar with the significance of protecting personal information. Furthermore, security awareness can alter a person's personality so that they are more concerned about exposing personal information in the social media platforms [9].

Furthermore, the weakest link in any business is its regular users, who receive very little security awareness training as organizations grow their usage of cutting-edge security technologies and continually train their security personnel. As a result, organized hackers are working very hard right now to develop cutting-edge hacking techniques that can be used to steal both personal data and money from the general population [14]. Additionally, the Middle East is a desirable target for cybercriminals due to the region's rapid internet use rate and low consumer security awareness of the threats that may arise [10].

Accordingly, to escalate information security awareness of users, threats and harmful activities by online hackers should be pointed out and acknowledged.

Threats in Social Media Platforms

There are various threats done on social media platforms and applications, which a large number of users are not aware about, including the following.

Multimedia content threats. Multimedia content include threats associated with static links, Video and audio conferencing, and steganography.

Static links are used by 48.6% of social networking service users to exchange information from interactive media. This act causes the exposure of personal information and data loss for the users.

Moreover, most social media users post their own video and audio content to social media platforms in order to share their skills and ideas, some people abuse these audios and videos by modifying them to make them uncomfortable or life threatening [12].

Another threat of multimedia is steganography, which concentrates on encoding secret communications in a form that only the sender can comprehend in order to conceal sensitive information in visual form without the recipient awareness. For instance, a car image can contain some sort of computer viruses that deletes or steals the users' system files [13].

Traditional threats. Traditional threats include digital stalking, spamming, phishing data, and click jacking. Digital stalking is the practice of following and stalking someone online via email, or through other electronic communication channels. Typically, stalking requires a person engaging in persistent annoying or threatening actions [12].

While spamming refers to unsolicited texts or emails, which are distributed with multiple copies over the internet. Usually, spam messages are about commercial advertising. Spamming consumes a significant amount of network capacity in addition to wasting people's time.

Phishing is a fraud strategy used to obtain private data by misrepresenting a reliable organization, such as a password. Attackers frequently utilize phishing emails to spread risky links [8]. Figure 1 shows an illustration of the phishing technique used by hackers.

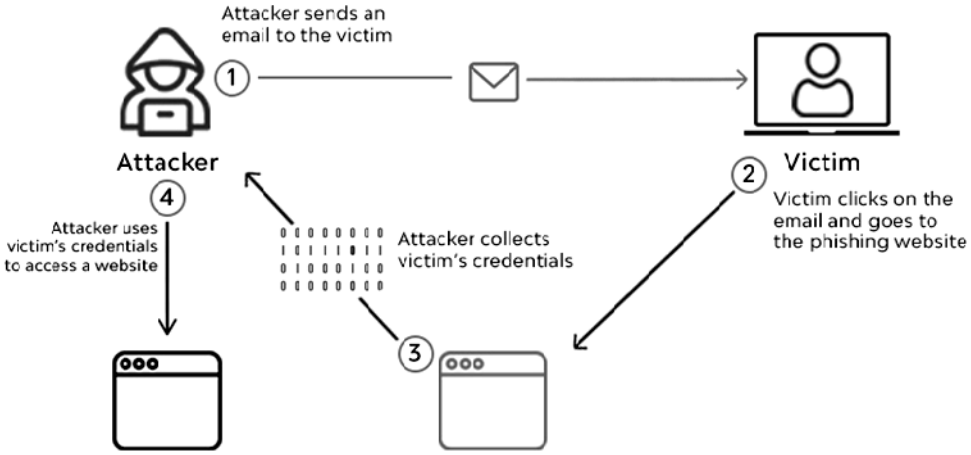

Fig. 1. Phishing technique [11]

Another method of traditional threats is click jacking, which is based on deceiving a user into clicking on a wrong link. Users may unintentionally download spywares and viruses as a result, browse dangerous websites, or make unwanted online purchases.

Social Media Issues and Security Awareness among the users

Social media and its user have a relationship that is affected by cybersecurity and its environment. This relationship intensifies as social media use rises, as cybercriminals broaden their scope of interest and begin to focus on social media accounts. Users of social media are increasingly becoming one of their targets because the majority of them are unaware of the security and privacy measures that can be applied to individual accounts. Nowadays, social media plays a significant role in how individuals live their daily lives. This amply demonstrated the rise in popularity of social media in the modern day as well as the fact that its users have attained a critical mass necessary for influence, which increases their susceptibility and makes them even more vulnerable as hacking victims [15].

Teenagers in particular are using the Internet more and more frequently as a result of its increased popularity globally [16]. The majority of these adolescent social media users are students whose academic and social lives have been greatly impacted by changes in the global environment. These young adults and teenagers

have no idea how to use their privacy settings. Teenagers and young adults want to express their identity and take the chance of being discovered and coming into touch with hackers because they are more interested in seizing the opportunity to connect with others and forge genuine relationships [17].

The majority of social media users do not really understand the significance of their privacy settings. Young adults and teenagers are more likely to be careless with their social media privacy settings. According to Livingstone's research findings from 2008, teens mostly use social media to create dangerous and intimate content by expressing themselves. Identity theft is one type of cybercrime that might occur as a result of this lack of privacy settings. The percentage of social media users who actively utilize various social network sites raises along with the overall growth of social media users. This brings us to the second action, where people are making it easier for hackers to find them. Users frequently link their social network account authorizations together or use the same password for several accounts because they maintain multiple social networks for personal usage [18].

For the hackers, this is a target straight out of heaven. Simply by acquiring access to one of the person's many accounts, they can quickly gain access to multiple accounts. A social network aggregator is what this is. Although it makes it easier for users to keep an eye on their social media profiles, it poses certain security risks [19]. Given that once one of their accounts has been hijacked, hackers will be able to find all of their other accounts, thereby increasing the risk to other accounts. For these teenagers and young adults, a cyber-security knowledge gap might be a problem. Due to their ignorance of the significance of security implementation, they are blind to nearby cases of accounts being compromised. Although social engineering assaults may not appear to be as sophisticated as other hacking techniques, they have produced some of the most effective attacks on targets [20].

The Need for Effective Information Security Awareness

Over the past few years, the Middle East has seen a steady rise in the number of internet users. While the Middle East only accounts for 3.2% of all internet users globally, it has seen an increase in internet usage of 1825% over the previous 10 years, compared to a rise of 445% for the rest of the globe, according to the World Internet Usage Statistics News [21]. Additionally, it stated that as of June 30, 2010, Bahrain, the United Arab Emirates, and Qatar had the greatest rates of internet penetration in the Middle East, representing 88%, 75.9%, and 51.8% of their respective populations, respectively. Numerous online businesses have been drawn to the Middle East by this expansion, enabling many already-established industries including education, health, aviation, and government to expand [22].

A thorough investigation of the difficulties and dangers that social networking sites and social networks face is the goal of Yassein M. et al. in [15]. In this study, electronic crimes were analyzed in relation to user-posted content on social networking sites and the use of that information to locate the original victims. Users are unaware of the risks associated with sharing this information when it is being published. After that, they list the flaws and give a brief summary of the protective strategies now in use, highlighting the weaknesses.

In [23] Almarabeh et al. discuss the distribution of the different sorts of attacks that social media sites are subject to. They present two different sorts of attacks in this context: classic attacks and modern attacks. A clear picture of the

attacks has emerged thanks to the information on the different sorts of strikes. What kinds are there? And what techniques do they employ? There is information concerning social media users' flaws, such as the fact that their personal accounts have a low level of secrecy, which makes it simple to hack them. The primary goal of this research is to increase online social networking users' awareness of how to protect themselves and their data against risks and assaults while using social media platforms.

Security and privacy issues with social networks and social engineering were examined by Ali et al. [24]. Additionally, information about OSNs was covered, including its explanation, methods, resources, and the growth and fall of different OSNs. The report emphasized crucial privacy safeguards as well as user risks and weaknesses. By classifying risks into several categories that were investigated as part of a knowledge-sharing strategy, taxonomy has been constructed. In this study, the aftermath of a catastrophe is discussed, as well as how terrorism undermines the support for privacy. They incorporated privacy rules to take care of user privacy for the goal of reducing and monitoring personal information or data, encouraging users to reply appropriately and utilize social media solely for public topics.

The issues that could endanger the privacy of social media users were discussed by Ali et al. in [25]. There were two categories of issues: traditional threats and contemporary threats. To learn more about users' attitudes on privacy settings as well as their knowledge and interest in them, a questionnaire was created. Unfortunately, the findings were disappointing because a significant portion of users did not take use of privacy-preserving settings offered by service providers. Finally, recommendations and fixes for safeguarding user content and privacy were made. In [26] Aghasian et al. introduced an automated Fuzzy model for calculating the score of privacy of unstructured data of social media users on Facebook and Twitter. They also cautioned these users of the risks associated with using social media. The model consists of two phases that record privacy and calculate the privacy risk score. The machine learning model first identifies the features that have an impact on users' privacy. The final privacy score is then calculated using a fuzzy based approach. Information retrieval and pre-processing make up the first of the model's three phases. The second is by giving them some fundamental information so they can obtain the source of sentimental privacy. The outcome of the privacy score for users who have shared their information is determined at the final stage (Fig. 3).

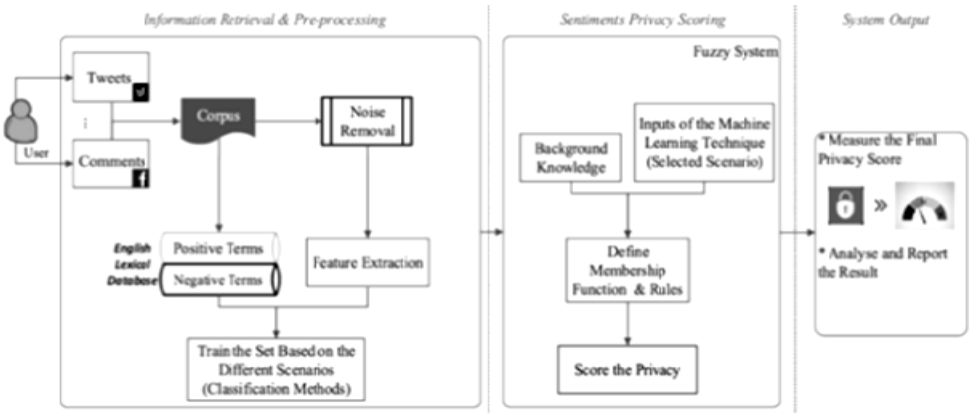

Fig. 3. Flow of privacy scoring process of proposed method [24]

Soomro et al. talked about a new list of crimes in social media like cyber intrusion, credit card fraud alongside disaster fraud and data breaches in [27], as well as many different types of crimes pertaining to social media like social engineering and phishing, burglary via social networking, identity theft, malware, cyber-casing, and cyber-stalking. Researchers in this area have employed a variety of strategies and deterrents to combat these crimes. Finally, this study emphasized a number of tips and methods for preventing cybercrime.

A deep learning-based efficient categorization technique for assaults that target Twitter users was proposed by Mostafa et al. [28]. The sole supporting method, the feature extraction issue, the lack of precision, and the slow speed were all issues this paper addressed. The tweets are first pre-processed using Sen2Vec rather than the element being extracted. The method used in this work is a sophisticated deep learning language processing technique that can convert a word or piece of text into a vector that represents it. Then, using a variety of machine learning methods, a machine learning model is created to distinguish between spam and non-spam. At the following level, parameter settings are assigned for spam filtering. An actual ground truth dataset is used to build up their testing.

Users were informed about the issues and potential harms caused by the dissemination of content on social media sites and the absence of privacy by, [26], and [28]. In this instance, the most significant security flaws affecting social media platforms and the most significant contemporary methods preventing the spread of hazardous content were investigated. Users and their exploitation or targeting were discussed. In order to lessen users' lack of privacy on social networking sites and to stop the spread of hazardous content in social networks, [24] offered a cutting-edge technology that has been researched and developed. "Fuzzy-based" is the name of the technology in use.

CONCLUSION

Social media is effective and beneficial in many areas, but new challenges and concerns regarding privacy and security continue to grow. This review discussed the most important papers that talk about the problems caused by the content of social networking sites, and the review also dealt with information security among social media users in the Middle East. This issue remains a fundamental and important issue. Accordingly, research and studies are ongoing. We suggest for future studies to focus more on information security awareness among social media users in the Middle East.

As Middle Eastern organizations expand their use of social media, advanced security technology, and use of the latest hardware and software, launching technical attacks has become more and more difficult. Similarly, organizations develop complete and well-written security policies and hire IT security experts who also help reduce the number of potential attacks. Unfortunately, little is used to secure the weakest link, that is, social media users. This drives attackers to gain unauthorized access to information by exploiting the user's trust and propensity to help. The paper discussed the level of information security awareness among social media users in the Middle East and reported the results of several IT security awareness studies. Discuss the importance of assessing security awareness by conducting monitoring audits. Several key factors have also been shown to help raise security awareness among social media users.

REFERENCES

1. L. Zhang, C. Amos, and I. Pentina, "Information Disclosure on a Chinese Social Media Platform," *J. Inf. Priv. Secur*., vol. 11, no. 1, pp. 3–18, 2015. doi: 10.1080/15536548.2015.1010981
2. S. Rathore, P.K. Sharma, V. Loia, Y.S. Jeong, and J.H. Park, "Social network security: Issues, challenges, threats, and solutions," *Information Sciences*, 421, pp. 43–69, 2017. doi: 10.1016/j.ins.2017.08.063.
3. M. Al-Enazi and S. El Khediri, "Advanced Classification Techniques for Improving Networks Intrusion Detection System Efficiency," *Journal of Applied Security Research*, 17(1), 2021. doi: 10.1080/19361610.2021.1918500.
4. A. Ali, A. Kamran, M. Ahmed, B. Raza, and M. Ilyas, "Privacy concerns in online social networks: A users' perspective," *International Journal of Advanced Computer Science and Applications*, 10(7), 2019.
5. S. Ali, N. Islam, A. Rauf, I.U. Din, M. Guizani, and J.J. Rodrigues, "Privacy and security issues in online social networks," *Future Internet*, 10(12), pp. 1–12, 2018. doi: 10.3390/fi10120114.
6. M. Koohikamali, D.A. Peak, and V.R. Prybutok, "Beyond self-disclosure: Disclosure of information about others in social network sites," *Comput. Human Behav*., vol. 69, pp. 29–42, 2017. doi: 10.1016/j.chb.2016.12.012.
7. F. Aloul, "The Need for Effective Information Security Awareness," *Journal of Advances in Information Technology*, 3(3), pp. 176–183, 2012. doi: 10.4304/jait.3.3.176-183.
8. S. Alotaibi, K. Alharbi, H. Alwabli, H. Aljoaey, B. Abaalkhail, S. El Khediri, "Threats, crimes and issues of privacy of users' information shared on online social networks," 2021 *International Symposium on Networks, Computers and Communications (ISNCC)*. doi: 10.1109/ISNCC52172.2021.9615815.
9. Dony Martinus Sihotang et al., "Factors Affecting the Intention of Social Media Users to Disclosure Personal Information," *2021 International Conference on Advanced Computer Science and Information Systems (ICACSIS)*. doi: 10.1109/ICACSIS53237.2021.9631351.
10. A. Ali, M. Mahmud, N. Molok, and Sh. Talib, "Information security awareness through the use of social media," *The 5th International Conference "Information and Communication Technology for The Muslim World"*, 2014. doi: 10.1109/ICT4M.2014.7020668.
11. "Cyber security Brief Guide for Beginners: Phishing Attacks", *Cyber Coastal*, 2022. Available: https://cybercoastal.com/cybersecurity-brief-guide-for-beginners-phishing-attacks/
12. A. Gupta, Sh. Mehetre, and A. More, "Security in Social Media," *International Research Journal of Innovations in Engineering and Technology*, 5(12), pp. 40–44, 2021. doi: 10.47001/IRJIET/2021.512008.
13. Y. Hafsari, F. Permatasari, and N. Rahman, "A Review on Social Media Issues and Security Awareness among the users," *Journal of Applied Technology and Innovation*, 1(1), pp. 28–36, 2017.
14. P. Potgieter, "The Awareness Behavior of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology," *Proceedings of 4th International Conference on the Internet, Cyber Security and Information Systems 2019*, 12, pp. 272–280. Available: https://doi.org/10.29007/gprf
15. "Global Digital Statistics. GWI Social Summary. GWI Quarter Report," *Global Web Index*. Accessed on: February 1, 2017. [Online]. Available: http://insight. globalwebindex.net/hsfs/hub/304927/file-2377691590-pdf/Reports/GWI_Social_Summary_Q4_2014.pdf?submissionGuid=d75c46ce922c-4efc-8ac3-08dbe9ba4904
16. S. Bennett, A. Bishop, B. Dalgarno, J. Waycott, and G. Kennedy, *Implementing Web 2.0 technology in higher education: A collective case study.* 1st ed., 2012
17. A. Charlesworth, *An introduction to social media marketing*. 1st ed. London: Routledge, 2015, 209 p.

18. K. Lewis, J. Kaufman, and N. Christakis, "The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network," *Journal of Computer-Mediated Communication*, 14(1), pp.79–100, 2008. Available: https://doi.org/10.1111/j.1083-6101.2008.01432.x
19. F. Benevenuto, T. Rodrigues, M. Cha, and V. Almeida, "Characterizing user navigation and interactions in online social networks," *Information Sciences*, 195, pp. 1–24, 2012. doi: 10.1145/1644893.1644900.
20. N.A. Abd Rahman, "A Review on Social Media Issues and Security Awareness among the users," *Journal of Applied Technology and Innovation*, vol. 1, no. 1, pp. 28–36, 2018.
21. "Miniwatts Marketing Group," *2010 Internet World Stats*. Available: http://www.internetworldstats.com/stats.htm
22. F. Aloul, "The Need for Effective Information Security Awareness," *Journal of Advances in Information Technology*, 3, pp. 176–183, 2012. doi: 10.4304/jait.3.3.176–183.
23. H. Almarabeh and A. Sulieman, "The impact of cyber threats on social networking sites," *International Journal of Advanced Research in Computer Science*, 10(2), 2019. doi: 10.26483/ijarcs.v10i2.6384.
24. S. Ali, N. Islam, A. Rauf, I.U. Din, M. Guizani, and J.J. Rodrigues, "Privacy and security issues in online social networks," *Future Internet*, 10(12), 2018. doi: 10.3390/fi10120114.
25. E. Aghasian, S. Garg, and J. Montgomery, "An automated model to score the privacy of unstructured information—Social media case," *Computers & Security*, 92(3), 101778, 2020. doi: 10.1016/j.cose.2020.101778.
26. T.R. Soomro and M. Hussain, "Social Media-Related Cybercrimes and Techniques for Their Prevention," *Applied Computer Systems*, 24(1), pp. 9–17, 2019. doi: 10.2478/acss-2019-0002.
27. M. Mostafa, A. Abdelwahab, and H.M. Sayed, "Detecting spam campaign in twitter with semantic similarity," in *Journal of Physics: Conference Series*, vol. 1447, no. 1, p. 012044, 2020.
28. K. Stokes and N. Carlsson, "A peer-to-peer agent community for digital oblivion in online Social networks," in *2013 Eleventh Annual Conference on Privacy, Security and Trust, IEEE 2013*, pp. 103–110.

Received 15.12.2022

INFORMATION ON THE ARTICLE

Hend Khalid Alkahtani, College of Computer and Information Sciences of Princess Nourah Bint Abdulrahman University, Saudi Arabia, e-mail: hkalqahtani@pnu.edu.sa

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СЕРЕД КОРИСТУВАЧІВ СОЦІАЛЬНИХ МЕДІА НА БЛИЗЬКОМУ СХОДІ / Хенд Халід Алкахтані

Анотація. Соціальні медіа створюють як можливості, так і ризики для будь-якої компанії. Інтернет нещодавно зробив все можливим. Завдяки низькій вартості і швидкості він користується великим попитом. Завдяки віртуальній техніці взаємодії через різні програми соціальних мереж, такі як Instagram, WhatsApp, Twitter, Facebook тощо, людей приваблює використання соціальних мереж. Незважаючи на те, що Інтернет пропонує переваги для обох сторін, постійно виникають нові загрози. Соціальні мережі використовуються широко, але поінформованість низька, що підвищує ймовірність значних кібератак. Існує багато категорій загроз, які загрожують споживачам. У праці розглянуто літературу про навчання користувачів соціальних мереж Близького Сходу щодо інформаційної безпеки. Крім цього, розглянуто різні загрози через соціальні мережі, запропоновано заходи протидії та розглянуто різні методи виявлення.

Ключові слова: безпека, соціальні медіа, WhatsApp, Twitter, Facebook.