Research on Victims' Acceptance Intention of Fraudulent Information and Sharing Behavior in Telecom Fraud Contexts (Postprint)

Authors: Li Hui

Date: 2023-04-01T16:02:48+00:00

Abstract

[Purpose/Significance] Based on the theory of individual information behavior motivation, an in-depth investigation into the mechanisms of interaction among various influencing factors throughout the process of victims' willingness to accept fraud information and their subsequent sharing behavior holds significant importance for the prevention of telecom fraud crimes. [Method/Process] Grounded in the logical framework of the "motivation-opportunity-ability" (MOA) model, a theoretical model was constructed to examine victims' fraud information acceptance willingness and sharing behavior from three dimensions: motivational factors, opportunity factors, and ability factors. Utilizing IBM SPSS 23.0 and AMOS 23.0 statistical software, empirical analysis and data processing were performed on 1,398 victim survey samples through questionnaire surveys and multiple statistical regression methods. [Results/Conclusion] Gender and marital status exert significant influences on victims' willingness to accept fraud information. Motivational factors—including the perceived "authoritativeness" of false information, trust in fraud perpetrators, and personal profit-driven mentality—serve as crucial driving forces behind victims' acceptance willingness. Victims' self-efficacy and cybersecurity identification capability demonstrate significant positive and negative effects on acceptance willingness, respectively, and both significantly and positively moderate the relationship between fraud information acceptance willingness and sharing behavior. Additionally, victims' smartphone dependence and individual time cost significantly and positively moderate this relationship. The findings suggest that combating telecom fraud requires a multi-pronged approach: strengthening regulation of false information, celebrity endorsements, and various media; enhancing victims' cybersecurity identification capabilities; and preventing irrational investment in smartphone-based network finance.

Full Text

Preamble

Vol. 65 No. 7 April 2021

Research on Victims' Willingness to Accept Fraud Information and Their Sharing Behavior in the Context of Telecom Fraud

Li Hui
School of Police Administration, People's Public Security University of China, Beijing 100038

Abstract: [Purpose/Significance] Based on theories of individual information behavior motivation, an in-depth examination of the mechanisms underlying victims' willingness to accept fraud information and the influencing factors in their information sharing behavior is crucial for developing effective telecom fraud prevention strategies. [Method/Process] Grounded in the "motivation-opportunity-ability" (MOA) model framework, this study constructs a theoretical model examining how victims' motivational, opportunity, and ability factors influence their willingness to accept fraud information and their subsequent sharing behavior. Using IBM SPSS 23.0 and AMOS 23.0 statistical software, empirical analysis and data processing were conducted on 1,398 victim survey samples through questionnaire surveys and multiple regression analysis. [Result/Conclusion] Gender and marital status significantly affect victims' willingness to accept fraud information. The "authority" of false information, trust in fraud perpetrators, and victims' own greed for profit are key motivational drivers. Victims' self-efficacy and cybersecurity identification ability exert positive and negative effects respectively on their fraud information acceptance willingness, and both significantly moderate the relationship between acceptance willingness and sharing behavior. Smartphone dependence and individual time costs also significantly moderate this relationship. The findings suggest that combating telecom fraud requires multi-pronged approaches, including strengthening supervision of false information, celebrity endorsements, and various media platforms, enhancing victims' cybersecurity identification capabilities, and preventing irrational investment in smartphone-based financial services.

Keywords: telecom fraud; fraud information; victim; acceptance willingness; sharing behavior

Classification Number: G252.7
DOI: 10.13266/j.issn.0252-3116.2021.07.009

With the rapid development of telecommunications networks and increasing smartphone penetration, telecom fraud crimes—including online lending, financial mutual aid, and virtual currency scams—have surpassed traditional criminal offenses in both case volume and impact, becoming a high-incidence "disaster area" for new types of crime in China. Due to the strong concealment, wide

geographical span, and technical investigation difficulties of telecom fraud, post-incident crackdowns and asset recovery remain challenging, with victims often suffering devastating financial losses that severely affect social stability. Cases such as the "E Zu Bao" mass fraud incident, involving numerous victims and substantial losses, can easily trigger collective petitioning events that may directly challenge government credibility if mishandled. Given these characteristics, scientific prevention has become key to curbing telecom fraud, shifting research focus from post-incident investigation to pre-incident prevention and examining the underlying causes of victimization.

Current research primarily focuses on three aspects: (1) Examining relationships between objective characteristics and victimization behavior. Findings on gender differences remain inconsistent—some studies suggest male victims outnumber females, others indicate women face higher victimization risk, while some find no significant gender differences. Geographic factors show no significant correlation with fraud amount, methods, or fund transfer channels, though victims exhibit high mobility and dispersion. Regarding age, while fraud losses typically correlate positively with age, findings diverge on age distribution among victim populations, with some research indicating the 19-40 age group predominates due to greater social resources and exposure to online lending and investment scams, while other studies based on 2009 Ministry of Public Security data suggest higher victimization rates among middle-aged and elderly populations. (2) Investigating psychological characteristics and victimization. Analyses follow two main paths: the "vulnerability-trust" model, which posits that victims' vulnerable psychology enables perpetrators to gain trust and transmit false information, and the "profit-seeking-risk-avoidance" model, which categorizes victim psychology into profit-seeking and risk-avoidance motives that perpetrators exploit after establishing trust. (3) Examining environmental characteristics and victimization. Research shows residents in poor public security communities and non-full-time workers are more vulnerable, as they are perceived as "easier targets" and have more time at home to receive fraudulent calls.

Two key limitations persist in existing research: First, findings remain controversial without a systematic theoretical framework. While studies have examined demographic, psychological, and environmental factors, no comprehensive theoretical framework has emerged to explain the deep causes of victimization, particularly from the essential perspective of "why victims accept fraud information." Second, quantitative empirical research remains scarce, with most studies relying on qualitative analysis and few employing multivariate regression for causal quantitative analysis, especially large-sample studies revealing fundamental patterns of fraud information acceptance.

Addressing these gaps, this study uses large-sample data to examine victims' willingness to accept fraud information and the underlying mechanisms driving them to share this information with others, tackling two critical prevention challenges: (1) Why do victims accept fraud information, and what factors drive this willingness? (2) Under what circumstances do victims share accepted in-

formation with others, "infecting" potential victims, and what factors constrain this sharing behavior?

2 Theoretical Model and Research Hypotheses

2.1 MOA Model and Telecom Fraud Victims' Fraud Information Sharing Behavior

The MOA model, originally proposed by D.J. MacInnis and B.J. Jaworski, provides a comprehensive theoretical framework for explaining individual information behavior motivation. The model posits that motivation, opportunity, and ability jointly determine individuals' information acceptance and processing behaviors. Motivation represents the direct driving force for action ("whether one wants to do it"), opportunity refers to restrictive environmental factors affecting motivation and behavior ("whether circumstances allow it"), and ability denotes the skill level required to drive behavior ("whether one can do it"). These three factors interact to trigger individual behavior, with motivation directly influencing behavior while opportunity and ability moderate the motivation-behavior path.

The MOA model has demonstrated strong explanatory power across various domains, including consumer advertising information processing, public relations management, community participation, organizational social capital, knowledge sharing, and health rumor dissemination. This study argues that the model similarly explains telecom fraud victims' information acceptance willingness and sharing behavior. In the context of telecom fraud, victims' sharing behavior can be viewed as an information acceptance response directly driven by motivations such as perceived false "authority" of fraud information, trust in perpetrators, and profit-seeking psychology. The model also explains how factors like physical environment (smartphone media), temporal environment (time costs), cybersecurity prevention ability, and self-efficacy influence the motivation-to-behavior process. Furthermore, it provides a comprehensive framework for depicting victims' information acceptance motivation and sharing behavior patterns.

2.2 "Do They Want To?"—Motivational Analysis of Victims' Fraud Information Acceptance Willingness

Motivation refers to the expression of willingness, interest, and desire to process information—an internal inducement that transforms into behavior when activated. In telecom fraud contexts, when victims cannot identify information as fraudulent, they become "captured" by false packaging, perpetrators' persuasive tactics, and their own greed. Three key motivational factors emerge:

First, from the fraud information perspective, perpetrators often exploit authoritative departments, media, or celebrities to package and disseminate false information, using this "authority" to hook targets and stimulate internal motivation. **H1a: The stronger the false information's "authority," the stronger the victim's fraud information acceptance willingness.**

Second, from the perpetrator perspective, fraudsters frequently interact with victims through "small favors," establishing interpersonal trust before executing the final deception. Based on trust transfer theory, once victims trust the perpetrator, this trust transfers to the fraudulent products or services being promoted. **H1b: Higher trust in perpetrators strengthens victims' fraud information acceptance willingness.**

Third, from the victim psychology perspective, most victims harbor greedy intentions, gradually falling into irreversible deception traps while pursuing "small profits." **H1c: Stronger profit-seeking psychology intensifies victims' fraud information acceptance willingness.**

2.3 "Are They Allowed To?"—Opportunity Factors' Influence on Fraud Information Sharing Behavior

MOA model opportunity factors refer to external environmental elements beyond the actor's control that facilitate or inhibit behavior in specific spatiotemporal contexts—situational factors influencing the motivation-to-behavior transition. In telecom fraud, two opportunity factors affect the shift from acceptance willingness to sharing behavior:

First, smartphone dependence serves as a tool enabling rapid fraud information transmission and may explain increasing victimization among younger populations. **H2a: Higher smartphone dependence strengthens the positive effect of fraud information acceptance willingness on sharing behavior.**

Second, time cost represents another critical determinant. While knowledge sharing research shows time costs constrain information processing and sharing, in fraud contexts, the anticipated economic benefits may increase time investment, paradoxically enhancing sharing behavior. **H2b: Higher time costs weaken the effect of fraud information acceptance willingness on sharing behavior.**

2.4 "Can They Do It?"—Ability Factors' Influence on Fraud Information Sharing Behavior

MOA model ability emphasizes individuals' internal capacity to influence activity completion within social relationships. Research confirms that victims' experience and expertise are crucial for resisting telecom fraud—individuals with higher network experience and security knowledge are less susceptible to phishing attempts.

Cybersecurity identification ability not only reduces fraud information acceptance motivation but also blocks fraud information transmission and sharing. **H3a: Higher cybersecurity identification ability reduces fraud information acceptance willingness.**

Self-efficacy—individuals' self-assessment of their capability to successfully complete tasks—also influences sharing behavior. In fraud contexts, overconfident victims may feel greater control over developments, paradoxically increasing their vulnerability. **H4a: Stronger self-efficacy increases fraud information acceptance willingness.**

Furthermore, both self-efficacy and cybersecurity identification ability may amplify the motivation-behavior relationship once victims develop acceptance willingness, acting as "boosters" for sharing behavior. **H3b: Higher cybersecurity identification ability strengthens the positive effect of fraud information acceptance willingness on sharing behavior. H4b: Stronger self-efficacy strengthens the positive effect of fraud information acceptance willingness on sharing behavior.**

The theoretical model based on MOA framework is illustrated in Figure 1 [Figure 1: see original paper].

3 Research Design and Confirmatory Factor Analysis

3.1 Research Design

3.1.1 Sample Source and Structure Using convenience sampling, this study surveyed telecom fraud victims from April to December 2019. A total of 1,500 questionnaires were distributed, yielding 1,427 responses, with 1,398 valid samples retained after excluding invalid ones. The questionnaire included a screening item: "Have you ever experienced a telecom fraud case? If not, please stop filling out this questionnaire." Additionally, respondents were asked: "During the fraud, did you share (or forward, verbally transmit) the fraud information to others while unaware?" to exclude those without sharing behavior. The sample structure demonstrates representativeness across demographic variables (see Table 1).

3.1.2 Variable Measurement All variables were measured using 7-point Likert scales (see Table 2). Measurements included: - False information "authority" (3 items, Cronbach's $\alpha = 0.890$), referencing X. Luo et al. and P. Fischer et al. - Trust in perpetrators (3 items, $\alpha = 0.869$), referencing R.C. Mayer et al. and J. Gould-Williams - Profit-seeking psychology (3 items, $\alpha = 0.911$), referencing Ge Yuewei and Ma Lifen et al. - Smartphone dependence (3 items, $\alpha = 0.905$), referencing A. Vishwanath - Time cost (3 items, $\alpha = 0.868$), referencing Song Xiaokang et al. and J. Wang - Self-efficacy (3 items, $\alpha = 0.942$), referencing Ming Junren et al. - Cybersecurity identification ability (3 items, $\alpha = 0.895$), referencing B. Harrison et al. - Fraud information acceptance willingness (3 items, $\alpha = 0.858$), adapted from Jia Mingxia et al.'s knowledge sharing research - Fraud information sharing behavior (3 items, $\alpha = 0.833$), similarly adapted

Eight domain experts validated all adapted variables for content validity.

3.1.3 Common Method Bias Test Common method bias testing addresses artificial covariance from shared data sources, collection environments, and contexts that may bias results. Following Zhou Hao and Long Lirong's recommended single-factor test method, the analysis shows poor fit for the single-factor model (RMSEA = 0.143 > 0.08), indicating no severe common method bias.

3.2 Confirmatory Factor Analysis

Due to space limitations, this study omits detailed description of preliminary work including in-depth interviews with 36 telecom fraud victims and exploratory factor analysis from pilot testing. The confirmatory factor analysis using AMOS 23.0 compared multiple models (see Table 3). The nine-factor model demonstrated superior fit indices compared to alternative models (single-factor through eight-factor models), confirming good discriminant validity and theoretical model feasibility. Table 2 and the correlation matrix (Table 4) show all factor loadings exceed 0.5 and AVE values exceed 0.5, meeting convergent validity requirements.

3.3 Variable Correlations

The correlation analysis (Table 4) reveals significant relationships among false information "authority," trust, profit-seeking psychology, smartphone dependence, time cost, self-efficacy, cybersecurity identification ability, fraud information acceptance willingness, and sharing behavior, supporting further empirical analysis.

4 Empirical Testing

This study used IBM SPSS 23.0 for hierarchical regression analysis to test direct effects of control variables, false information "authority," trust, profit-seeking psychology, self-efficacy, and cybersecurity identification ability on acceptance willingness, as well as moderating effects of smartphone dependence, time cost, self-efficacy, and cybersecurity identification ability.

4.1 Direct Effects Testing

Regression results (Table 5) show: - **Model 1**: Males exhibit stronger acceptance willingness than females ($\beta = 0.046$, $p < 0.05$); divorced individuals show stronger willingness than other marital statuses ($\beta = 0.047$, $p < 0.05$). - **Model 2**: False information "authority" significantly and positively affects acceptance willingness ($\beta = 0.521$, $p < 0.001$), supporting H1a. - **Model 3**: Trust significantly and positively affects acceptance willingness ($\beta = 0.552$, $p < 0.001$), supporting H1b. - **Model 4**: Profit-seeking psychology significantly and positively affects acceptance willingness ($\beta = 0.316$, $p < 0.001$), supporting H1c. - **Model 5**: Self-efficacy significantly and positively affects acceptance willingness ($\beta = 0.309$, $p < 0.001$), supporting H4a. - **Model 6**: Cybersecurity

identification ability significantly and negatively affects acceptance willingness (β = -0.109, p < 0.001), supporting H3a.

All VIF values remain below 10, indicating no severe multicollinearity, and the DW value of 2.046 suggests no significant serial correlation, confirming result robustness.

4.2 Opportunity Factors' Moderating Effects

Following G. Ahuja's recommended hierarchical regression method, variables were centered before testing to mitigate multicollinearity in interaction terms (centered variables denoted with "Z").

Smartphone dependence: Models 7-9 (Table 6) show that after controlling for main effects (β = 0.595, p < 0.001 for dependence; β = 0.683, p < 0.001 for acceptance willingness), the interaction term significantly improves model fit (ΔR^2 = 0.003, p < 0.001; β = 0.058, p < 0.01). Higher smartphone dependence strengthens the effect of acceptance willingness on sharing behavior, supporting H2a.

Time cost: Models 10-12 show that time cost (β = 0.582, p < 0.001) and acceptance willingness (β = 0.667, p < 0.001) both significantly affect sharing behavior. The interaction term is significant (β = 0.054, p < 0.001) but opposite to the hypothesized direction, indicating that higher time costs actually strengthen rather than weaken the relationship. H2b is not supported. This counterintuitive finding suggests that the anticipated economic benefits from fraud information increase victims' time investment, which in turn motivates sharing behavior.

4.3 Ability Factors' Moderating Effects

Self-efficacy: Models 13-15 (Table 7) demonstrate that after accounting for main effects (β = 0.614, p < 0.001 for self-efficacy; β = 0.668, p < 0.001 for acceptance willingness), the interaction term significantly improves model fit (ΔR^2 = 0.002, p < 0.001; β = 0.050, p < 0.01). Higher self-efficacy strengthens the effect of acceptance willingness on sharing behavior, supporting H4b.

Cybersecurity identification ability: Models 16-18 show that after controlling for main effects (β = 0.590, p < 0.001 for ability; β = 0.670, p < 0.001 for acceptance willingness), the interaction term significantly improves model fit (ΔR^2 = 0.006, p < 0.001; β = 0.076, p < 0.001). Higher cybersecurity identification ability strengthens the effect of acceptance willingness on sharing behavior, supporting H3b.

All regression equations show VIF and DW values within acceptable ranges, confirming result validity.

5 Conclusions and Discussion

5.1 Research Conclusions

As information technology 普及 and financial markets open, ordinary citizens face increasing investment channels but also greater fraud risks. Grounded in MOA theory, this study constructed and empirically tested a theoretical model of victims' fraud information acceptance willingness and sharing behavior using 1,398 victim samples, yielding four key findings:

1. **Demographic effects**: Males and divorced individuals show significantly higher fraud information acceptance and sharing willingness. This may reflect that Chinese males, as primary family providers facing greater economic pressure, seek more investment opportunities. Among elderly populations, retired males have more leisure time to encounter fraud information than females occupied with childcare. Divorced individuals, seeking independent income and holding autonomous financial decision-making power, may be more susceptible to fraud and more likely to share information.

2. **Motivational drivers**: False information "authority," perpetrator trust, and profit-seeking psychology significantly and directly drive acceptance willingness. Real-world cases confirm that perpetrators routinely use fake "official" information, celebrity endorsements, and authoritative media packaging to gain initial victim trust. Subsequent online interactions and "small favors" exploit victims' profit-seeking psychology. These findings align with P. Fischer et al.'s research showing victims' high acceptance of "official" notifications. Prevention implications include: strengthening supervision of online financial product information, increasing transparency of financial personnel information to reduce trust asymmetries, and enhancing anti-fraud propaganda to counter profit-seeking vulnerabilities.

3. **Ability factors**: Self-efficacy positively affects acceptance willingness while cybersecurity identification ability negatively affects it. However, both strengthen the acceptance-sharing relationship. Telecom fraud represents sophisticated, repeatedly tested schemes that average victims cannot 识破 through financial expertise alone. Overconfident victims may suffer from "smartness being fooled by smartness." Conversely, cybersecurity identification skills can reduce victimization risk, as B. Harrison noted that individual cybersecurity capability alone cannot explain victimization patterns. Importantly, once acceptance willingness develops, both self-efficacy and cybersecurity ability become "boosters" for sharing behavior, explaining fraud's wide contagion.

4. **Opportunity factors**: Smartphone dependence and time costs significantly moderate the acceptance-sharing relationship. Smartphones have become essential daily tools, especially for contactless payments during COVID-19. Higher dependence accelerates fraud information dissemina-

tion. The positive moderating effect of time costs, though counterintuitive, reflects that fraud information's strong appeal and anticipated benefits increase victims' time investment, which subsequently motivates sharing with others.

5.2 Contributions and Limitations

This study's primary contributions include: (1) Developing and validating an MOA-based theoretical model that reveals fundamental patterns of fraud information acceptance and sharing among telecom fraud victims, advancing theoretical understanding; (2) Providing evidence-based support for multi-level prevention strategies targeting victim capabilities, psychology, and media usage, with practical implications for strengthening false information supervision, enhancing cybersecurity identification skills, and preventing irrational smartphone-based financial investments.

Limitations include: (1) This retrospective study may deviate from victims' actual psychological processes during fraud incidents—future experimental research could provide more authentic behavioral measurement; (2) While focusing on core influencing factors, the model omits potential variables like external environment and product experience loyalty that may affect acceptance and sharing—future research should explore additional variables to enrich the theoretical framework; (3) The questionnaire focused primarily on "investment and financial information" fraud types, with limited coverage of health-related and other fraud categories—future studies should test the model's robustness across diverse fraud types.

References

[1] Jin Gaofeng, Shou Jiali, Lin Xin'nan. Analysis and Prediction of Crime Situation in China (2018-2019)[J]. Journal of People's Public Security University of China (Social Sciences Edition), 2019, 35(3): 1-11.

[2] Zhang Ying, Cheng Chuanjie. Empirical Analysis and Prevention Suggestions for Mass Illegal Fund-raising Crimes[J]. Chinese Prosecutor, 2019(9): 40-42.

[3] Yin Ming. Empirical Research on Telecom Fraud Victims—Based on Quantitative Analysis of Victim Statements[J]. Journal of China Criminal Police College, 2017(3): 57-62.

[4] Yuan Jinghui. Research on Telecom Fraud Prevention Mechanism Based on the "Pareto Principle"[J]. Journal of Changchun Normal University, 2019, 38(5): 34-37.

[5] Gao Yunlin, Zhou Yuling. Empirical Research on Telecom Fraud Investigation and Prevention Under Big Data—Based on C City Public Security Bureau Case Data[A]//Chinese Criminology Association Prevention Professional Committee, Shanghai University of Political Science and Law School of Criminal

Justice - Police College. Criminology Forum (Vol. 5). Shanghai: China Legal Publishing House, 2018: 880-887.

[6] Ma Zhonghong. On Sampling Evidence in Cybercrime Cases—Taking Telecom Fraud as an Example[J]. China Criminal Police, 2019(6): 6-10.

[7] Ji Xiquan. Combating and Preventing Telecom Network Fraud—Taking Sanming City, Fujian Province as an Example[J]. Journal of Zhejiang Police College, 2018(4): 78-84.

[8] Ge Yuewei. Research on Telecom Network Fraud Prevention Propaganda Strategies—Based on Analysis from the Perspective of Telecom Network Fraud Victims[J]. Journal of Zhejiang Police College, 2018(4): 69-78.

[9] Cai Guoqin, Zhao Zengtian. On Constructing a Three-dimensional Prevention and Control System for Telecom Fraud Crime[J]. Crime Research, 2011(4): 99-105.

[10] Song Ping. Psychological Analysis and Prevention of Telecom Network Fraud[J]. Journal of Guangxi Police College, 2017, 30(1): 121-125.

[11] MacInnis DJ, Jaworski BJ. Information Processing from Advertisements: Toward an Integrative Framework[J]. Journal of Marketing, 1989, 53(4): 1-23.

[12] Jia Mingxia, Xiong Huixiang. Exploration of Knowledge Exchange and Sharing in Virtual Academic Communities—Based on Integrated S-O-R Model and MOA Theory[J]. Library Science Research, 2020(2): 43-54.

[13] Chen Zeqian. Formation, Development and Core Constructs of MOA Model[J]. Library Science Research, 2013(13): 53-57.

[14] MacInnis DJ, Moorman C, Jaworski BJ. Enhancing and Measuring Consumers' Motivation, Opportunity, and Ability to Process Brand Information from Ads[J]. Journal of Marketing, 1991, 55(4): 32-53.

[15] Hallahan K. Enhancing Motivation, Ability, and Opportunity to Process Public Relations Messages[J]. Public Relations Review, 2000, 26(4): 463-480.

[16] Hung K, Sirakaya-Turk E, Ingram LJ. Testing the Efficacy of an Integrative Model for Community Participation[J]. Journal of Travel Research, 2011, 50(3): 276-288.

[17] Adler PS, Kwon S-W. Social Capital: Prospects for a New Concept[J]. Academy of Management Review, 2002, 27(1): 17-40.

[18] Song Xiaokang, Zhao Yuxiang, Song Shijie, et al. Health Rumor Sharing Intention Based on MOA Theory[J]. Journal of the China Society for Scientific and Technical Information, 2020, 39(5): 511-520.

[19] Luo X, Zhang W, Burd S, et al. Investigating Phishing Victimization with the Heuristic-Systematic Model: A Theoretical Framework and an Exploration[J]. Computers & Security, 2013, 38(5): 28-38.

[20] Fischer P, Lea SEG, Evans KM. Why Do Individuals Respond to Fraudulent Scam Communications and Lose Money? The Psychological Determinants of Scam Compliance[J]. Journal of Applied Social Psychology, 2013, 43(10): 2060-2072.

[21] Baranowski T, Smith M, Baranowski J, et al. Low Validity of a Seven-item Fruit and Vegetable Food Frequency Questionnaire Among Third-grade Students[J]. Journal of the American Dietetic Association, 1997, 97(1): 66-68.

[22] McAlexander JH, Schouten JW, Koenig HF. Building Brand Community[J]. Journal of Marketing, 2002, 66(1): 38-54.

[23] Vishwanath A. Mobile Device Affordance: Explicating How Smartphones Influence the Outcome of Phishing Attacks[J]. Computers in Human Behavior, 2016, 63(5): 198-207.

[24] Reinholdt M, Pedersen T, Foss NJ. Why a Central Network Position Isn't Enough: The Role of Motivation and Ability for Knowledge Sharing in Employee Networks[J]. Academy of Management Journal, 2011, 54(6): 1277-1297.

[25] Brennan LL. Understanding the Knowledge-sharing Challenge: Is a "Bottleneck" Perspective the Answer?[J]. Academy of Management Perspectives, 2008, 22(3): 112-114.

[26] Wright RT, Maret K. The Influence of Experiential and Dispositional Factors in Phishing: An Empirical Investigation of the Deceived[J]. Journal of Management Information Systems, 2010, 27(1): 273-303.

[27] Mayer RC, Davis JH. The Effect of the Performance Appraisal System on Trust for Management: A Field Quasi-experiment[J]. Journal of Applied Psychology, 1999, 84(1): 123-136.

[28] Gould-Williams J. The Importance of HR Practices and Workplace Trust in Achieving Superior Performance: A Study of Public-sector Organizations[J]. The International Journal of Human Resource Management, 2003, 14(1): 28-54.

[29] Ma Lifen, Lv Yao. Analysis and Governance Path of Telecom Fraud Crimes in Universities[J]. Journal of Beijing Police College, 2017(4): 110-114.

[30] Wang J, Herath T, Chen R, et al. Research Article Phishing Susceptibility: An Investigation into the Processing of a Targeted Spear Phishing Email[J]. IEEE Transactions on Professional Communication, 2012, 55(4): 345-362.

[31] Ming Junren, Yu Shiying, Yang Yanni, et al. Construction of a Technology Acceptance Model for Mobile Libraries[J]. Information and Documentation Services, 2014, 35(5): 49-55.

[32] Harrison B, Svetieva E, Vishwanath A. Individual Processing of Phishing Emails: How Attention and Elaboration Protect Against Phishing[J]. Online Information Review, 2016, 40(2): 265-281.

[33] Zhou Hao, Long Lirong. Statistical Tests and Control Methods for Common Method Biases[J]. Advances in Psychological Science, 2004(6): 942-950.

[34] Ahuja G. Collaboration Networks, Structural Holes, and Innovation: A Longitudinal Study[J]. Academy of Management Proceedings, 2000, 45(3): 425-455.

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