An Empirical Study of Factors Influencing Personal Information Security Behavior in Social Networks: Postprint

Authors: Wang Xiwei, Wang Lei, Jia Ruonan, Wang Duo

Date: 2023-08-27T00:00:00+00:00

Abstract

[Purpose/Significance] With the increasing number of social network users, research on personal information security behavior in social networks plays a positive role in helping users better avoid social network security risks and promoting platform developers to improve information security technologies. [Methods/Process] Based on social cognition theory and protection motivation theory, this study constructs a model of factors influencing personal information security behavior in social networks and tests the model's applicability using questionnaire surveys and structural equation modeling. [Results/Conclusions] Data results indicate that response efficacy is the most significant influencing factor of personal information security protection behavior in social networks, followed by perceived threat and self-efficacy positively affecting personal information security protection intention, while avoidance behavior negatively affects information security protection intention; users' information security protection intention positively influences information security protection behavior.

Full Text

Preamble

Volume 62, Issue 18, September 2018

An Empirical Study on the Influencing Factors of Personal Information Security Behavior in Social Networks

Wang Xiwei[1],[2], Wang Lei[1], Jia Ruonan[1], Wang Duo[1]
[1]School of Management, Jilin University, Changchun 130022
[2]Big Data Management Research Center, Jilin University, Changchun 130022

Abstract

[**Purpose/Significance**] With the increasing number of social network users, research on personal information security behavior in social networks plays a positive role in helping users better avoid social network security risks and urging social network platform developers to improve information security technology. [**Method/Process**] Based on social cognitive theory and protection motivation theory, this paper constructs a model of influencing factors of personal information security behavior in social networks, and tests the applicability of the model using questionnaire surveys and structural equation modeling. [**Result/Conclusion**] The results show that response efficacy is the most important factor influencing personal information security protection behavior in social networks, followed by perceived threat and self-efficacy, which positively influence personal information security protection willingness, while avoidance behavior negatively influences information security protection willingness. Users' information security protection willingness positively influences information security protection behavior.

Keywords: social network, personal information security, behavior, influencing factors
Classification Number: G250
DOI: 10.13266/j.issn.0252-3116.2018.18.003

1. Introduction

In recent years, global cyberspace security threats have shown new changes, with some emerging network threats spreading globally. According to Tencent's "2017 Annual Internet Security Report," the field of network security presents both opportunities and challenges, with security incidents such as network attacks, social network information leaks, and fraud emerging endlessly, constantly sounding the alarm for public data and information security [1]. The 41st Statistical Report on China's Internet Development shows that in 2017, the proportion of users who experienced cybersecurity incidents reached 52.6% of all internet users, with 48.4% involving fraud through impersonating friends on social software [2]. Well-known domestic and foreign social network companies such as LinkedIn, Yahoo, and NetEase have all experienced user information theft by hackers, resulting in thousands of user accounts being exploited by criminals. Unsafe information behavior by social network users is the primary cause of personal privacy leaks and theft by illegal elements [3].

With the increase in social network users, personal information security behavior in social networks has become a new issue of concern in both industry and academia. Foreign scholar A. Bandura appropriately studied users' information security behavior through social cognitive theory models [4]; A.C. Johnston and other scholars conducted research when users decide to adopt information security behavior, believing that users' perception of the social environment will affect their behavioral intentions [5]; Y. Chen and other scholars compared

information security behavior from the perspective of individual online security behavior patterns in Chinese and American contexts [6]. Domestic scholar Zhang Xiaojuan, based on privacy concern theory, constructed a model of influencing factors of privacy concern on smartphone users' information security behavioral intention, deeply studying three key influencing factors: trust, privacy risk perception, and past experience [7]; Wang Luyao, based on fear appeal theory, constructed a model of influencing factors of social network users' adoption of privacy security protection measures, studying the influence mechanism of users' personal information security in social networks [8]; Luo Li proposed three effective ways to protect personal information security in social networks, including strengthening legislative protection and industry self-regulation, improving the information security management level of social network enterprises, and enhancing users' information security literacy [9].

From the existing research results of domestic and foreign scholars, most current achievements focus on user privacy security protection and comparative studies of information security behavioral intentions between East and West, but there are relatively few studies on users' information security behavior in social networks, especially regarding the impact of "avoidance behavior" on users. This study attempts to address three research questions: the influencing factors of users' information security behavior in the context of social networks; the role of avoidance behavior on users' information security behavior; and to verify the practicality of the social network information security model constructed in this paper through empirical research.

This paper constructs a model of influencing factors of users' information security behavior in social networks based on social cognitive theory and protection motivation theory, providing a new theoretical perspective for research on personal information security behavior in social networks and helping social network users better avoid security risks in practice.

2. Related Concepts and Theoretical Foundations

2.1 Social Networks and User Personal Information Security

Social networks (SNS) are the gridding of social relationships. The social networks discussed in this paper refer to online platforms that use real-name systems as the main feature and aim to establish and manage personal or institutional social relationships [9]. Most foreign definitions of social networks refer to them as a service based on the Internet platform that enables users to create their own online space, establish their own circle of friends, and provide public or semi-public social tools for strangers or friends to browse, comment on, and forward [10]. In China, Weibo, WeChat, and QQ Space are predominantly used as social network tools, while Twitter and Facebook are typical representatives abroad.

Personal information security of social network users mainly refers to users' own information security issues. Personal age, gender, religious beliefs, ways of

thinking, motivation, and cultural background all affect social network users' personal information security. With the rapid development of the Internet, many hackers have evolved from "intrusion for showing off skills" to later "hacker economy" [11], and the frequent occurrence of risky links and online fraud in social networks has made human factors increasingly prominent in influencing personal information security behavior in social networks.

2.2 Social Cognitive Theory and Social Network Security Behavior

Social cognitive theory (SCT) holds that social psychology is stored in human minds in a certain structure, with interrelationships between the structure and its parts. At the same time, individuals' acquisition of knowledge is usually influenced by the external social environment and personal experience. Its core viewpoint is the "triadic reciprocal" determinism, which means that environment, behavior, and person have dynamic interactions, influencing and depending on each other. B.E. Holt, the proposer of social cognitive theory concepts, believes that all human behavior is based on meeting the psychological needs of "feelings, emotions, and desires" [12]. Among them, self-efficacy is an important concept in social cognitive theory, referring to the confidence level of users in deciding whether they have the ability to actively deal with problems during the assessment process [5, 13].

A. Inkeles believes that people in modern Western society have high individualistic principles, with strong self-efficacy in dealing with challenges and tend to adopt proactive attitudes to handle problems [14]. However, when current Chinese users face social network security issues, they often adopt "harmonious" and "avoidance" behaviors [15]; traditional Chinese culture has also always emphasized "collective response" and "reliance on authority" to deal with various risks [16]. Currently, many domestic scholars have ignored exploring social network users' information security behavior from the perspective of "avoidance," so this paper introduces "avoidance" as an independent variable into the model, combined with social cognitive theory to jointly discuss users' information security behavior.

2.3 Protection Motivation Theory and Social Network Security Behavior

The protection motivation theory (PMT) framework is divided into three parts: information source, cognitive mediation process, and coping mode. It specifically refers to the process of explaining behavioral change through threat assessment and coping assessment in the cognitive regulation process, on which basis individuals make corresponding decisions. The theory believes that information sources influence information behavior. R.W. Rogers once used it to study security behavior, believing that threat assessment and coping assessment are the two most important factors in protection motivation theory. Threat assessment reflects individuals' evaluation of threat susceptibility and threat severity, while

coping assessment reflects individuals' evaluation of self-efficacy and response efficacy [17].

When users face personal information security risks brought by social networks, they first judge the possibility of experiencing this threat and the severity of harm caused by this threat, and then adopt behaviors that they personally believe can effectively avoid the threat. In addition, H. Liang and Y. Xue and other scholars believe that perceived susceptibility and perceived severity can influence security behavioral intention through the mediating variable of perceived threat, so they introduced perceived threat into the protection motivation theory model [13]. Many scholars have proven through several experiments that protection motivation theory plays an important role in studying social network user behavior. In view of this, this paper, by sorting out relevant foreign literature on information security behavior and using questionnaire surveys and structural equation methods, aims to address the influencing factors of information security behavior in social networks and provide references for related research.

3. Research Model and Questionnaire Design

3.1 Literature Review

3.1.1 Influence of Perceived Threat in Social Networks on Personal Information Security Protection Willingness Perceived threat in social networks refers to when users perceive harmful content or risks in social networks and take corresponding measures to deal with them. P.A. Rippetoe and other scholars believe that when users' perception of information security threats intensifies, individuals will adopt more active behaviors to get rid of the threat [18]; H. Liang and other scholars believe that perceived threat plays a positive role in adopting protective behaviors [19]. However, there are obvious differences between Eastern and Western users regarding social network content, and users in different societies choose different strategies to deal with social network threats [20]; Chinese users have relatively weaker personal information security protection awareness compared with European and American countries in the rapidly developing Internet society, making it difficult for them to distinguish which content is threatening when facing different content on social networks, leading to violations of user information security [21]; H. Liang and other scholars also believe that perceived threat can be introduced as a variable into the protection motivation theory model. If social network users believe that the probability of information security risks is high but they don't believe it will bring serious threats to themselves, or they believe that information security risks are serious but the probability of happening to themselves is extremely low, then they may not generate information security protection willingness. Only when users actually perceive information security risks can they possibly generate information security protection willingness [13]. Therefore, based on the above literature research results, this paper believes that perceived threat in social networks positively influences social network users' personal information

security protection willingness.

3.1.2 Influence of Response Efficacy in Social Networks on Personal Information Security Protection Willingness Response efficacy in social networks refers to users' cognition of the behaviors they adopt. In other words, if users believe that the behavior measures they adopt are useful, they will adopt this behavior earlier. Many users have never used security scanning software or only used pirated software to scan the websites they use, making them more vulnerable to information security threats [22]; using effective technical tools can greatly reduce the risks of users using social networks, such as regularly changing social network platform passwords, using firewalls, and regularly backing up systems [23]; C. Yoon and other scholars believe that response efficacy positively influences information security behavioral intention [24]; K. Witte believes that response efficacy evaluation is a cognitive process in which individuals form thoughts about their ability to respond to threats, and individuals' final cognition of response efficacy determines how they deal with threats [25]. Only by believing in the effectiveness of information security behavior and believing that security behavior is beneficial to information security will individuals generate the willingness to adopt this behavior. If individuals do not believe that the behavior is effective, even if they are worried about information security, they may not necessarily have the willingness to protect or adopt information security protection behaviors. Therefore, based on the above literature research results, this paper believes that response efficacy in social networks positively influences social network users' personal information security protection willingness.

3.1.3 Influence of Self-Efficacy in Social Networks on Personal Information Security Protection Willingness Self-efficacy in social networks refers to a person's ability to engage in a certain behavior and achieve expected results in the specific context of social networks. It largely refers to individuals' own feelings about their relevant abilities, that is, their confidence in their own success in using social networks. Self-efficacy is a core part of social cognitive theory and protection motivation theory. Many scholars have confirmed through research that self-efficacy has a great influence on information security intention behavior. J. Schaubroeck and other scholars believe that the inequality of information quality between Eastern and Western society members caused by cultural differences plays an important role in self-efficacy [26]; M. Workman and other scholars believe that users with high self-efficacy are more inclined to adopt information security protection behaviors when using the Internet [27]; A.C. Johnston and others, combining protection motivation theory, believe that since social network users need to conduct threat assessment when receiving privacy security protection measures, and user behavior itself is easily influenced by their own environment, self-efficacy will positively influence users' information security intention behavior [5]. Individuals with high self-efficacy are often confident when adopting information security behaviors. Similarly, if individuals have high self-efficacy in social networks, it will be more conducive to adopting

information security behaviors. Therefore, based on the above literature research results, this paper believes that self-efficacy in social networks positively influences personal information security protection willingness.

3.1.4 Influence of Avoidance Behavior in Social Networks on Personal Information Security Protection Willingness Avoidance behavior in social networks refers to refusing to use social networks to varying degrees, especially sensitive operations such as online payment in social networks, to prevent user information security risks in social networks. The role of avoidance behavior is similar to the herd effect. Many users' personal behaviors in social networks are unconsciously influenced by the behavior of most people, regardless of whether this behavior is correct or not. H. Liang and other scholars describe users' avoidance behavior as a normal positive feedback cycle that enables users to comprehensively understand information threat avoidance [13]; Y. Chen and other scholars believe that avoiding using the Internet to varying degrees is a coping strategy for information security, defining avoidance as a coping behavior that prevents information security threats by not using social networks [6]. T. Hamamura and other scholars believe that Easterners have stronger avoidance willingness than Westerners [28]. Influenced by traditional culture, many Chinese users have always hoped to avoid directly facing information security issues in social networks. On social network platforms, online fraud is common, and Chinese users, because of their relatively small personal wealth, are more likely to worry about threats and avoid using social networks. If a social network user believes that most people protect their own information security by refusing to use social networks, then he will have stronger resistance to information security protection willingness. Therefore, based on the above literature research results, this paper believes that avoidance behavior negatively influences social network users' personal information security protection willingness.

3.1.5 Influence of Personal Information Security Protection Willingness on Personal Information Security Protection Behavior in Social Networks Information security protection willingness refers to the motivation to adopt information security protection behavior. In this study, we do not distinguish between willingness and motivation. Willingness is users' psychological tendency to use social networks, which also includes users' behavioral tendency to use social networks. F. Kujur and other scholars found that in social networks, usage willingness, information content, risk, and entertainment affect users' behavior of using social networks, but users' willingness to use social networks is the most critical factor affecting usage behavior [29]; I. Ajzen believes that intentional behavior is a powerful predictor of actual behavior, which can guarantee the realization of behavior to the greatest extent [30]; E.V. Gool and other scholars, through studying teenagers' information sharing behavior on social networks, found that teenagers' willingness to share information is the most critical variable affecting teenagers' active information sharing behavior on social networks [31]. Therefore, consistent with previous research by other

scholars, we believe that users with stronger information security protection willingness are more likely to adopt behaviors to protect personal information security. Based on the above literature research results, this paper believes that information security protection willingness positively influences social network users' information security protection behavior.

3.2 Research Model

Based on the research hypotheses proposed above, this paper takes the self-efficacy variable from social cognitive theory and the perceived threat and response efficacy variables from protection motivation theory as the foundation, introduces the new variable of avoidance behavior as the independent variable of the entire model, uses user information security behavioral willingness as the mediating variable, and uses user information security behavior as the dependent variable to construct a theoretical model of influencing factors of personal information security behavior in social networks, as shown in Figure 1 [Figure 1: see original paper].

To test the causal relationships between latent variables, this study adopts structural equation modeling as the data processing method and uses confirmatory factor analysis to test the reliability and validity of the data.

3.3 Questionnaire Design

To ensure the credibility of the empirical research results, this paper, referring to the research results of Y. Chen [6], Zhang Xiaojuan [32], and other scholars, designed a questionnaire suitable for influencing factors of social network personal information security behavior. The questionnaire includes two parts: the first part has 6 questions for sample basic information; the second part has variable questions, with a total of 6 variables, each variable designed with 5 questions, totaling 30 questions. The questions adopt a 7-level Likert scale form, with each item consisting of a set of statements. Before large-scale distribution, the author conducted a pre-survey to correct problems in the questionnaire, such as professional terms being difficult for respondents to understand, ambiguous question expressions, and low discrimination of question options. Finally, the questionnaire was distributed on a large scale. This survey targeted young people who use social networks as the survey object and recruited respondents through various social media platforms.

4. Empirical Research

4.1 Data Collection and Research Methods

During the survey process, 450 questionnaires were distributed. After identification and screening, 385 valid questionnaires were obtained, with an effective recovery rate of 85.6%. Among the respondents in this survey, there were more females than males, accounting for 61.0% and 39.0% respectively; the age group

of 18-30 years old had the most respondents, accounting for 76.1%; the education level of undergraduate had the most respondents, accounting for 66.8%; the occupation of student had the most respondents, accounting for 53.2%; the length of time using social networks of more than 6 years had the most respondents, accounting for 47.5%; the frequency of using social networks 7 times per day had the most respondents, accounting for 32.7%. Specific statistics are shown in Table 1 .

4.2 Confirmatory Factor Analysis

Confirmatory factor analysis was conducted on the measurement model constructed in this paper. Through Cronbach's α coefficient test, the data has reliability (Cronbach's $\alpha > 0.7$), and further data analysis can be conducted. The correlation matrix between variables is shown in Table 2 . From the data in Table 2, it can be seen that the square root values of AVE for each factor are greater than the correlation coefficients in their respective columns and rows, indicating that the various factors in this study have good discriminant validity.

As shown in Table 3 , the standardized factor loadings for each item of perceived threat, response efficacy, self-efficacy, avoidance behavior, information security protection willingness, and information security protection behavior are between 0.738-0.889, all greater than 0.7. The CR values are 0.887, 0.912, 0.921, 0.913, 0.928, and 0.909 respectively, all greater than 0.7. The AVE values are 0.612, 0.675, 0.699, 0.678, 0.722, and 0.668 respectively, all greater than 0.5, indicating that each factor has good convergent validity.

4.3 Model Testing

This study used AMOS software for structural equation modeling to verify the relationships between these variables. According to the hypotheses of this study, a complete structural equation model to be verified was established based on the proposed conceptual model. After inputting the data, the structural equation model shown in Figure 2 [Figure 2: see original paper] was obtained. The model fit indices are shown in Table 4 .

From the statistics in Table 4, it can be seen that the fit indices of the theoretical model basically meet the standards, and the model fit is good. As shown in Table 5 , perceived threat has a significant positive impact on information security protection willingness ($\beta = 0.279$, $p < 0.001$), and the hypothesis is supported; response efficacy has a significant positive impact on information security protection willingness ($\beta = 0.406$, $p < 0.001$), and the hypothesis is supported; self-efficacy has a significant positive impact on information security protection willingness ($\beta = 0.250$, $p < 0.001$), and the hypothesis is supported; avoidance behavior has a significant negative impact on information security protection willingness ($\beta = -0.158$, $p < 0.001$), and the hypothesis is supported; information security protection willingness has a significant positive impact on

information security protection behavior (β = 0.644, p < 0.001), and the hypothesis is supported.

5. Discussion and Analysis

From the data results in the above charts, it can be seen that the hypothesis testing results are all supported by data. The data analysis results show that information security protection willingness positively influences information security protection behavior (β = 0.64). The coefficients of positive influence of external latent variables on social network users' information security protection willingness are, in order, response efficacy (β = 0.41), perceived threat (β = 0.28), and self-efficacy (β = 0.25). Among them, social network users' avoidance behavior has a negative influence on information security protection willingness (β = -0.16).

5.1 Influence of Response Efficacy on Social Network Users' Information Security Protection Willingness

Social network users' response efficacy positively influences information security protection willingness, with an influence coefficient of 0.41 and a significance P-value < 0.001, meeting the significance requirement. This data result shows that users' response efficacy indirectly influences users' information security protection behavior by influencing information security protection willingness. This conclusion has a certain degree of consistency with K. Witte's research on information security intention. He believes that because users form thoughts about their ability to respond to threats during the response efficacy evaluation process, users' final cognition of response efficacy determines how they deal with threats [25].

This data analysis result shows that if users recognize that using some security scanning software or other social network security protection tools, or understanding social network security policies, can help users detect or reduce security risks in social network usage, then users are more willing to use social networks. Therefore, social network platforms should enhance cooperation with security scanning modules, protect users' personal information security, provide security risk warnings, improve social network security protection policies, and standardize social network platform security management systems and establish user personal information security guarantee mechanisms, thereby reducing security risks in social network usage. In addition, government and industry regulatory platforms should also publicize the importance of personal information security to social network users and improve users' means, tools, and operational guidance for information security protection and privacy protection through training. This can not only form positive information security protection behavioral willingness but also better promote the construction of information security and privacy protection related systems.

5.2 Influence of Perceived Threat on Social Network Users' Information Security Protection Willingness

Social network users' perceived threat positively influences information security protection willingness, with an influence coefficient of 0.28 and a significance P-value < 0.001, meeting the significance requirement. This data result shows that users' perceived threat can help users automatically resist friend requests from unknown people in social networks, preventing personal information from being stolen and tampered with by malicious people, playing a relatively important role in users' information security protection. This result has certain similarity with Zhang Xiaojuan's research, which treats perceived threat as a positive factor influencing users' information security intention and believes that stronger information security intention leads to stronger motivation to adopt information security behavior [7].

This data analysis result shows that in the process of users using social networks, perceived threat will positively influence the recommended information security risk avoidance solutions. Introducing the threat assessment process can make users identify with the cognition of security protection behavior efficacy, further having a positive effect on their willingness to adopt security protection behavior. Currently, young people and elderly people are vulnerable user groups in social networks, with relatively weak perceived threat ability, and they are easily credulous of strangers. Young people often meet netizens through social networks, threatening their personal safety; elderly people easily leak personal account and privacy information through social networks, threatening their financial security. It is particularly important for the national and industry levels to strengthen the perceived threat ability of vulnerable groups in social networks. Governments and enterprises should focus on strengthening training and publicity guidance for vulnerable groups' information security protection, making vulnerable groups aware of potential risks in social networks during usage and adopt appropriate self-protection mechanisms and establish risk prevention awareness.

5.3 Influence of Self-Efficacy on Social Network Users' Information Security Protection Willingness

Social network users' self-efficacy positively influences information security protection willingness, with an influence coefficient of 0.25 and a significance P-value < 0.001, meeting the significance requirement. This data analysis result shows that self-efficacy plays a key role in users' information security protection willingness. This conclusion is consistent with the research conclusions of scholars such as M. Workman, who believe that users with high self-efficacy are more inclined to adopt information security behavior when using the Internet [27].

This data analysis result shows that users' self-efficacy in social networks is mainly reflected in their ability to flexibly master various operational skills in social networks, identify and deal with various security threats encountered,

and understand social network security guidelines. Therefore, for social network platform operators, to ensure the daily active volume of the platform, they must fully consider the ease of use, functionality, and practicality of the social network platform, enabling users to protect personal information security through simple operations. At the same time, network social platform operators should also do a good job in corresponding guidance to help reduce users' various possible information security and personal privacy leakage risks, and prevent various possible security hazards through simplified and easy-to-use self-risk protection operation functions and risk warning functions in social network platform design and information security protection technology, helping users avoid various risks and hidden dangers that may occur during platform usage, thereby allowing more users to use social networks.

5.4 Influence of Avoidance Behavior on Social Network Users' Information Security Protection Willingness

Social network users' avoidance behavior negatively influences information security protection willingness, with an influence coefficient of -0.16 and a significance P-value < 0.001, meeting the significance requirement. This data analysis result shows that avoidance behavior has a negative impact on users' information security willingness. This hypothesis also supports previous research views, such as scholar H. Liang and others who pointed out in related research that people's avoidance motivation is closely related to the behaviors they adopt [13]; in addition, Y. Chen and other scholars concluded through research that influenced by traditional culture, avoidance is a very common behavior in China [6], so it can be seen that avoidance behavior has a direct impact on users' information security behavior in social networks.

Social network platforms are different from traditional social means, with many characteristics such as immediacy, extensiveness, communicability, and risk. With the rapid development of informatization, users in various regions have more contact with social networks. Since most users lack the ability to identify the authenticity of online information, fraud and privacy leakage on social networks occur frequently, causing many users to adopt avoidance behavior of refusing to use social networks to protect their own privacy and financial security. In the information age, this part of users has the risk of being marginalized. Facing potential information security threats in social networks, the majority of users can effectively fight back by enhancing their own information security self-protection literacy and risk identification literacy, as well as using some security scanning tools; social network tools should strengthen the development of network information security protection technology.

5.5 Influence of Information Security Protection Willingness on Social Network Users' Information Security Protection Behavior

Social network users' information security protection willingness positively influences information security protection behavior, with an influence coefficient of

0.64 and a significance P-value < 0.001, meeting the significance requirement. In the social network environment, users' information security behavior is mainly determined by their willingness. Social network users' perceived threat, response efficacy, self-efficacy, and avoidance behavior indirectly influence social network users' information security protection behavior through users' information security protection willingness. Among them, willingness plays a good mediating variable role. This conclusion is consistent with the research of foreign scholar H. Liang and others in the field of information security behavior, that is, the stronger users' information security willingness when using social networks, the more likely they are to adopt information security behavior [13].

This data analysis result shows that social network platforms need to convey the current situation and importance of information security to the majority of users, making users aware that appropriate behavior helps protect personal information security. In addition, users should actively learn knowledge about other aspects of information security, actively accept personal information security training, carefully read relevant privacy agreements when using social networks, know privacy setting methods, and form personal information protection awareness. At the same time, society should also strengthen information security legislation. For example, the "Cybersecurity Law" implemented on June 1, 2017, is an important measure to enhance information security protection that is endorsed by legal professionals.

6. Research Conclusions

The theoretical contribution of this paper lies in constructing a model of influencing factors of social network users' information security behavior based on social cognitive theory and protection motivation theory, and analyzing the influencing factors of social network users' information security behavior. The data analysis results show that perceived threat, response efficacy, and self-efficacy in social networks have direct positive effects on users' information security protection willingness; avoidance behavior has a negative effect on information security willingness and an indirect effect on information security protection behavior; information security protection willingness is the mediating variable of the social network personal information security behavior influencing factor model. This study provides a new behavioral analysis model for research on users' information security behavior in social networks.

The practical value of this paper lies in using structural equation modeling and questionnaire survey methods to explore the influencing factors of social network personal information security behavior. Empirical analysis shows: users should recognize and use personal information security protection tools to reduce security risks in social network usage; introducing the threat assessment process can make users identify with the cognition of security protection behavior efficacy; network social platform operators should also do a good job in corresponding guidance to help reduce users' various possible information security and personal privacy leakage risks; facing potential information secu-

rity threats in social networks, the majority of users can enhance their own information security self-protection literacy and risk identification literacy.

This study also has certain limitations. In the study, the empirical research sample mainly came from university students, who generally use social networks for a long time every day, while samples from other ages and occupations are relatively few, which may affect the universality of the influencing factors of this study for different groups. In subsequent research, the author will expand the scope of survey objects to better verify the applicability of the model to different groups. At the same time, the influencing factor model will appropriately increase variables in future research to increase the granularity of model analysis.

References

[1] Tencent Technology. 2017 Annual Internet Security Report [EB/OL]. [2018-01-19]. http://tech.qq.com/a/20180119/012161.htm.
[2] China Internet Network Information Center. 41st Statistical Report on China's Internet Development [EB/OL]. [2017-01-22]. http://www.cac.gov.cn/2018-01/31/c_{1122347026}.htm.
[3] Meng Xiaoming, He Wei. Personal Privacy Protection in the Commercial Development and Utilization of Social Network Big Data [J]. Library Forum, 2015(6): 67-75.
[4] BANDURA A. Human agency in social cognitive theory [J]. American psychologist, 1989, 44(9): 1175-1184.
[5] JOHNSTON AC, WARKENTIN M. Fear appeals and information security behaviors: an empirical study [J]. MIS quarterly, 2010, 34(3): 549-566.
[6] CHEN Y, ZAHEDI FM. Individuals' Internet security perceptions and behaviors: polycontextual contrasts between the United States and China [J]. MIS quarterly, 2016, 40(1): 205-222.
[7] Zhang Xiaojuan. Research on the Influence of Privacy Concern on Smartphone Users' Information Security Behavioral Intention [J]. Information Studies: Theory & Application, 2017(11): 3-10.
[8] Wang Luyao. Research on the Influence of Fear Appeal on Social Network Users' Privacy Security Protection Behavior [J]. Journal of Intelligence, 2016(12): 2-6.
[9] Luo Li. Research on User Personal Information Security Protection in Social Networks [J]. Library Science Research, 2012(14): 36-40.
[10] BOYD DM, ELLISON NB. Social network sites: definition, history, and scholarship [J]. Journal of computer-mediated communication, 2007, 13(1): 210-230.
[11] Liu Zhihui, Zhang Zhiqiang. Author Keyword Coupling Analysis Method and Empirical Research [J]. Journal of Intelligence, 2014(12): 268-275.
[12] HOLT BE, BROWN HC. Animal drive and the learning process, an essay toward radical empiricism [J]. Journal of nervous and mental disease, 1933, 78(5): 586-600.
[13] LIANG H, XUE Y. Avoidance of information technology threats: a

theoretical perspective [J]. MIS quarterly, 2009, 33(1): 71-90.
[14] INKELES A. Becoming modern: individual change in six developing countries [J]. Ethos, 2010, 3(2): 323-342.
[15] Abbassi A. Culture and anxiety: a cross-cultural study [J]. Journal of professional counseling practice theory & research, 2007, 35(1): 2006: 1-26.
[16] WONG PTP, WONG LCJ, SCOTT C. Beyond stress and coping: the positive psychology of transformation [A]//Handbook of multicultural perspectives on stress and coping. New York: Routladge, 2006: 1-26.
[17] ROGERS RW, CACIOPPO JT, PETTY R. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation [A]//Social psychophysiology. New York: Guilford Press, 1983.
[18] RIPPETOE PA, ROGERS RW. Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat [J]. Journal of personality and social psychology, 1987, 52(3): 596-604.
[19] LIANG H, XUE Y. Understanding security behaviors in personal computer usage: a threat avoidance perspective [J]. Journal of the Association for Information Systems, 2010, 11(7): 394-413.
[20] HEPPNER PP, HEPPNER MJ, LEE DG, et al. Development and validation of a collectivistic coping styles inventory [J]. Journal of counseling psychology, 2006, 53(1): 107-125.
[21] Economist intelligence unit. Digital economy rankings 2010 beyond e-readiness [EB/OL]. [2018-01-19]. http://www-935.ibm.com/services/us/gbs/bus/pdf/eiu_{digital}-economy-ranking-2010_{{{final}}_{{web}}}.pdf.
[22] BSA. Sixth annual bsa and idc global software piracy study [EB/OL]. [2018-01-19]. http://www.global.bsa.org/globalpiracy2008/index.htm.
[23] IFINEDO P. Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition [J]. Information & management, 2014, 51(1): 69-79.
[24] YOON C, HWANG JW, KIM R. Exploring factors that influence students' behaviors in information security [J]. Journal of information systems education, 2012, 23(4): 407-415.
[25] WITTE K. Putting the fear back into fear appeals: the extended parallel process model [J]. Communication monographs, 1992, 59(4): 329-349.
[26] SCHAUBROECK J, LAM SS, XIE JL. Collective efficacy versus self-efficacy in coping responses to stressors and control: a cross-cultural study [J]. Journal of applied psychology, 2000, 85(4): 512-525.
[27] WORKMAN M, BOMMER HH, STRAUB D. Security lapses and the omission of information security measures: a threat control model and empirical test [J]. Computers in human behavior, 2008, 24(6): 2799-2816.
[28] HAMAMURA T, MEIJER Z, HEINE SJ, et al. Approach-avoidance motivation and information processing: a cross-cultural analysis [J]. Personality and social psychology bulletin, 2009, 35(4): 454-462.
[29] KUJUR F, SINGH S. Engaging customers through online participation in social networking sites [J]. Asia pacific management review, 2017, 22(1): 16-24.
[30] AJZEN I. The theory of planned behavior [J]. Organizational behavior & decision processes, 1991, 50: 179-211.

[31] GOOL EV, OUYTSEL JV, PONNET K, et al. To share or not to share? adolescents' self-disclosure about peer relationships on Facebook: an application of the prototype willingness model [J]. Computers in human behavior, 2015, 44(3): 230-239.
[32] Zhang Xiaojuan. Research on Smartphone Users' Information Security Behavioral Intention Based on Social Cognitive Theory [J]. Modern Information, 2017(9): 2-5.

Author Contributions:
Wang Xiwei: Proposed research propositions and ideas, wrote and revised the final version of the paper;
Wang Lei: Responsible for paper writing, revision, and data collection;
Jia Ruonan: Assisted in paper collection and organization;
Wang Duo: Translation and processing of English content in the paper.

Nanjing Declaration on Library Development (2018)

At present, socialism with Chinese characteristics has entered a new era, and China's library cause is also entering a new era. The library cause in the new era should have new missions, new goals, and new responsibilities. The vigorous development of scientific research, education, and cultural undertakings, the widespread popularization and application of information and communication technologies, and users' new demands for literature information resources and services have all posed new challenges and provided new development momentum for the library cause. The library cause is also nurturing new vitality and energy.

To re-understand the strategic positioning of the library cause in the new era, accelerate the transformation from traditional libraries to new-era libraries, and give greater play to the new role of libraries, more than 160 library practitioners, theorists, and educators from various types of libraries and library science teaching and research institutions across the country held the "New Era, New Development: Service Efficiency and Legal System" China Library Development High-Level Forum at Nanjing University on June 20, 2018. After discussion, the experts and representatives formed the following consensus and recommendations:

1. **The library cause in the new era has significant responsibilities and a glorious mission.** The library cause in the new era faces both opportunities and challenges. Library colleagues must recognize the development direction, clarify their own positioning, keep pace with the times, reshape their image, have the courage to take responsibility, strengthen their sense of social responsibility, more effectively play their functions, continuously innovate and develop, continuously improve their service efficiency, enhance their social value and contribution, and turn crises into opportunities.

2. **Further strengthen the legal system construction of libraries.** Library regulations are an important guarantee for the sustainable and healthy development of the library cause. The promulgation of the "Public Library Law of the People's Republic of China" is of milestone significance. Governments at all levels and libraries at all levels should perform their duties according to law and promote the development of China's library cause. At the same time, we should continue to promote a good library legal environment construction from both practical and theoretical aspects, promote the introduction of a "Library Law" including various types of libraries, build a complete library legal system, incorporate the library cause into the track of legalization, standardization, and order, and ensure the sustainable and healthy development of the library cause.

3. **Accelerate the research and application of new technologies.** New technologies represented by the Internet, big data, and artificial intelligence help accelerate the realization of libraries' core values and functions. The development of new technologies and their wide application in libraries have already and will continue to promote the development process of the library cause and promote the improvement of libraries' business capabilities and service capabilities. New technologies are the booster and accelerator for libraries to realize their vision and goals. Librarians should actively embrace new technologies, actively absorb and apply new technologies, accelerate the process of new technology application, control new technologies, and use them for our own purposes.

4. **Further strengthen service capacity building.** Providing library services based on different needs, levels, and methods is the core value and fundamental task of libraries. The development of the library cause must adhere to people-oriented principles, adhere to user-centered principles, abide by the library service principles of universality, openness, sharing, and equality, continuously deepen service content, expand service methods, improve service capabilities, and guarantee service effects.

5. **Libraries must follow a high-quality development path.** We should encourage various types of innovation in libraries, pay attention to innovation effectiveness, continuously improve library service efficiency, and increase libraries' own value. Talent is the foundation of libraries' high-quality development. Libraries must attach importance to the construction of various types of talents, strengthen talent echelon and team building. Librarians should love their jobs, be diligent and dedicated, strengthen professional research and professional capacity improvement, and strive to become expert librarians.

6. **Further promote the co-construction and sharing of libraries.** Public libraries, university libraries, and professional libraries should achieve balanced and sufficient development. We should strengthen the top-level design of the library cause, consolidate the basic work of libraries, do a good job in statistics and evaluation according to law, strengthen

exchanges and cooperation between libraries, and collaboratively carry out various business and service work of libraries.

7. **Further give play to multiple forces to run libraries well.** Social forces are important participants in the development of the library cause. With the development of China's economy and culture, more and more people of insight in society are willing to contribute to the library cause. The library community should actively strengthen cross-boundary cooperation with social forces and give full play to the enthusiasm and irreplaceable role of social forces in founding libraries.

8. **Further strengthen library science education and research.** Library science education must live up to its mission, boldly reform the curriculum system, improve the knowledge structure, and encourage expansion based on the core content of the discipline. Library researchers should vigorously advocate research in library science and interdisciplinary subjects, strengthen the standardization of disciplinary terminology and basic theoretical research, and strengthen teaching, scientific research, and new technology application research. We should adhere to the close combination and interaction of theory and practice, attach equal importance to theoretical research, applied research, and technology development, study and solve the main difficulties and existing problems faced by the library cause in its current and future development, promote development through research, and produce more forward-looking research results.

Note: Figure translations are in progress. See original paper for figures.