International Journal of Intelligent Information and Management Science
ISSN: 2307-0692, Volume 8, Issue 2, April, 2019

Investigation and Research on the Impact of Mobile APP Access Rights on Personal Information Security

Jiajie Huo[1], Yan Zhuang[1], Fan Hu[1], Qing Zhao[1], Suzhai Wang[2]
[1]Humanities College Tianjin Agricultural University, Tianjin, 300384, China
[2]College of Marxism Tianjin Agricultural University, Tianjin, 300384, China

Abstract: In the era of mobile Internet, the number of people who use smart phones has increased dramatically. The powerful functions of smart phones are mainly based on the support of various types of APP. At present, the leakage of personal privacy by mobile APP has attracted the attention of government departments and users. There are also many reports on the impact of mobile APP access rights on personal information security. Starting from the various privacy rights involved in the pre-installed APP of smart phones, this paper attempts to discuss the subject, reasons, the current situation of legal system and the improvement of legislation of privacy leakage at present, so as to arouse great attention from all walks of life to the problem of privacy leakage caused by mobile APP, and provide theoretical basis for users to use APP scientifically.

Keywords: Mobile APP; Access rights; Privacy leakage

1. Introduction

Analysis of the results of the online questionnaire survey. The basic information of users. The main methods of this survey are questionnaire and interview. We distributed the questionnaire of "Investigation on Personal Privacy Security Awareness" on the Internet, and received 143 questionnaire responses. The people who filled out the questionnaires were mainly college students, and they accounted for 87.4%. Among the 143 questionnaires, 56 were males, accounting for 39.16%, and 87 were females, accounting for 60.84%. There are 125 people with bachelor degree or above, accounting for 87.41%. The user's age is mainly from 18 to 40, a total of 139 people, accounting for 97.2%.

2. Research Content Feedback

2.1. The privacy security consciousness of users

The survey results show that users generally have a strong sense of privacy security. In this survey, 18.1% and 49.1% of the respondents thought that their privacy security awareness was very strong and strong, from which it can be seen that most people attach great importance to their privacy security. 76.8% of the respondents stored important documents in their mobile phones, but 20.9% of the 76.8% of the respondents do not implemented protective measures for important documents. Important documents are likely to cause information leakage due to the lack of protective measures, causing damage to their property or personal safety.

2.2. User's attitude and cognition to access rights and privacy provisions

When installing the mobile APP, only 9.09% of users will read the privacy protection clause carefully, 34.9% of users will not read it at all and skip it directly. This shows that most people do not pay attention to the privacy protection clause of mobile APP, and this kind of neglect may promote users' privacy leakage by mobile APP. For the access rights of the mobile APP privacy rights, 65.7% of the users allow to open privacy rights such as camera, recording, and positioning to the mobile phone APP according to the situation. And 69.2% of the users are not aware of the reason to open the access rights of mobile phone APP, which shows that most people are more cautious about the privacy-related rights. But for some access rights which are not understood, blind open access rights to mobile APP may increase the leakage of privacy.

2.3. Investigating users' privacy leakage

33.5% of users have experienced serious consequences caused by privacy leakage, 51.7% of users worry about the privacy leakage of mobile phone software and have no way to deal with it. Most of the 143 people have such experience: after searching things by shopping software, there will be relevant recommendations on the browser; after purchasing certain items, they will receive short message reminders from third parties (e.g. merchants); the consumer willingness (e.g. travel, weight loss, beauty, games, etc.) mentioned in chat software will be recom-

mended by browsers; they will also have similar recommendations for other entertainment software, such as certain music videos; and they will receive promotional messages from strangers. 44% percent of users strongly hope that the situation of privacy leakage can be improved. It shows that the current network and mobile phone APP are far from protecting the privacy of users. Even some mobile phone software actively reveals the privacy of users. These data also show that privacy leakage have caused a lot of trouble for users' lives, and even some users have paid the price.

3. Evaluation and Analysis of The Questionnaire Results

3.1. Analysis of users' psychological situation

In this online survey, when asked "some apps (software) will request access to privacy rights (camera, recording, location, reading contacts, etc.)", more than 60% of the respondents answered "it will depend on the situation, if necessary, it will be allowed." However, nearly 70% of the respondents do not know why these apps (software) will request access rights, and they even feel it doesn't matter if they don't know. In addition, more than half of users worry that their privacy will be leaked, but they feel that there is no way to deal with that. Some people even do not worry, and they feel that their privacy information has already been exposed in the network era. In this regard, some people have lamented: "Personal privacy can't be concealed from Internet companies even if it's concealed from the surrounding people."

From this point of view, our privacy protection awareness is still too "dull" for those behaviors and phenomena that are not obvious and potentially invade personal privacy. In the face of the omnipotent Internet, we are relatively passive. It is precisely because we are insensitive to privacy information when it needs to be collected that our personal information is largely collected. The leakage of privacy is largely due to ourselves.

3.2. Reasons for privacy leakage based on users' psychological analysis

3.2.1. Insensitivity of mobile APP users to whether access rights are opened

When the mobile APP pops up requesting access to privacy rights (camera, recording, location, reading contacts, etc.), the users do not carefully analyze the need to open certain privacy rights when using the APP (software). Therefore, some unnecessary access requests are actually opened by ourselves. The first murderer who leaks some private information is actually ourselves!

3.2.2. Other reasons of privacy leakage

(1) Lack of industry supervision. Some software developers are too chasing interests, internal management is not in place, some practitioners are not strong in legal consciousness, some staff seek private interests, resell user information, resulting in personal information leakage "disaster areas".

(2) The imperfection of relevant laws. The case disputes in this field are not absent, and they are getting worse and worse. It is not enough to rely solely on people's moral self-discipline, and strong laws are needed to support it.

4. Solutions to Protect Personal Information Security of Mobile APP Users

4.1. The aspect of mobile APP users

The results of the questionnaire survey show that mobile APP users have a relative high awareness of privacy protection, which needs to be affirmed. Only the ways to protect privacy need to be further strengthened. For property information, more complex password combinations should be set up; in order to prevent privacy leakage caused by mobile phone loss, important information should be backed up in time to ensure personal information security; pay attention to mobile phone usage habits to prevent virus Trojans from entering; do not click on links to unknown web pages, and do not browse unknown websites at will. In a word, it's not wrong to think twice before operating personal information.

4.2. The aspect of relevant industries

The industry standards should be established to regulate the market order of mobile phone software. The protection of personal information in the United States started earlier, we should learn from the industry self-discipline model under the guidance of the government and give enterprises more autonomy. However, for the enterprises, it is necessary to protect the privacy of the users served as much as possible, minimize the impact of reading users privacy on the users, and minimize the collection of users privacy. In addition, it is necessary to regulate the supervision and implementation of users' privacy information, not to do bad business, and not to do things beyond the law.

4.3. Strengthening national legislation

In recent years, China has made a lot of efforts in legal compliance. The Criminal Law Amendment (VII), which was revised and adopted in 2009, regulates the behaviour of illegal stealing, sale, and leakage of personal information. The Criminal Law Amendment (IX) also set the crime of illegally obtaining personal information of citizens. In addition to the Network Security Law of the People's Republic of China promulgated in 2017, the content of personal information protection also appeared in nearly 40 laws, more than 30 regulations and 200 rules and regulations, such as the General Principles of the Civil Law, the Consumer Rights and Interests Protection

Law, the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection. However, it is far from enough to improve the legislation. There should be laws to abide by, enforcement of laws must be strict, law breakers must be dealt with, so as to make legal supervision more operable. Users are given the right to say no, to avoid being "kidnapped" by software developers. Clear the right of users to seek a lawsuit, take corresponding measures to reduce personal losses and change the dilemma of no help.

4. Conclusion

There are still many ways to protect the personal information security of mobile APP users, so there are no more examples here. But only when both individuals and society work together, can we purify the network environment, return network tranquility to users, and return personal information security to everyone.

5. Acknowledgment

College students innovation and entrepreneurship training program (No. 201807016).

References

[1] He R.G., Xuan H.L. Criminal law sword personal information protection, 2009, 5, 16-19.

[2] He P.Y., Wang X.R., Lin Y. On the technical means and coping mechanism of personal information theft in the era of big data, 2018, 5.