Eng Int Syst (2022) 6: 475–481

Engineering
Intelligent Systems

Unsafe Factors Associated With Internet Social Information Dissemination

Xiaohua Jin[1,*], Jiyu Zheng[2], Xiaoyan Li[1], Jiankun Gong[1], and Zhihao Lin[1]

[1] *School of Energy & Environment, Zhongyuan University of Technology, Zhengzhou, Henan 450007, China*
[2] *School of resources and safety Engineering, Henan University of Engineering, Zhengzhou, Henan 451191, China*

In the process of social networking, there are several unsafe factors associated with information dissemination and an increasing number of unsafe factors seriously affect personal daily life. Based on the specific functions of social networking software, the risk of each function is divided into three levels: high, medium and low, and the risk of each function is calculated. This paper analyzes various unsafe factors, such as personal injury caused by family information disclosure, network fraud caused by personal information disclosure, personal information being used for illegal activities, public opinion being affected by false and misleading information, social accounts being stolen for illegal activities and so on. Finally, it suggests countermeasures for the unsafe factors of network social information communication, which is of significance to prevent network social risk.

Keywords: Internet; social contact; information dissemination; unsafe factors

1. INTRODUCTION

A social network includes both hardware and software. It is a social network service application that takes hardware as the carrier (mobile phone, computer, tablet, etc.), social network software as the tool, and relies on real social relations to realize information dissemination and interactive communication between interested parties (Zhong, 2020). While applying social network software, the software is also collecting personal information and using big data to judge personal preferences and push advertising, which often results in trouble for the users. In serious cases, it results in information leakage and is used by criminals (Zou, 2017; Li and Zhu, 2021; Xu et al., 2021).

Social networks provide people with a platform for information sharing and recording personal good moments in their lives. On the one hand, these records themselves disclose some of their own information, such as one's personal living environment, their workplace, address, children, identity information, etc. and this information can be collected by criminals, resulting in potential information risks. Social software information is stored on electronic devices and servers at the same time. Some hackers and phishing software are able to steal relevant information and use this information to defraud (Zhang and Kang, 2014; Mutambik et al., 2021; Murire et al., 2021; He and Ji, 2021). Since the 4G era, with the rapid development of mobile terminals, the functions of various social software have become increasingly powerful. The personal use of social software has increased rapidly in frequency, personal information sharing is increasing, and there are a growing number of problems. There is an urgent need for individuals to improve their information security literacy (Zhao et al., 2016).

In addition to criminal behavior, the reasons for the frequent occurrence of network security incidents also lie in people's weak awareness of personal information security risks, their insufficient attention to network security and a lack of network security knowledge (Liang, 2017). To pursue profits, commercial companies and software operation companies constantly collect personal information. Due

*Corresponding address: No. 41, Zhongyuan Middle Road, Zhengzhou 450007, China. Email: xiaohjin@yeah.net.

to internal leakage, technical loopholes, network viruses and network attacks by criminals, personal registration information is facing a significant threat (Wu, 2017). Social media information dissemination is fast, two-way, open and convenient. While information dissemination provides great convenience, due to the limited ability of personal judgment, it leads to the dissemination of false information, which has a serious negative impact on society and individuals (Tang, 2018). Some functions of social software increase the risk of information disclosure, such as a *location-sharing service* exposing the user's location and *viewing nearby people* which provides location services for others. Criminals can analyze the user's location information, judge the user's home and work address, as well as the user's activities and rest rules (Han et al., 2017).

Internet fraud, personal safety and property losses caused by social network information leakage are increasing, which has a negative impact on the healthy development of the Internet (Wu, 2018). Improper or inappropriate speech which violates the laws, customs and the morals of the state, often leads to a serious violation of personal safety (Han and Lin, 2020). Smart phones provide the hardware basis for the development of mobile social networking and contain a large amount of personal information, such as an address book, SMS, mobile payment account information and phone records. Once mobile phone information is leaked, it has the potential to seriously breach personal information security (Sun, 2018; Dong et al., 2009; Zheng et al., 2016; Vojković et al., 2020; Murire et al., 2021). Through the risk classification of common social software functions, this paper analyzes the unsafe factors of Internet social information dissemination and proposes countermeasures and suggestions.

2. SOCIAL SOFTWARE FUNCTION AND RISK ANALYSIS

According to the statistical report on China's Internet development, the social application WeChat the highest utilization rate of 85% and the utilization rate of QQ and microblogging is also high, indicating that the use of online social software has become a part of people's daily lives and people use online social software to communicate with the outside world every day.

Social communication on the Internet takes social software as the carrier. Taking Tencent QQ, WeChat and microblogging as examples, this paper analyzes the functions and potential unsafe factors of all social software. An instant chat can be carried out when both parties are good friends. If someone's account is stolen, a fraudster may pretend to be a good friend and look for various excuses to ask for money. The person whose account has been compromised may think the fraudster is a friend in trouble and is likely to extend a helping hand, but by the time they discover they have been cheated, it is too late. An online video can be used for a video chat, but after a person's account is stolen, the fraudster usually uses the friend's video instead of a direct video. The person whose account has been compromised thinks it is a real video from their friend and readily trusts the other party, resulting in property loss. File transmission is hidden and it is easy to spread a Trojan virus and improper information while facilitating file transmission. Information from a circle of friends not only includes daily life information and other information shared by individuals, it is also the main channel for personal information disclosure. However, if other people's information is not verified when it is forwarded, it is easy to spread false information. The comment function is a response to the views of others. In the process of communication, it is also possible to disclose personal information. The private message function is a means of communication between non-friends, which may lead to network harassment. The sharing function is used to share information or network links with others, which may reveal personal information. Also, unreliable links may be Trojan viruses (Yang et al., 2021). The positioning function is a function with high risk. Through the positioning function, personal activities can be tracked which could be a threat to personal safety. The drifting bottle is one of WeChat's friend-finding tools. It is a game between strangers that could result in network harassment. The shake function helps strangers find friends, but there is also a risk of network harassment because once two people have become friends, it is possible for them to obtain information about each other.

An experiment was conducted a few years ago using the WeChat "shake" function to add a stranger as a friend, and both users spent half an hour analyzing 100 pieces of information on each other's circle of friends, and both obtained the following information: their real appearance; their real name; color and registration number of private car; the age of their children and the address of the child's kindergarten and their school hours; the children's appearance, clothes and preferences; and daily activities such as going to parks and cinemas. The payment function is used for shopping payment hence there is a risk of account theft. In relation to online fraud, the existence of the payment function provides a convenient opportunity for fraudsters to steal money. The "people nearby" function allows the user to see people near them and the user will also be seen by the other people. It is also a way for strangers to make friends and there is a risk of network harassment. The functions and risks of several Internet social software applications are shown in Table 1.

3. ANALYSIS OF UNSAFE FACTORS AND CONSEQUENCES CAUSED BY INFORMATION DISSEMINATION

3.1 Data Collection Method

3.1.1 Personal Survey of Internet Users

(1) Total survey China has a residential fixed telephone line (dormitory telephone, home telephone) and those over the age of 6 are allowed to use a mobile phone. Sample size: there are 30000 samples in the survey, which are subdivided as follows:

Sub-population A: People covered by residential fixed telephone (including residents, students' dormitories and other dormitories);

Table 1 Functions and risks associated with of several social software applications.

Function	QQ	WeChat	Micro-blog	Degree of insecurity	Possible risks
Instant chat	√	√		High	Network fraud
Online video	√	√		High	Network fraud
File transfer	√	√	√	Average	Spread inappropriate information and viruses
Circle of friends information	√	√	√	High	Divulging information and spreading false information
Comment function	√	√	√	Low	Divulging information
Private message function	√	√	√	Average	Online harassment
Sharing function	√	√	√	Average	Divulging information, unreliable website links
Positioning function	√	√	√	High	Personal safety
Drifting bottle	√	√		Average	Online harassment
Shake it	√	√	√	Average	Online harassment
Payment function	√	√		High	Network fraud
People nearby	√	√	√	Average	Online harassment

Sub population B: people covered by mobile phones;

Sub population C: people covered jointly by mobile phones and residential fixed lines (the overlapping part of fixed phones and mobile phones), $C = a \cap B$.

(2) Sampling method

The sub-population ABC was investigated and the double sampling frame method was adopted to cover the Internet users to the greatest extent. The first sampling frame is used to investigate sub-population a, and the second sampling frame is used to investigate sub-population B. For the fixed telephone coverage group, the hierarchical two-stage pumping method is adopted, which is divided into 31 layers according to the provincial administration, and each layer takes samples independently. For the mobile phone coverage group, the sampling method is similar to the fixed line telephone. The research method is to extract all mobile phone numbers in each city, combine the effective sample size, generate a certain number of four-digit random numbers, combine them with the mobile phone office number of each city to form a number library, then sort them and dial them randomly.

3.1.2 Automatic Online Search and Statistical Data Reporting

An automatic online search takes technical statistics on a number of websites and the statistical report data is the number of IP addresses. The provincial statistics of IP addresses are from the databases of the Asia Pacific Internet Information Center and the China Internet Information Center. The data registered in the two databases can identify the province to which the address belongs according to the provincial administrative region to obtain the corresponding data. To ensure the accuracy of the IP address data, the China Internet Information Center verifies the data from the Asia Pacific Internet Information Center and determines the number of IP addresses.

3.2 Personal Injury Caused by Personal and Family Information Disclosure

According to the 2020 WeChat data report, in 2020, there were 1205.5 million active WeChat monthly accounts. As shown in Figure 2, from 2015 to 2020, the number of active WeChat monthly accounts continued to grow and the personal use of online social software became a part of daily life. Personal life information is regularly shared on social networks which enables personal information on women and children to be easily found. Children may be subject to malicious retaliation or abduction, while women may be sexually harassed by sexual predators, which may lead to personal injury. Disclosing personal family information reveals the family's address and wealth and the family may face the risk of property theft.

As an example, a woman often shared information about her children in her circle of friends, which almost resulted in her five-year-old daughter being kidnapped and trafficked. Through her circle of friends, a strange woman found out where she and her children live, and the places her children frequent such as dancing lessons due to photos posted of her children participating in literary and artistic performances. The woman claimed to be a good friend of the child's mother and easily obtained the child's trust. Fortunately, the police discovered this situation in time to avoid the child being abducted.

3.3 Personal Information Disclosure can Lead to Network Fraud

Personal information disclosure results in a large proportion of online fraud. Personal information can be leaked in the following ways: employees can illegally resell company information; a computer or mobile phone can be infected with a virus or Trojan software, resulting in the unintended disclosure of personal information; hackers can invade a database to save information and steal data; social networks can disclose personal information. There are various ways

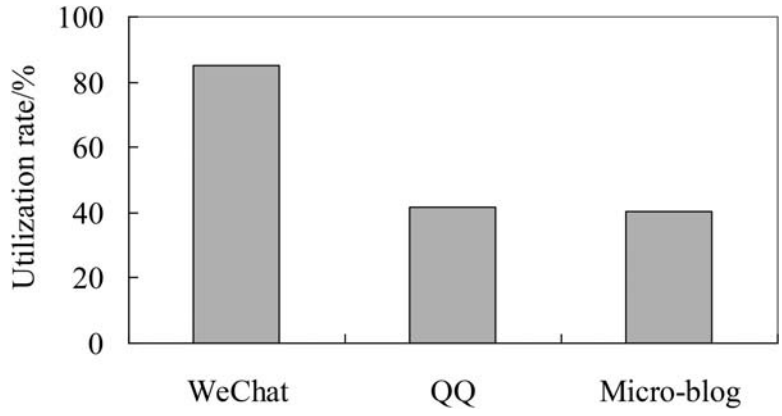

Figure 1 Typical social software usage (2020.06).

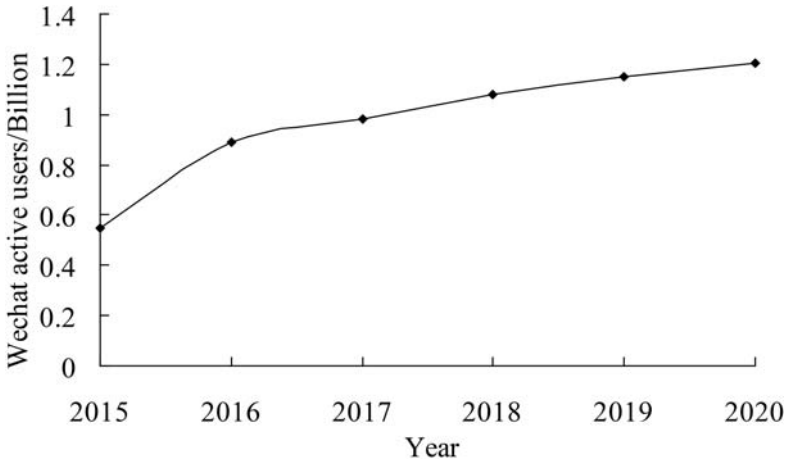

Figure 2 Number of WeChat monthly active accounts.

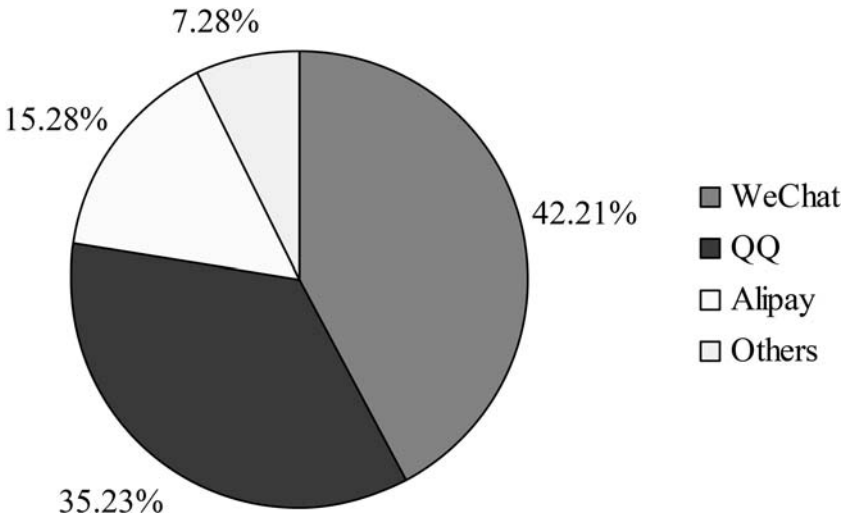

Figure 3 Percentage of social software used as a fraud tool.

to commit fraud, including refund fraud, fraud by posing as public security officers, prosecutors and judges, security account fraud, accident fraud of relatives, fraud by posing as friends, fraud by posing as the manager of a company, winning fraud and fictional kidnapping fraud.

Social networking software is not only a platform for individuals to spread information in real time, it is also a tool for online fraudsters. Between the years of 2016–2018, social networking software has been frequently used for Internet fraud. The proportion of social software which is used as a fraud tool is shown in Figure 3. The most used social software is WeChat, accounting for 42.21% of all social software used, followed by QQ at 35.23%, Alipay at 15.28% (although Alipay's main function is payment, it also has social functions), and other software accounts for 7.28%.

Table 2 Data on the use of personal identity cards for illegal activities(2018.01–2019.08).

Name	Number of ID card cases	Criminal suspect	Dens for manufacturing false certificates	Illegal information of ID card
Number	32000	16000	1900	4460

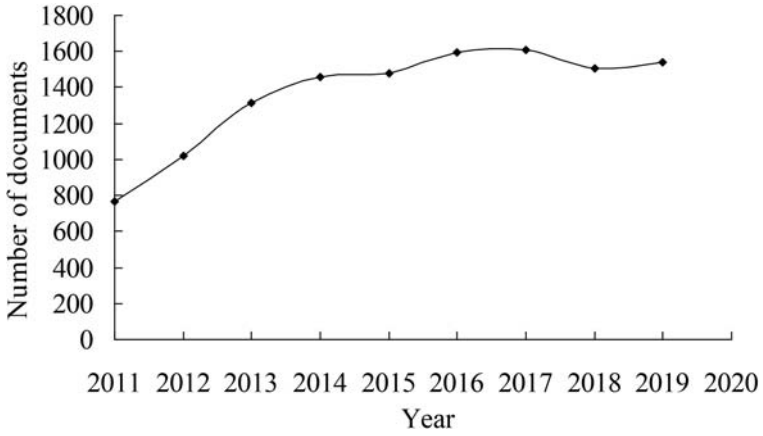

Figure 4 Number of online public opinion documents (China HowNet).

3.4 Personal Information can be Used for Illegal Activities

According to a press conference held by the Ministry of Public Security in August 2019, since 2018, more than 32000 identity cards have been seized and more than 16000 suspects have been arrested. As shown in Table 2, identity cards are sold as fake ID cards, and there are trading chains on the Internet.

Personal ID information may also be leaked via Internet social activities. Some businesses do not need an original ID card, and only need a copy of an ID card. However, copies of ID card is often used for illegal activities: a copy of an ID card can be falsely used for credit card transactions and can be maliciously overdrawn; a copy of an ID card can be falsely used to apply for bank loans or small loans; a company can forge a copy of other people's ID cards for employment purposes, and evade their tax obligations by paying wages; a copy of an ID card can be used to apply for a telephone card to commit telephone fraud.

As an example, a woman unexpectedly received a notification from the bank that her credit card was overdrawn. It turned out that she had mistakenly left a copy of her ID card when applying for a job. The company used the copy of the applicant's ID card to apply for multiple credit cards under a false name to access the woman's capital. Although the identity information of the woman had not been leaked through Internet social channels, it is crucial that people are vigilant to protect their personal information when they socialize on the Internet.

3.5 Personal Inappropriate Remarks may Impact Public Opinion

Public opinion events caused by improper speech showed an increasing trend. From 2011 to 2020, a literature search was conducted on China HowNet with "network public opinion" as the keyword. The number of relevant studies, as shown in Figure 4, increased to 1607 in 2017, which was more than twice that in 2011. Although the number of studies decreased after 2017, it is still at a high level.

Although there is no strict standard to define improper speech, its impact cannot be ignored. Improper speech often has three kinds of effects. First, it has adverse effects, which is inconsistent with the moral standards and social customs recognized by the public, for example, if someone says to their circle of friends, "I really hope the epidemic lasts a little longer, so that the masks we are making at home will continue to sell". Second, it violates people's general value standards and damages the social order, for example, a public security incident caused many deaths, and someone said "good death" to their circle of friends. Third, it runs counter to traditional values and violates the law, such as propagating terrorism, fostering national hatred, endangering national security, etc. As an example, after a girl was killed in a taxi, someone spread insulting remarks on the Internet saying "you deserve what you got because you were wearing skimpy and provocative clothing", which seriously affected society. The man who made the remark was administratively detained.

3.6 Social Accounts can be Stolen for Illegal Activities

Some social accounts are the same as payment accounts. After a person's social account has been stolen, consumption increases and malicious loans are generated. The increased consumption and the loans are often to the maximum amount of the personal accounts, causing serious property losses to the victims. After the account has been stolen, the thieves conduct illegal transactions, sell the account to sell accounts to other people. After some individuals and platforms have purchased the account, they can use it for voting, comment, praise,

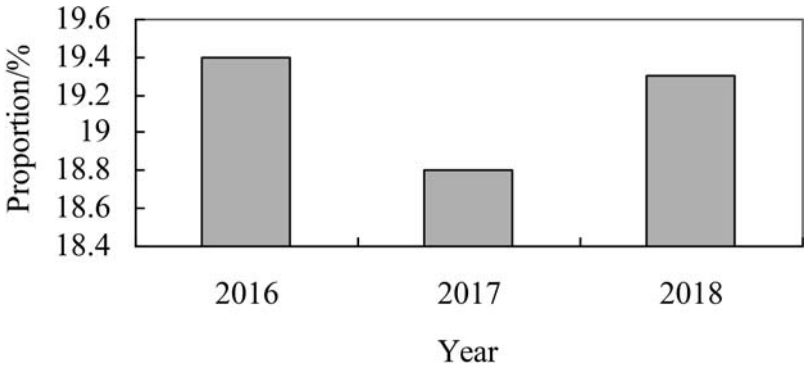

Figure 5 Percentage of online fraud after obtaining personal information.

Table 3 Number of "fake news" reports by media platforms.

Time	Web News	Forum	Newspapers and periodicals	WeChat
First half of 2015	26860	10542	3137	12461
Second half of 2015	35224	11327	2565	12349
First half of 2016	30552	14329	2235	14493

fans, fraud, etc. In addition, after account numbers have been illegally obtained, they can be sold to organizations and individuals whereupon it is possible to carry out more serious criminal activities, such as spreading illegal and harmful information, conducting illegal transactions, increasing traffic to illegal websites, etc. In addition, the stolen account may also be used for malicious marketing to fund illegal interests.

Internet social networking always carries a risk associated with information disclosure which makes it easy for fraudsters to conduct fraud. According to the special report on judicial big data (shown in Figure 5), from 2016 to 2018, the percentage of targeted online fraud compared to all cases of online fraud was 19.4%, 18.8% and 19.2% respectively. It can be seen that as a result of Internet social information dissemination, the disclosure of personal information has serious consequences, fraud prevention awareness is not strong, and there is not enough understanding of the unsafe factors associated with information dissemination.

3.7 Dissemination of False Information

False information is unproven information and can be either malicious or unintentional. The malicious fabrication and dissemination of false information is often aimed at retaliation, increasing data flow and attract attention. The dissemination of false information can have adverse social effects, disrupting social order or causing problems for those involved. For example, the false news about a Shanghai girl fleeing the Jiangxi countryside triggered a fierce regional dispute, which was finally called a public opinion event. The false news emanated from a female netizen, who didn't want to travel to her husband's hometown for the new year to quarrel with her husband. she was feeling extremely anxious, she invented the content and triggered public opinion. To attract attention, two young people in Hangzhou fabricated the incident of "The woman had an improper relationship with the courier". As this information was forwarded many times, this rumor was spread widely on the Internet, damaging the reputations of those involved, which constitutes the crime of defamation.

According to the public opinion channel of renmin.com, there are many media platforms which disseminate false information, of which web news accounts for a large proportion, as shown in Table 3, followed by WeChat and forums. Therefore, in the dissemination of false information, social networking software is an important platform. It is a crime to deliberately fabricate and spread false information on the network or other media as this can seriously disturb social order and violates criminal law. Therefore, in the process of networking, individuals should have the ability to identify false information and avoid spreading false information.

4. COUNTERMEASURES AND SUGGESTIONS

(1) When sharing personal information using Internet social software, care should be taken to avoid disclosing sensitive details such as the family address, family photos, information about children etc. For example, a mosaic can be used to cover key information.

(2) Personal information should not be shared when engaging in Internet social networking to avoid ID card information being used for illegal activities. If one's identity information is used for illegal activities, the police should be informed.

(3) The disclosure of personal information when engaging in Internet social networking can lead to network fraud. This can occur due to the efforts of disgruntled employees, malware or hackers. Therefore, it is important that personal information is kept secure and businesses must ensure the security of their network.

(4) As false or misleading information can damage the social order, care must be taken to ensure that rumors are not spread via social media and that deformation

laws are not broken. Businesses should increase their network security and develop strict codes of conduct for employees.

(5) To prevent account theft, users should ensure their anti-virus software is up to date they should strengthen their security protection level to avoid malware attacks; complex account passwords should be used for multiple authentication; and users should be wary of phishing links.

(6) For the spread of false information, strengthen the supervision of media, microblog and wechat accounts, avoid the rapid spread of false information on the Internet, and promote network legislation. When individuals have serious consequences due to the spread of false information, relevant personnel shall be investigated for legal responsibility.

5. CONCLUSION

(1) An analysis was conducted to determine the percentage of online fraud which occurred from 2016 to 2018 after personal information had been obtained, showing that the risk of online social information dissemination is significant. The specific functions of WeChat, QQ and microblogging were analyzed, and the risk of each was classified to serve as a warning for users of social software.

(2) This paper analyzes the safety concerns associated with information dissemination on Internet social software and it analyzes and gives examples of the harm caused by personal family information disclosure. It discusses how network fraud occurs due to personal information disclosure and how personal information can be used for illegal activities. It also discusses how public opinion is influenced by false and misinformation spread on social software and how social account theft is used for illegal activities.

(3) This paper suggests countermeasures to prevent Internet social software information dissemination and personal information leakage. It also suggests ways to improve account security, Improve personal legal knowledge and relevant legal systems, which requires the joint efforts of individuals, network platforms and governments to achieve good results.

REFERENCES

1. Dong, H., Cheng, G.X., Liu, Z.H. & Zou, H. (2009). Mobile SNS social network tends to be mobile. *Communication World*, *4*(27), 54–55.
2. Han, D.D. & Lin, Y.T. (2020). Improper speech is the highest or will face criminal responsibility. *Citizen and Law (Comprehensive Edition)*, (02), 31–32.
3. Han, Y., Kong, Y.H. & Jiang, J.G. (2017). Security protection and strategy analysis of social software location information. *Security Science and Technology*, (10), 65–67.
4. He, Y.X. & Ji, J.Z. (2021). Analysis of Information Security Risk Defense in the Development of Big Data. *Journal of Physics: Conference Series*, *1881*(3), 66–69.
5. Li, F. & Zhu, J.L. (2021). Network traffic monitoring and real-time risk warning based on static baseline algorithm. *Engineering Intelligent Systems*, *29*(3), 183–189.
6. Liang, R.Y. (2017). Research on network security awareness education of college students. *Guangxi Normal University*.
7. Murire, O.T., Flowerday, S., Strydom, K. & Fourie, C.J.S. (2021). Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa. *The Journal for Transdisciplinary Research in Southern Africa*, *17*(1), 14–18.
8. Murire, O.T., Flowerday, S., Strydom, K. & Fourie, C.J.S. (2021). Narrative review: Social media use by employees and the risk to institutional and personal information security compliance in South Africa. *J. Transdisciplinary Research in Southern Africa*, *17*(1), 44–49.
9. Mutambik, I., Almuqrin, A., Liu, Y.L., Maryah, A. & Fatmah, Q.H. (2021). Gender Differentials on Information Sharing and Privacy Concerns on Social Networking Sites: Perspectives From Users. *Journal of Global Information Management (JGIM)*, *29*(3), 12–18.
10. Sun, Z.B. (2018). Research on Influencing Factors of smart phone users' information security behavior. *Heilongjiang University*.
11. Tang, X.H. (2018). Credibility analysis and evaluation of content in social media. *Southeast University*.
12. Vojković, G., Milenković, M. & Katulić, T. (2020). IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law. *Business Systems Research: International Journal of the Society for Advancing Innovation and Research in Economy*, *11*(3), 57–60.
13. Wu, S.W. (2017). Analysis on information security and protection of mobile social network users. *Communication World*, (04), 49–50.
14. Wu, Y.X. (2018). Research on Influencing Factors of information security of social network users. *Heilongjiang University*.
15. Xu, W.C., Zhu, X.Y., Chen, Z., Chen, J.W. & Yu, Y.C. (2021). Research on the Governance and Control of Personal Information Security in the Big Data Environment–Based on the Comparative Method. *Journal of Social Science and Humanities*, *3*(5), 35–40.
16. Yang, Y.X., Yang, H.F., Wang, J., Liu, R.Y., & Nie, X.Q. (2021). A?5G?network-oriented mobile edge computing offloading strategy and cloud computing network security. *Engineering Intelligent Systems, 29*(2), 109–116.
17. Zhang, Y.X. & Kang, X.R. (2014). Research on personal information security of social networks in the era of big data. *Lantai World*, (05), 24–25.
18. Zhao, Z.Y., Teng, L.C., Chen, Q. & Wang, H.Y. (2016). Research on personal information security of social networks in the era of big data. *Computer Knowledge and Technology*, *12*(24), 44–45.
19. Zheng, W., Pan, Q. & Deng, Y.F. (2016). Link prediction method based on common neighbor network centrality in mobile Social Networks. *Computer Application Research*, *33*(09), 2743–2746
20. Zhong, X.S. (2020). Research on Influencing Factors of information security awareness of social network users. *Shandong University*.
21. Zou, Y.Z. (2017). Users are in a dilemma in the era of big data. *Science and Technology Communication*, *9*(21), 105–106.