Research on the Influence of Fear Appeal on APP Users’ Privacy Protection Behavior: An Empirical Study

Peng Zhu\textsuperscript{a}, Jian Hu\textsuperscript{b} and Xingzhen Zhu\textsuperscript{c}
Nanjing University of Science and Technology, Nanjing, 210094, China
\textsuperscript{apzhu@njust.edu.cn, \textsuperscript{b}hujame@njust.edu.cn, \textsuperscript{czhuxingzhen2016@163.com}

Abstract. Under the background of Big Data Era, this paper explores the influencing factors of APP Users’ Privacy Protection Behavior based on the theory of fear appeals. We used scene-based questionnaire to collect the needed data. We found that self-efficacy, fear and response efficacy have a positive impact on APP users to adopt privacy security measures wishes. We did not include other influencing factors such as threat control, fear control and social factors in this study. This paper has some reference and reference significance for APP operators and service providers who provide third-party network security.

1. Introduction
When people benefit from big data, the protection of personal privacy becomes more difficult, and this problem of users' privacy protection is particularly significant in the mobile APP industry with a high degree of platform openness and confusing functions and modules. The privacy and security problems of users exposed by mobile intelligent terminal apps are not only illegal self-starting, private networking, private sending of information, malicious deduction of fees and other operations on mobile terminals. At the same time the APP users' call log, contacts, accounts, passwords, confidential documents, geographical location, Internet records and other data are faced with peer and the risk of theft. Once users' privacy information is leaked, users may not only be harassed by a large number of advertisements, but also face with more deceptive and targeted fraud risks by those with ulterior motives.

For another, in recent years, scholars at home and abroad began to study the impact of the fear appeal theory on users' security protection measures which they took under the background of the Internet, and introduced the fear appeal theory into the information security field (Das, de Wit, & Stroebe, 2003). Shillair et al. (2015) introduced personal responsibility into the theory of protection motivation to explore the influencing factors that encourage online users' safety behavior. Johnston and Warkentin (2010) have confirmed by researching that fear appeals did impact end user behavioral intent to comply with recommended individual acts of security and thus IT users would accept recommendations to comply with security behavior. Based on the protection motivation theory, Chen and Zahedi (2016) underlined the importance of context-sensitive theory building in security research and provided insights into the motivations of individuals' online security behavior in China and the United States.

At present, there are few researches on the fear appeal theory in China. Through the ERP experiment, Yu Guoming, Li Wei, and Li Ying(2009) studied the relationship between the priming fear-appeal messages and the principal messages as well as that between the difference of subjects' Happiness Sense and their processing of the priming messages, The processing differences and the processing
characteristics to target message of three types of priming fear-appeal message have also get measured. Diao wei, Xu Yaoshan, and Li Yongjuan (2010) explored the effect of fear appeal on risky driving behavior (speeding and failure to wear safety belt) and behavioral intent based on EPPM (extended parallel process model). Domestic related research mainly focuses on communication and security analysis, and research on information security is relatively rare.

Based on the theory of fear appeal and the related research of information security management, this paper constructed a research model that APP users adopt privacy and security protection measures to explore the influence mechanism of fear appeal theory on APP users' information security.

2. Theoretical Basis

2.1. Privacy Security and Protection Behavior of APP Users
The research on mobile APP has gradually become an academic focus. Especially in the background of the accelerated development of big data industries and it has gradually become one of the research trends in recent years. The research on mobile apps has gradually become a scholastic hot spot. Especially in the context of the accelerated development of big data industry, the problem of information security and privacy protection of mobile phone users has become more and more prominent, and these problems are mainly concentrated on the privacy protection of APP users.

Enck, Ongtang, and McDaniel (2009) found through research that security configuration bundled with Android applications provides practical means of detecting malicious software. Chin et al. (2011) examined mobile APP interaction and identified security risks in the application component, and they also provided a tool to detect mobile application communication vulnerabilities. Considering the efficiency of analyzing mobile APP permissions, the user's comprehensibility of analysis results, and the effectiveness of user's privacy information protection, Lu YaFeng (2013) designed and implemented a privacy protection method of users. Jian-hua wu, Moran fang, and Li xiang (2012) explored the privacy data protection methods of mobile phone users by designing black and white lists to authorize access to private data, monitoring each process in real time and encrypting private data using an encryption algorithm.

In addition to helping APP service providers take the initiative to protect users' privacy and security from the perspective of technology, there are few relevant studies on promoting user groups to take the initiative to adopt privacy information protection measures. So this paper will study the impact mechanism of the fear appeal theory on the privacy and security protection behavior of mobile APP users to enrich the research field.

2.2. Fear Appeal Theory and Application Model
The fear appeal theory was first proposed by Hovland et al, which stimulates the inner fear of the audience as a driving force to change their behavior. Meanwhile, the theory held that the relationship between fear and the change of the audience's attitude was in an inverted "U" shape, that is to say, the medium level of fear appeal would make the biggest change of the audience's attitude. Based on the research, the fear appeal theory has successively obtained research results such as 'new parallel response model', 'protection motivation theory' and 'fear arousal stage model'. However, the research found that the effect of inverted u-shaped curve could not be verified, so the model was rarely used in empirical research. In the study of the new parallel response model, Witte (1993) divided the mechanism of fear appeal into two independent processes: cognitive perspective and emotional perspective. The protection motivation theory was widely used and Rogers (1983) used cognitive processes to explain the motivational mechanism how users perceive threats and how they respond to threats to reduce the expected negative impact. Meanwhile, Witte (1992) and Rogers (1975) confirmed the threat severity and threat susceptibility as the threat elements of fear appeal respectively in their respective studies.

Fear appeal theory is widely used in the field of communication and medical research. In recent years, foreign scholars have begun to pay attention to the study of fear appeal theory in information security management. However, there are relatively few studies on information security management in China.
3. Conceptual Model and Empirical Design

3.1. Conceptual Model and Hypotheses
Rogers (1975) made a detailed description of the threat control process in the research, that is, when the individual obtained the efficacy of the product, he also feels the threat from the two dimensions of severity and susceptibility, when the individual's feeling of efficacy and threat are both at a high level, the individuals self-protection motives are activated and he will make the corresponding changes. In addition, the research results of Witte (1993) in the new parallel model theory were similar to those of Rogers, he held that when individuals with fear appeals were afraid of the outcome of a threat assessment, the effectiveness assessment would make individuals take actions to control danger or fear.

When APP users receive the fear appeal of personal information security protection measures, they will conduct self-assessment of threat degree and risk control feedback. The users' self-protection process caused by this fear appeal and the APP users' privacy security threat research conducted are similar to the model proposed and its study on spyware threats (Johnston and Warkentin, 2010). In his research, Johnston has verified that threat perception and threat severity are negatively correlated with self-efficacy and response efficiency in the situation of information security, while both self-efficacy and response efficiency have positive effects on behavioral intent. Therefore, this paper takes the model of Johnston and Warkentin as the basis to establish a conceptual model of fear appeal and APP users' privacy and security protection behavior to verify the impact of fear appeal on APP users' privacy and security protection behavior.

Boss et al. (2015) extended the protection motivation theory. Through the empirical research on information security behavior of MBA students, the results showed that threat severity and threat susceptibility were positively correlated with behavioral intent in the situation of higher fear appeal. Combined with the research results, the study introduces the factors of panic perception based on Johnston's model, in order to verify whether the threat severity and threat susceptibility would affect the app users' fear appeal (see Table 1 for H1b and H2b). Meanwhile, the influence path of H4 is added in the model to verify the influence of panic perception on the behavioral intent of APP users in this background.

![Figure 1. Conceptual model of APP users' privacy and security protection behavior](image)

Table 1. Summary of research hypotheses

| Serial number | Assumed content |
|---------------|-----------------|
| H1a           | Threat severity positively affects the self-efficacy of APP users |
| H1b           | Threat severity positively affects the fear of APP users |
| H1c           | Threat severity positively affects the response efficacy of APP users |
| H2a           | Threat susceptibility negatively affects the self-efficacy of APP users |
| H2b           | Threat susceptibility positively affects the fear of APP users |
| H2c           | Threat susceptibility negatively affects the response efficacy of APP users |
| H3            | Self-efficacy positively affects the behavioral intent of APP users to protect privacy |
| H4            | Fear positively affects the behavioral intent of APP users to protect privacy |
| H5            | Response efficacy positively affects the behavioral intent of APP users to protect privacy |
3.2. Empirical Design

The empirical design of this study includes two parts: information description design and questionnaire design for mobile APP users' privacy and security protection behavior by fear appeal. The design of fear appeal information is based on Johnston's experimental design and combined with the characteristics of mobile APP users' privacy protection in the background of big data. The design of fear appeal information, adding a description of the role of fear perception, is based on Johnston's experimental design and combined with the characteristics of mobile APP users' privacy protection in the background of big data. The questionnaire designed 18 measurement items in total and employed the five-point variable method of Lickter to investigate the interviewer's personal basic information and APP users' experience of using privacy protection measures. Respondents in this study need to have basic ability and experience of independently using mobile apps(such as WeChat, baidu map, Meituan takeaway, etc.) and a basic understanding of privacy and security protection of mobile apps. Before conducting the main survey, this study conducted pre-tests and tested 20 respondents with experience in using phone apps in the early stage. Respondents were asked to comment on a range of questions related to the structure item, including the presentation of the scale, the length of the device, and the format of the questionnaire. Finally, in order to reduce possible expression ambiguity, we selected 50 respondents from a group of APP users for pilot test, and the test results showed that the reliability and validity of the scale were acceptable.

Table 2. Structure definitions

| Structure        | Definition                                                                 | Source                  |
|------------------|---------------------------------------------------------------------------|-------------------------|
| Threat severity  | The severity perceived subjectively by the audience that a threat will     | Rogers (1975)           |
|                  | cause harm to oneself                                                    |                         |
| Threat susceptibility | The probability perceived subjectively by the audience that a threat      | Rogers (1975)           |
|                  | will occur on oneself                                                     |                         |
| Self-efficacy    | The ability perceived subjectively by the audience that they successfully| Beck&Frankel (1981)    |
|                  | implement the recommended measures about risk response by themselves     |                         |
| Fear             | The degree of fear perceived subjectively by the audience when a threat   | Witte (1992a)           |
|                  | arises                                                                    |                         |
| Response efficiency | The effectiveness of the recommended measures about risk response        | Witte (1996)            |
|                  | perceived subjectively by the audience                                   |                         |
| Behavioral intent | The willingness of audience that they accepts the recommended measures   | Johnston (2010)         |
|                  | about risk response and carry out self-safety protection                 |                         |

3.3. Sample Collection

The experimental data of this study was collected through an online survey of phone app users in Nanjing. Firstly, 517 respondents were collected on the social media platform. Then we would screen the respondents according to the sample requirements and sent out questionnaires to collect data. Finally, we would conduct necessary data cleaning of the collected data.

In order to ensure that the number of samples meets the specified requirements, the research has set a long time for questionnaire collection. From March 25, 2017, a total of 45 days of questionnaire collection was conducted. In addition, if respondents use the same IP address or email account for repeated filling, the content will be filtered out. The contents of the questionnaire are also supplemented with tips which are mainly used to ensure that respondents complete all survey items so as to reduce the number of invalid questionnaires. Finally, 387 valid questionnaires were received in the online survey, among which the effective recovery rate accounted for 82.78% and the effective questionnaire rate accounted for 90.42%. The sample statistical information is shown in table 3. The age of the surveyed group is mainly between 19 and 35 years old; male accounts for 48%; the number of people under the age of 30 accounts for 81%; those with a bachelor's degree or above accounted for 58%; APP Users
with experience in using privacy and security measures are mainly concentrated in these two dimensions (No use experience and Use time is 1 to 2 years or more).

### Table 3. Sample Statistics

| Variables                  | options                     | Number | Proportion | Variables                  | options                     | Number | Proportion |
|----------------------------|-----------------------------|--------|------------|----------------------------|-----------------------------|--------|------------|
| Educational background     | Junior college and below    | 163    | 42%        | Gender                     | Male                        | 186    | 48%        |
|                            | Bachelor degree             | 139    | 36%        |                            | Female                      | 201    | 52%        |
|                            | Graduate degree or above    | 85     | 22%        |                            | No experience               | 136    | 35%        |
| Age                       | Under 20 years old          | 54     | 14%        | Experience in using privacy | 0-6 months                  | 33     | 9%         |
|                            | 21-25 years old             | 151    | 39%        | security measures          | 7-12 months                 | 52     | 13%        |
|                            | 26-30 years old             | 108    | 28%        |                            | 1-2 years                   | 79     | 20%        |
|                            | 31-35 years old             | 43     | 11%        |                            | More than 2 years           | 87     | 23%        |
|                            | More than 35 years old      | 31     | 8%         |                            | Valid samples: 387          |        |            |

4. Data Analysis and Hypothesis Test

4.1. Descriptive Statistics

Table 4 displays the mean and standard deviations of the structures. On the whole survey participants seem to pay less attention to behavioral intent, which may indicate that the APP users' awareness of privacy protection is weak.

### Table 4. Descriptive statistics (mean and standard deviation)

|                          | Mean  | Standard deviation |
|--------------------------|-------|--------------------|
| Threat severity          | 4.080 | 0.883              |
| Threat susceptibility    | 3.940 | 0.862              |
| Self-efficacy            | 3.370 | 0.938              |
| Response efficiency      | 3.590 | 0.877              |
| Fear perception          | 3.830 | 0.910              |
| behavioral intent        | 3.610 | 0.753              |

4.2. Analysis Strategy of Model Evaluation

In order to evaluate the normality of the data, we first use the skewness and kurtosis for a single-factor normality test. The result shows that the absolute values of skewness and kurtosis of all variables are less than 2 (table 5), it indicates that the data in this study is very close to normal distribution. In addition, Mardia coefficient is used in this paper to evaluate the multivariate normality of sample data. In this study, Mardia coefficient was lower than 360 (p(p+2), p=18). Therefore, the data hypothesis in this study satisfies the multivariate normal distribution. Considering the sample size, data normality and the characteristics of evaluation methods, the study would use the maximum likelihood method for model analysis.

4.3. Model Test

The measurement model was tested by confirmatory factor analysis (CFA). According to previous research, measurement models should be evaluated and modified before evaluating structural models. After redefining the contents of the questionnaire, we retained 18 questions (table 5). The data indicates that the reliability of these problem options exceeds the minimum acceptable value (0.5), and the internal consistency of the measurement model can be obtained by calculating the comprehensive reliability.
The comprehensive reliability of all question items exceeded the benchmark (0.60), and the value of average variance extracted exceeded the threshold value (0.5). The above three reliability values are higher than the recommended threshold, so the scale evaluating the structure is considered to have sufficient convergence reliability. Table 6 shows that the square root of the average variance extracted are greater than the correlation coefficient between latent variables, which indicates that the discriminant validity of the questionnaire is good. In summary, the measurement result of the model test is satisfactory.

The purpose of model adaptive degree test is to measure the degree of conformity between the hypothetical model and the actual observation data. In this study, the adaptation index of the model is divided into three categories: absolute adaptation index, value-added adaptation index and contracted adaptation index. Table 7 shows the test of the overall adaptive degree of the model. On the whole, both the absolute adaptation index and contracted adaptation index meet the requirements, and the result is satisfactory.

In addition, the study evaluates the multicollinearity problem by variance inflation factor. we make regression analysis by taking behavioral intent as the dependent variable and the other five variables as independent variables. The results show that VIF is between 1.178 and 2.889, so there is no obvious multicollinearity problem.

### Table 5. Measurement reliability, Comprehensive reliability and Average variance extracted

| Measurement item | Skewness | Kurtosis | Reliability | Comprehensive reliability | Average |
|------------------|----------|----------|-------------|---------------------------|---------|
| Threat severity  | TSEV1    | -0.589   | 0.968       | 0.902                     | 0.912   |
|                  | TSEV2    | -0.638   | 1.548       | 0.869                     | 0.763   |
|                  | TSEV3    | -0.531   | 0.336       | 0.818                     |         |
| Threat susceptibility | TSUS1 | -0.139 | -0.141 | 0.819 | 0.942 | 0.879 |
|                  | TSUS2    | 0.011    | -0.262      | 0.948                     |         |
|                  | TSUS3    | -0.068   | -0.211      | 0.955                     |         |
| Threat susceptibility | TSUS1 | -0.139 | -0.141 | 0.819 | 0.942 | 0.879 |
|                  | TSUS2    | 0.011    | -0.262      | 0.948                     |         |
|                  | TSUS3    | -0.068   | -0.211      | 0.955                     |         |
| Self-efficacy    | SEFF1    | -0.431   | 1.216       | 0.841                     |         |
|                  | SEFF2    | -0.459   | 0.836       | 0.838                     | 0.894   |
|                  | SEFF3    | -0.613   | 1.671       | 0.931                     | 0.736   |
| Response efficiency | RESP1 | -0.186   | -0.424      | 0.824                     |         |
|                  | RESP2    | -0.013   | 0.218       | 0.937                     | 0.937   |
|                  | RESP3    | -0.058   | -0.169      | 0.962                     | 0.851   |
| Fear perception  | FEAR1    | -0.054   | -0.357      | 0.923                     | 0.943   |
|                  | FEAR2    | -0.057   | -0.321      | 0.918                     | 0.827   |
|                  | FEAR3    | -0.352   | 0.283       | 0.881                     |         |
| behavioral intent | BINT1   | -0.697   | 0.716       | 0.904                     | 0.911   |
|                  | BINT2    | -0.688   | 1.058       | 0.806                     | 0.747   |
|                  | BINT3    | -0.625   | 0.719       | 0.893                     |         |

### Table 6. Discriminant validity

|                     | Threat severity | Threat susceptibility | Self-efficacy | Response efficiency | Fear perception | behavioral intent |
|---------------------|-----------------|-----------------------|---------------|---------------------|-----------------|-------------------|
| Threat severity     | 0.78            |                       |               |                     |                 |                   |
| Threat susceptibility | 0.26           | 0.83                  |               |                     |                 |                   |
| Self-efficacy       | 0.34            | 0.22                  | 0.73          |                     |                 |                   |
| Response efficiency | 0.09            | 0.28                  | 0.12          | 0.76                |                 |                   |
| Fear perception     | 0.29            | 0.37                  | 0.24          | 0.25                | 0.81            |                   |
| behavioral intent   | 0.33            | 0.28                  | 0.27          | 0.17                | 0.41            | 0.82              |
### Table 7. Analysis of the overall model adaptive degree

| Adaptation index          | Research result | Sources                        |
|---------------------------|-----------------|--------------------------------|
| Absolute adaptation index |                 |                                |
| X2/d. f. (p-value)        | 2.871 <5        | Schumacker & Lomax (2011)      |
| GFI                       | 0.879 >0.8      | Seval & Rahman (2002)          |
| AGFI                      | 0.863 >0.8      | Segars & Grover (1993)         |
| RMSEA                     | 0.055 <0.1      | Browne & Cudec (1992)          |
| Value-added adaptation index |                |                                |
| NFI                       | 0.923 >0.9      | Hair et al (1998)              |
| CFI                       | 0.939 >0.9      | Bentler (1990)                 |
| IFI                       | 0.918 >0.9      | Bentler & Bonett (1980)        |
| Contracted adaptation index |                |                                |
| PNFI                      | 0.767 >0.5      | Mulaik et al (1989)            |
| PCFI                      | 0.734 >0.5      | Mulaik et al (1989)            |

### 4.4. Path Analysis of Model

Figure 2 shows the estimation results of path coefficient. Combined with the research hypothesis, we can conclude that H1a, H1b and H1c are supported as threat severity has a significant positive impact on self-efficacy ($\beta=0.608$), fear ($\beta=0.261$) and Response efficiency ($\beta=0.641$) and their p values are significant. Similarly, H2b are supported as threat susceptibility also has a significant positive effect on fear ($\beta=0.563$, P<0.001). The path coefficient of threat susceptibility to self-efficacy is -0.079 and P value is significant, so H2a is true. The path coefficient of H2c is -0.023(P=0.364>0.05), so the hypothesis does not hold. The path coefficient of self-efficacy, fear emotion and response efficacy to behavioral intention are 0.339, 0.457 and 0.203 respectively, and P value are all significant, so H3, H4, H5 is true.

![Figure 2. Analysis results of the structural model](image_url)

In order to compare the influence of the privacy protection experience of mobile APP users under different background of using experience on their behavioral intent, the sample was further divided into experienced and inexperienced users to explore the behavioral differences between the two groups. The result is that there are 136 people with privacy protection behavior and 251 with no relevant experience.

In this study, two independent structural model analyses were performed for these two groups of participants. As shown in Figure 3, for experienced users, we found that the threat severity still has a positive impact on self-efficacy ($\beta = 0.679$) and response effectiveness ($\beta = 0.615$), and P values were all significant. But threat severity has no significant positive effect on fear. The path coefficient of threat susceptibility to self-efficacy was -0.132, P value was significant and it still had negative influence. However, the positive effect of threat susceptibility on fear is not significant, nor does it have significant effect on response efficiency. In addition, self-efficacy ($\beta=0.327$) and response efficacy ($\beta=0.276$) still have positively effect on behavioral intent, and P values were all significant. Meanwhile, the influence of fear on behavioral intent ($\beta=0.706$, P<0.001) was more significant.
As shown in Figure 4, for inexperienced users, threat severity has a positive effect on self-efficacy ($\beta=0.582$), fear ($\beta=0.413$) and response efficiency ($\beta=0.656$), and P values were all significant. Threat susceptibility has negative influence on self-efficacy ($\beta=-0.067, P<0.001$). The positive effect of threat susceptibility on fear ($\beta=0.814, P<0.001$) was significantly increased and threat susceptibility has no significant effect on response effectiveness. In addition, self-efficacy ($\beta=0.343$) and response efficacy ($\beta=0.189$) still positively affect behavioral intent, and P values were all significant. However, the positive influence of fear on behavioral intent was significantly reduced ($\beta=0.378, P<0.001$).

5. Conclusions and Prospects
Based on the fear appeal theory and combined with the development characteristics of mobile users' privacy security under the background of big data, the study constructs a model of influencing factors which mobile APP users' behavioral intent of adopting privacy and security protection measures, and it deeply explores the influencing factors of APP users' behavioral intent of adopting privacy and security protection measures. The conclusion is as follows.

First of all, the perceived threat that the fear appeal brings to the APP user can have an impact on users' efficiency. The threat severity perceived by users will positively affect the user's efficiency perception of the recommended protection scheme. So the threat assessment process plays a positive role in promoting APP users to adopt privacy protection measures.

Secondly, users' threat susceptibility has a negative impact on self-efficacy, but its impact is limited. It indicates that the sensitivity of APP users to threats in the fear appeal has little impact on the efficacy of protective measures they accept. So we can directly influence and increase users' adoption intentions by enhancing descriptions of threat susceptibility in the fear appeal.
Thirdly, the user's self-efficacy and response efficiency have a direct positive impact on the behavioral intent of adopting protective measures, which indicates that enhancing the effectiveness, convenience and easy operating of the recommended protective measures will greatly improve the user's self-efficacy, response efficiency and behavioral intent. The result also shows that the fear appeal brings to the APP user also has a significant positive impact on users' fear, and the increase of fear emotions can further increase the willingness of APP users to adopt privacy protection measures, which is more obvious in the background of big data.

Finally, there are differences in the determinants that affect the intention of adopting APP users' privacy protection measures between APP users with experience in privacy protection and inexperienced APP users. For experienced users, threat severity and threat susceptibility do not have significant positive effects on users' fear, while for inexperienced users, threat severity and threat susceptibility have significant positive effects on users’ fear. In addition, the fear of experienced users has a more significant positive impact on the adoption intention of privacy protection measures of APP users than that of inexperienced users. This study suggests that the reason for this result may be that APP users with experience in privacy protection are not sensitive to fear, but once they feel fear, such users will have a higher willingness to adopt privacy protection measures, but inexperienced users are the opposite.

The study further expanded the theoretical scope of fear appeals. The research results have certain reference value for mobile APP operators and service providers that provide third-party mobile network security. Meanwhile, APP operators can use advertisement of fear appeal to improve users’ willingness of adopting security protection measures and related service software, so they can gain users' satisfaction and trust of APP environment and improve their competitiveness. However, there are still some deficiencies in the study. In the follow-up research, we will introduce other influencing factors (such as threat control, fear control and social factors) to further explore the influencing mechanism of APP users' privacy and security protection, and we also will further study the impact of other factors of fear appeal on users' information security protection behavior.

Acknowledgments
This research was supported by National Natural Science Foundation of China(71874082), Ministry of Education Humanities and Social Sciences Project of China (18YJA870021), Social Science Fund of Jiangsu Province, China(16TQC005) and University Philosophy and Social Sciences Project of Jiangsu Province, China(2016SJD870005).

References
[1] Das E H, de Wit J B, Stroebe W. Fear appeals motivate acceptance of action recommendations: evidence for a positive bias in the processing of persuasive messages [J]. Personality and Social Psychology Bulletin, 2003, 29 (5): 650-664.
[2] Ruth Shillair, Shelia R. Cotten, Hsin-Yi Sandy Tsai, Saleem Alhabash, Robert LaRose, Nora J. Rifon. Online safety begins with you and me: Convincing Internet users to protect themselves [J]. Computers in Human Behavior, 2015, 48.
[3] Johnston A C, Warkentin M. Fear Appeals and Information Security Behaviors: An Empirical Study [J]. Mis Quarterly, 2010, 34 (3): 549-566.
[4] Chen Y, Zahedi F M. Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China [J]. Mis Quarterly, 2016, 40 (1): 205-222.
[5] Yu Guoming, Li Wei, Li Ying. Fear appeal: the communication effect of ERP experimental research —— a communication research based on neuroscience [J]. Journal of International Communication, 2009 (1): 40-46.
[6] Diao wei, Xu Yaoshan, Li Yongjuan. Influence of fear appeal on safe driving attitude and behavioral intention of professional drivers [J]. China Safety Science Journal, 2010, 20 (11): 36-41.
[7] Enck W, Ongtang M, McDaniel P. On lightweight mobile phone application certification [C].
Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009: 235-245.

[8] Chin E, Felt A P, Greenwood K, et al. Analyzing inter-application communication in Android [C]. International Conference on Mobile Systems, Applications, and Services. ACM, 2011: 239-252.

[9] LuYaFeng. Protecting User's Privacy by Analyzing the Combination of Application's Permissions on Android System [D]. Nanjing university, 2013.

[10] Jian-hua wu, Moran fang, Li xiang. Android users' privacy protection system [J]. Information network security, 2012 (9): 50-53.

[11] Hovland, CarlIver. Communication and persuasion [M]. Communication University of China Press, 2013.

[12] Tan Zhong. The Research of Fear Appeals Theory and Application in Advertisements Communication [D]. Sichuan university, 2006.

[13] Witte K. Message and conceptual confounds in fear appeals: The role of threat, fear, and efficacy [J]. Southern Communication Journal, 1993, 58 (58): 147-155.

[14] Rogers R W. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation [M]. Social Psychophysiology: A Sourcebook. 1983.

[15] Witte K. Putting the fear back into fear appeals: The extended parallel process model [J]. Communication Monographs, 1992, 59 (4): 329-349.

[16] Rogers R W. A protection motivation theory of fear appeals and attitude change1 [J]. The journal of psychology, 1975, 91 (1): 93-114.

[17] Johnston A C, Warkentin M. Fear Appeals and Information Security Behaviors: An Empirical Study [J]. Mis Quarterly, 2010, 34 (3): 549-566.

[18] Boss S R, Galletta D F, Lowry P B, et al. What do systems users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors [J]. Mis Quarterly, 2015, 39 (4): 837-864.