Research on Personal Information Security Protection of Social Networks in the Era of Big Data

Xuerong Zuo(✉)

School of Marxism, Hohai University, Nanjing, Jiangsu, China

Abstract. With the advent of the era of big data, there are some new problems in the security protection of personal information on social networks, such as user data privacy leakage, spam and network attacks, network rumors and network public opinion information. In view of the current situation of personal information security protection in social networks, this paper analyzes the hazards and causes of personal information security protection in social networks, and puts forward some protection countermeasures, such as improving the awareness and skills of self-security prevention in social networks, strengthening the self-discipline of social network service providers, strengthening social credit system and information ethics construction, establishing and perfecting relevant laws and regulations.

Keywords: big data · social networks · personal information security protection

1 Introduction

With the advent of the era of big data, social networks have gradually become an important way of communication between people. We are most familiar with domestic social software such as QQ, WeChat, Weibo, Tiktok and Xiaohongshu, while foreign popular social software such as Twitter, Facebook, Instagram and WhatsApp. They have become network tools for hundreds of millions of people to exchange information. Social networks can not only enrich users' daily life, but also use social networks for office and online business. However, with the extensive use of social networks, there are also problems in information security.

2 Types of Personal Information Security Problems in Social Networks

2.1 User Data Privacy Disclosure

User data privacy disclosure can be seen as the most frequent problem of personal information security in social networks, and even lead to the occurrence of network crimes in varying degrees. It belongs to the behavior caused by computer abuse [1, 2]. In the era of big data, users should pay more attention to filling in private information,

J. Yen et al. (Eds.): ICBIS 2023, AHCS 14, pp. 1478–1484, 2023.
https://doi.org/10.2991/978-94-6463-198-2_153

such as mobile phone number, ID card number, bank card account number and other information. If the user does not get professional information security protection after submitting real personal information, it may cause personal information disclosure. Social networks also have proliferation and security violations [3], Criminals can also use other people's true identities to engage in fraudulent activities by stealing numbers, which directly threatens users' property security. For example, in March 2018, Facebook had nearly 100 million users' data leaked, and "Cambridge Analytica" illegally used these data to send political advertisements to the public. As a social software manufacturer, it has a high degree of control over users' information. "Cambridge Analytica" also collected users' test results on "personality" to predict their consumption behavior and political tendency. Even Facebook clearly stipulates in the terms of use of users that the content uploaded by users will directly become the property of the website, which increases the information security risks of social networks.

2.2 Spam and Network Attacks

These spam messages are sometimes accompanied by fraud links and malicious plug-ins. The spam messages are spread wantonly through mass distribution, advertising, and user information purchased from criminals. Network attacks also seriously threaten the security of users' personal information. Criminals usually use malicious code to steal users' personal information. After obtaining personal information, they also use Trojan horse and virus attacks, which has caused very serious consequences to users' information security. For example, with the help of fake base stations, some lawbreakers can send 15000 spam messages to second-class mobile phone users in the area covered by the base stations every 10 min on average. Some mobile apps can easily send spam messages to users directly from the background by setting up programs. The contents of spam messages are various, most of which are advertisements. There are also fraudulent messages sent by posing as public security organs, banks or sellers. Some text messages are also attached with URL links. As long as users click to enter, the bank account information or mobile phone charges bound to the mobile phone will fall into the hands of criminals, causing personal economic losses.

2.3 Network Rumors and Network Public Opinion Information

In the era of big data, network rumors and public opinion information [4] will also bring great security risks to personal information. In addition to the information security problems from the traditional technical level and the user's subjective level, personal information security will also suffer from the dangers of network rumors and negative public opinion information. The main forms of expression include rumor, incitement, speculation, release of malicious information, and trafficking in property rights. At present, the spread of false news and wrong information on the Internet is increasing day by day, and unconfirmed false information can easily lead to mass emergencies and disrupt people's normal life order. For example, in 2011, due to the nuclear accident in Japan, some lawless elements began to spread rumors on the Internet, which caused panic about radiation and "salt grabbing storm" in many areas of China, and caused certain losses to public

Table 1. Types of personal information security problems in social networks

Personal information security problems	Contents
User data privacy disclosure	Phone number, ID number, bank account, etc.
Spam and network attacks	Fraud SMS, malicious plug-in, virus attack, etc.
Network rumors and network public opinion information	Spread rumors, publicity stunt, release malicious information, trafficking property rights, etc.

safety, property and life. Personal information security problems in social networks can be summarized into the following situations, as shown in Table 1.

3 Current Situation of Personal Information Security Protection in Social Networks

According to the report of China Internet Information Center, the proportion of users who do not use social networks is 2.97%, the proportion of information leakage 0 times is 23.58%, the proportion of information leakage 1–5 times is 61.28%, the proportion of information leakage 6–10 times is 5.93%, the proportion of information leakage 11–20 times is 2.31%, and the proportion of information leakage more than 20 times is 3.93% [5]. The survey results show that the personal information of most users with social accounts has been leaked in the era of big data (Fig. 1).

The survey on users' perception of the current situation of personal information security protection in social networks shows that 55.78% of users have the awareness of prevention but have not taken protective measures, 45.51% of users are very worried about the lack of protection of personal information security, 38.64% of users can consciously take measures to protect information security, and 33.82% of users have been

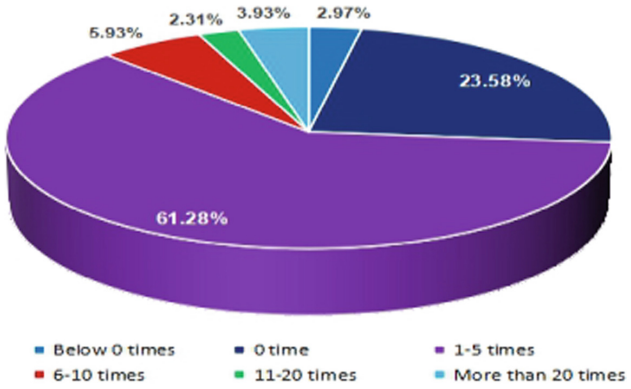

Fig. 1. Statistics of the number of personal information leaks in social networks

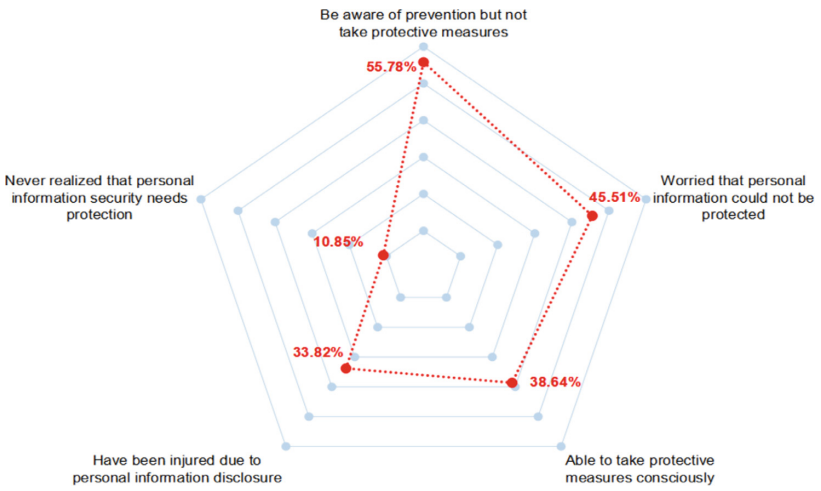

Fig. 2. Users' perception of the current situation of personal information security protection in social networks

injured due to personal information disclosure, 10.85% of users never realize that their personal information needs to be protected [5]. This survey revealed that the current situation of personal information security protection in social networks is relatively serious (Fig. 2).

According to the survey, 76.8% of users think that personal life, study and work are troubled, and even pose a threat to personal security when personal information security is not protected; 56.28% of users believed that it would arouse doubts about web-based applications; 40.3% of users believe that social information ethics has been challenged in terms of moral bottom line; 51.9% of users believed that relevant laws and regulations were provoked; 48.6% of users believe that it will destroy interpersonal communication, which is not conducive to building a harmonious society [5] (Fig. 3).

4 Analysis of the Causes of Personal Information Security Protection Problems in Social Networks in the Era of Big Data

4.1 Personal Reasons for Users: Weak Network Security Skills, Lack of Awareness of Personal Privacy Protection in Social Networks

On the one hand, the current network security education in China is still in progress, and there are weaknesses in individual network security skills. For example, the password setting is too simple, and most people are accustomed to using the number related to personal information as the login password of social networks. Although the simple password is convenient for users to remember, but it is very easy to crack, thus exposing personal information in social networks. On the other hand, users' awareness of personal information security protection in social networks is still lacking. Most people can't identify the true identity of friends in social networks, and are easy to disclose personal information in the chat process.

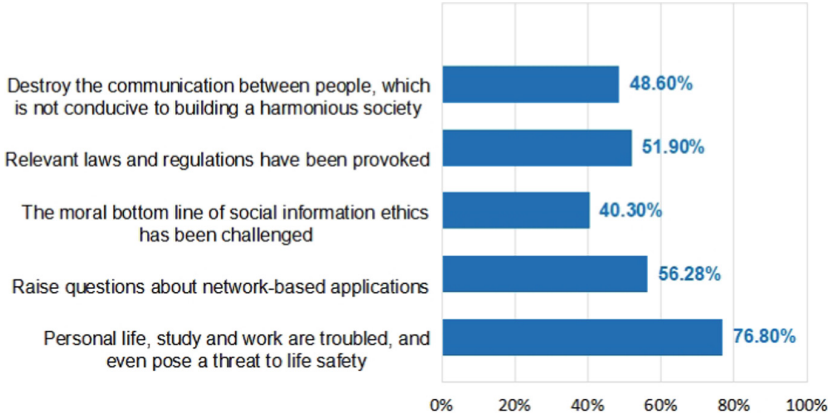

Fig. 3. Statistics of possible hazards caused by unprotected personal information security

4.2 Social Network Service Providers: Lack Industry Self-discipline

The personal information security of social network users and social network service providers are inherently contradictory. In the era of big data, although social network service providers can provide users with more humanized services and experiences, they continue to open social network platforms and introduce third-party application developers, which include the need to collect more personal information while gaining economic benefits. However, excessive collection of personal information of users in social networks is a common reality among current social service providers, which in essence has harmed personal information security.

4.3 Incomplete Laws and Regulations

Compared with the traditional society, the personal information of social networks in the era of big data presents new features of variation in the way of leakage, expansion of information users, combination of economy and spirituality. Therefore, the laws and regulations of traditional society are no longer applicable to the protection of personal information security in social networks in the era of big data. It is necessary to further prevent the abuse of information security policies [6] and information system [7], promote the compliance of information security policies [8, 9].

5 Strategies for Personal Information Security Protection in Social Networks

5.1 Improve the Awareness and Skills of Self-security Prevention in Social Networks

On the one hand, social network users should develop good network application habits, establish a high awareness of the importance of personal information security protection Users' perception of the current situation of personal information security protection

in social networks, carefully abide by the operating rules of social networks, clarify the potential hazards caused by personal information disclosure, and truly implement this network application habit into every step of operation. On the other hand, it is also necessary for users to master certain information security protection measures or security technologies. For example, develop good online social habits and do not open links to unknown websites and unknown emails at will.

5.2 Strengthen the Self-discipline of Social Network Service Providers

Industry norms and industry self-discipline conventions can promote the healthy and long-term development of the industry. To a certain extent, industry self-discipline can effectively make up for the lag of national laws, and can also protect the safety of personal information in social networks and regulate the behavior of social network service providers. Social network service providers should follow the user-centered principle, fully respect the personal information security of social network users, and prohibit private collection, sale and utilization of personal information in social networks.

5.3 Establish and Improve Relevant Laws and Regulations

The existing information protection law is not enough to deal with the new problems related to information security in the era of big data, so it cannot provide users with a comfortable social network environment. It is suggested that the relevant departments should combine the actual situation of China's development and learn from the beneficial experience of personal information security protection in developed countries to continuously improve and develop the current laws and regulations.

6 Conclusions

Personal information security of social networks is an urgent issue in the era of big data. If it cannot be solved properly, it will affect the confidence of users to participate in and use social networks, and seriously endanger the healthy development of China's social economy and network [10, 11]. In the era of big data, the protection of social network personal information security is essentially a very complex systematic project, which not only involves users' awareness of personal information security protection Users' perception of the current situation of personal information security protection in social networks, network information security technology, social information ethics and the improvement of relevant laws and regulations, but also is closely related to our daily life. The above research shows that the most direct and effective way to protect personal information security in social networks is that users themselves truly realize the importance of security protection and can actively master basic information security protection skills, thus reducing personal information security problems in social networks.

References

1. Kling, Rob. Computer abuse and computer crime as organizational activities[J].Acm Sigcas Computer&Society,1981,11(4):12–24.
2. Straub D W,Jr.Effective IS Security: An Empirical Study[J].Information Systems Research,1990,1(3):255–276.
3. Michael, Workman,John,et al.Punishment and ethics deterrents: A study of insider security contravention[J].Journal of the American Society for Information ence and Technology, 2007, 58(2):212–222.
4. Puxing. Research on personal information security of social networks in the era of big data [J]. Information Communication, 2014 (11): 154.
5. China Internet Information Center. 43rd Statistical Report on China's Internet Development [EB/OL]. [2021–09–15]. https://www.cnnic.net.cn/n4/2022/0401/c88-1132.html.
6. Hu Q, Xu Z, Dinev T, et al.Does deterrence work in reducing information security policy abuse by employees?[J].Communications of the Acm,2011,54(6):54–60.
7. D'Arcy J,Hovay A, Galletta D.User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach[J].Information Systems Research,2009,20(1):79–98.
8. Bulgurcu B, Cavusoglu R,Benbasat R.Information Security Policy Compliance:An Empirical Study of Rationality-Based Beliefs and Information Security Awareness[J].Mis Quarterly, 2010,34(3):523–548.
9. Chan M, Woon I,Kankanhalli A.Perceptions of Information Security in the Workplace:Linking Information Security Climate to Compliant Behavior[J].Journal of InformationPrivacy&Security,2005,1(3):18–41.
10. Junheng Wang. Research on personal information security of social networks in the era of big data [J]. China New Communications, 2019, 21 (24): 132.
11. Xueqi Dong. Administrative law protection of personal information in the era of big data [J]. Economist, 2021,384 (02): 57-58.