An Analysis of Anti-deception Education for Fraud Detection

Jie Jian[1], Yanshuang Zhang[1, a] and Siqi Chen[1]

[1]School of Economics and Management, Chongqing University of Posts and Telecommunications, Chongqing 400065, China.

[a]1247866253@qq.com

Abstract

In order to explore the impact of anti-deception education on Internet users' deception detection, and to make suggestions for improvement, through the construction of the behavior model of Internet users' fraud detection, a phishing link experiment and questionnaire survey are carried out among students, and the experiment and questionnaire data are analyzed by variance analysis. It is found that Internet users detect network fraud. The behavior is affected by both trust and education.

Keywords

Network fraud, anti-deception education, fraud detection, trust.

1. Introduction

According to the 360 Network fraud reporting platform statistics, in 2017 a total of 24,260 online fraud reports were received, including fraudulent acts such as "false part-time job," "phishing website payment," and "financial fraud," which caused losses of up to 350 million yuan. Compared with 2016, the number of online fraud reports increased by 17.6% in 2017, and the per capita loss increased by 52.2%[1]. In a prominent case, A Tsinghua professor was deceived by 18 million[2], and other high-profile groups were deceived, making it even more questionable whether the experience in education can help netizens detect fraud. Therefore, it is important to explore whether anti-deception education is effective for netizens to detect fraud and what type of anti-deception education can effectively affect the detection behavior of netizens. It is of great significance to improve anti-deception education, effectively intervene in online fraud, and support government supervision.

Among the different kinds of online deception detection, previous studies have focused on two aspects. The first are deception detection behavior models. Grazioli proposed the Model of Detecting Deception (MDD), which analyzed the four stages of netizen fraud detection: activation, hypothesis generation, hypothesis evaluation, and comprehensive evaluation[3]. Wright et al. added confirmation behavior and personal characteristics to the Grazioli model[4]. Algarni believes that netizens detect fraud in three aspects: detecting fraud and refusal, falling into fraud, and participating in it[5]. The above literature studies the psychological mechanism and behavioral process of netizens' fraud detection and proposes a research framework that can be used for reference, but lacking empirical tests. The second aspect involves the subjective and objective influencing factors of netizens detecting fraud.

In terms of subjective factors, Pratt believes that people with a higher trust tendency are more likely to be defrauded, and individuals with more experience are more likely to detect fraud[6]. Ibrahim believes that Internet users' extroversion characteristics, trust, and compliance are more likely to lead them to be defrauded[7]. Chen suggests that netizens who show characteristics of these things that numbness, lack of understanding of fraud, vigilance, and overconfidence are more likely to be defrauded[8]. Xiao believes that the leakage of personal information and lack of awareness of prevention are the main reasons for netizens being

defrauded[9]. Sheng et al. believe that women are more likely to become victims of phishing than men, and people in the 18–25 age range are more likely to become phishing targets[10].

In terms of objective factors, Mavlanova found that the characteristics of the website (such as amateurish appearance, content, whether it actually exists, etc.) affect the judgment of netizens on fraud[11]. Constantinos S et al. have adopted supervision and non- supervision methods to detect the impact of fraud, and found that the supervision method can enhance the effect of detecting fraud, but sometimes an unsupervision method can be adopted[12]. Boxiao (2015) analyzed the impact of website security-prompting mechanisms on netizens' detection of fraud based on the "stimulus-organism-response" model and a netizen detection behavior experiment, and found that prompt information with negative suggestions can effectively enhance the detection effect of netizens[13]. In addition, some scholars focus on the impact of education on the detection of fraud by netizens.

However, on the subject of whether education can help netizens detect fraud, different scholars have different views. Among them, Algarni et al. pointed out that degree of education has an impact on netizens' fraud detection[14]. Ding et al. proposed that strengthening education can effectively prevent netizens from being defrauded[15]. Kirlappos et al. pointed out that education that can improve the awareness of netizens and correct their online behavior is effective in detecting fraud[16]. But Evers et al. believe that education is ineffective for netizens to detect online fraud[17]. The above literature studies the influencing factors of netizens' fraud detection from different perspectives, such as trust, network experience, and education. However, there are many studies on the subjective factors (experience, personality characteristics, trust) and accidental factors that affect netizens' detection behavior. There are few studies on objective factors, especially the empirical test of educational factors. Therefore, it is necessary to study anti-deception education's effect on netizens' detection behavior, and empirically test its impact so as to provide a theoretical basis for improving the existing anti-deception education and intervening in fraudsters' efforts to spread online fraud.

This paper aims to address two questions: 1) Can anti-deception education affect netizens' deception detection, and 2) What type of education can improve the detection ability of netizens? To answer these two questions, this paper develops a theoretical model and a set of hypotheses describing the relationships between anti-deception education, trust, and fraud detection, and considering influencing factors such as age, gender, network familiarity, etc. The proposed model is then tested by using a variance analysis method with the data collected via a potential victims experiment and web surveys.

2. Definition and Hypothesis

2.1. Trust

Interpersonal trust in the network is a partial extension and mapping of real interpersonal trust in cyberspace. The higher the trust of netizens in the trustor, the higher the trust in the trustor's information, which affects the netizens' rational judgment on fraud. Reyns pointed out that in the prevention of online fraud, not only must we guard against strangers, but we must also be vigilant toward acquaintances[18]. Shan et al. found that the higher the trust of netizens in the trustor, the better the forwarding effect[19]. Therefore, we propose the following:

Hypothesis 1: There is a negative relationship between the trust of netizens and netizens' deception detection.

2.2. Anti-deception Education

In this paper, anti-deception education is defined as social practice activities that directly or indirectly affect the detection of fraud by netizens, including life experience, daily cybersecurity education, and intensive education before the phishing link experiment in this article. Life

experience refers to various online anti-deception knowledge that netizens experience or hear during the daily contact with the network and social interaction. Daily network security education mainly refers to the daily reports and reminders of various types in the mass media about online fraud information. Intensive education refers to all kinds of special education activities carried out by network security-related departments on the netizens in a timely manner. By setting up reward mechanisms, these encourage netizens to actively learn and master cybersecurity knowledge, and the relevance and timeliness of such education is compared with the former. Therefore, according to the intensity of education, anti-deception education can be divided into three categories: 1) only life experience, 2) has both life experience and daily cybersecurity education, and 3) has life experience, daily cybersecurity education, and intensive education.

We propose that:

Hypothesis 2: There is a positive relationship between anti-deception education and netizen fraud detection. The higher the education intensity, the better the effect on netizens in detecting fraud.

Hypothesis 3: Under various levels of trust (very distrustful of H3a, distrustful of H3b, uncertainty of H3c, trustful of H3d, and very trustful of H3e), there is a positive relationship between anti-deception education and netizen fraud detection.

Hypothesis 4: Anti-deception education regulates the relationship between trust and netizens' fraud detection.

The structure of the Research model is shown in Figure 1:

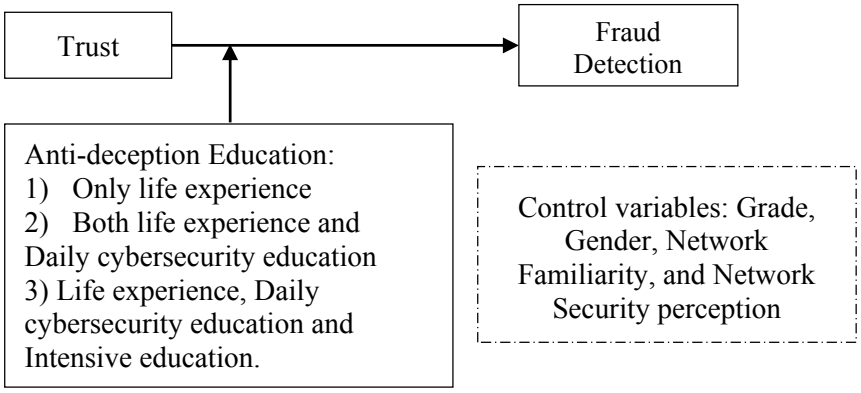

Figure 1. Research Model

3. Research Methodology and Data Collection

3.1. Experimental Processing

Since online fraud incidents occur frequently in colleges and universities, it is not uncommon for fake QQ friends to send phishing links. The deception process typically works as follows: The QQ number of a classmate in the university is stolen, and most of the other classmates in the same class also receive the phishing link sent by the classmate, because the class members are mostly QQ friends. But because of the difference in trust levels between them, some students may click, and other students may not click. Therefore, this experiment was conducted by selecting the undergraduate students and postgraduates as the experimental subjects and using the typical fraud case in which a QQ account is stolen and sends a phishing link to a friend as a reference background.

The experiment randomly selected six classes at the university, numbered 1, 2, 3, 4, 5, and 6. First of all, within a class, two classmates (hereinafter referred to as deceivers) are selected in each class to pretend to be the deceivers. In training them, the training content includes the

specific content of the fraudulent information, when and how to send the fraudulent information to a friend. The rest of the students are the subjects (hereinafter referred to as the ordinary netizens who don't know the experiment). Then, the six classes are divided into two groups. The 1, 2, and 3 classes are group A, and the 4, 5, and 6 classes are group B. The group A ordinary netizens are intensively educated, and the group B ordinary netizens are not intensively educated. Finally, the ordinary netizens of each class are randomly divided into two groups. The deceivers send fraud information to one of the ordinary netizens through QQ private chat.

One week after the intensive education of group A, the deceivers sent fraudulent information to the ordinary netizens in groups A and B through QQ friends chat. The fraud information is shown in Figure 2. After the ordinary netizen sees the fraudulent information, he/she will make different behavioral responses: 1) directly click or forward to others, 2) call and ask the link sender to verify that they sent the link, 3) verify the identity of the other party through QQ chat, 4) forward this fraud information to the class group or space to inform everyone that this person's QQ number was stolen, 5) inquire face to face, or 6) ignore the fraud information. Then we observe and record the behavior of the ordinary netizen. For behavior 1), after the link is clicked, the subject will see a blank web page (secure web page), which is considered falling victim to deception. For behaviors 2) to 6) are considered to be able to detect fraud successfully.

After the end of the experiment, we explain the purpose and significance of the experiment to the subject and ask them to fill out the questionnaire.

3.2. Sample Characteristics

A total of 303 responses were received. After eliminating incomplete and inappropriate responses, a total of 241 usable responses were included in the sample for hypothesis testing.

The sample characteristics obtained are shown in Table 1. Males accounted for 38.3%, Females accounted 61.7%. The grade distribution of the samples was mainly concentrated in sophomores and seniors. The average online duration of the network was mainly concentrated in less than two hours.

Table 1. Sample feature statistics

Subject	Option	Frequency	Percentage(%)	Subject	Option	Frequency	Percentage(%)
Gender	Male	93	38.6				
	Female	148	61.4		t<1h	85	35.3
Grade	Freshman	45	18.7	Average network online time	1h≤t<2h	66	27.4
	Sophomore	91	37.8		2h≤t<3h	34	14.1
	Junior	30	12.4		3h≤t<4h	13	5.4
	Senior	60	24.9		t≥4h	43	17.8
	Postgraduate	15	6.2				

4. Data Analyses and Results

4.1. ANOVA Analysis

The one-factor ANOVA analysis was used to test the anti-deception education, trust, and control variables. The results showed that the control variables (grade, gender, network familiarity, and network security perception) did not have a significant impact on netizens' fraud detection. Under the condition of a confidence level of 5%, there is a negative relationship between

netizens' trust in the trustor and netizens' fraud detection. That is to say, the higher the netizen's trust in the trustor, the less likely he or she is to detect the trustor. Hypothesis 1 passes the test (M=1.248 vs. 0.123, F (4,236)=10.142, P<0.05). There is a positive relationship between anti-deception education and netizens' fraud detection. That is to say, the higher the intensity of the anti-deception education, the better the effect of netizens detecting fraudulent information. Hypothesis 2 passes verification (M=1.424 vs. 0.131, F (2,238)=10.867, P < 0.05).

4.2. Sample Analysis under Different Levels of Trust

Under the condition of "very distrustful," the mean variance analysis of fraud detection results showed that the F value was 0.933 and the significance probability was 0.406>0.05, so H3a was not verified. Under the condition that the degree of trust is "distrustful," the mean of the fraud detection is 0, so H3b is not verified. Under the condition of "uncertainty," the mean variance analysis of fraud detection results showed that the F value was 3.193 and the significance probability was 0.048<0.05. Therefore, H3c passed the verification. Under the condition that the degree of trust is "trustful," the fraud detection's mean variance analysis showed that the F value was 4.668 and the significance probability was 0.012<0.05, so H3d passed the verification. Under the condition of "very trustful," the fraud detection's mean variance analysis showed that the F value was 0.655 and the significance probability was 0.530>0.05, so H3e was not verified.

Table 2. Summary of results of analysis of variance by education type at different levels of trust

Hypothesis	trust	Sample size	F	Sig.
H3a	1(very distrustful)	30	0.933	0.406
H3b	2(distrustful)	30	.	.
H3c	3(uncertainty)	62	3.193	0.048*
H3d	4(trustful)	95	4.668	0.012*
H3e	5(very trustful)	24	0.655	0.530

*. The significant level of mean difference was 0.05

5. Conclusion

To improve the detection effect of netizens on online fraud, netizens need to know the fraudulent methods commonly used by deceivers and make judgments based on their own experience and accepted education. We start with anti-deception education and construct a behavior model for netizens to detect fraud. Through the simulation of phishing link experiments to collect data and analysis, we found that anti-deception education has no significant effect on regulating the negative relationship between trust and fraud detection, but there is a positive relationship between anti-deception education level and netizen fraud detection. There is a negative relationship between trust and netizen fraud detection, and in the case of the trust degrees "uncertainty" and "trustful," there is a positive relationship between anti-deception education level and netizen fraud detection. Therefore, intensive education in anti-deception education can improve the effect of netizens' detection of fraud to a certain extent. For netizens whose trustworthiness is uncertain, the intensive education can generally improve the detection effect of netizens.

Of course, our research still has some shortcomings. In the selection of experimental subjects, the types are relatively simple, since all of them are students. In addition, the distinction between different anti-deception education programs is not detailed and comprehensive. In the future research, we can consider combing and analyzing the types of existing anti-deception education from different aspects, and explore the influence of various types of education on the

fraud detection effect of netizens, so as to provide guiding suggestions for the improvement of anti-deception education.

Acknowledgements

This work is funded by The National Social Science Fund of China: Research on the spread and intervention of e-commerce fraud(15BGL204); Technical meeting and system innovation project of Chongqing science and Technology Commission: Research on the prevention strategy of network fraud spread in social media (cstc2017jsyj-zdcxAX0053); Major projects of social science fund of Chongqing University of Posts and Telecommunications in 2016: Research on the defensive behavior of social engineering intrusion victims in social media(2016KZD07).

References

[1] 2017 online fraud data analysis [EB/OL]. [2018-02-27]. http: // www. askci. com/ news/ chanye/ 20180131/ 162836117346. shtml. (in Chinese).

[2] Professor Tsinghua was defrauded of 18 million by telecom fraud: 8 suspects were arrested and deceived [EB/OL]. [2017-12-25]. http://tech.qq.com/a/20170217/033581.htm. (in Chinese).

[3] Grazioli S. Where Did They Go Wrong? An Analysis of the Failure of Knowledgeable Internet Consumers to Detect Deception Over the Internet. Group Decision & Negotiation, 2004, 13(2):149~172.

[4] Wright R, Chakraborty S, Basoglu A, et al. Where Did They Go Right? Understanding the Deception in Phishing Communications. Group Decision & Negotiation, 2010, 19(4):391~416.

[5] Alseadoon I M A. The impact of users' characteristics on their ability to detect phishing emails. 2014.

[6] Pratt T C, Holtfreter K, Reisig M D. Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. Journal of Research in Crime and Delinquency, 2010, 47(3) :267~296.

[7] Alseadoon I, Othman M F I, Chan T. What is the influence of Users' Characteristics on Their Ability to Detect Phishing Emails. Berlin: Springer International Publishing,2015: 949~962.

[8] Chen Jinhua. The reasons why college students fall into the trap of false information fraud and preventive strategies. The Party Building and Ideological Education in Schools,2017(06):61~62. (in Chinese).

[9] Xiao Xie,Huang Jiangying. University Students Deceived on Network: Types, Reasons and Countermeasures. Journal of Chongqing University of Posts and Telecommunications (Social Science Edition),2015,27(05):67~72. (in Chinese).

[10] Sheng S,Holbrook M,Kumaraguru P,et al.Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of intervenetions. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.ACM,2010: 373~382.

[11] Mavlanova T, Benbunan-Fich R, Koufaris M,et al.The effect of positive and negative signals on perceived deceptiveness of websites in online markets.Journal of theoretical and applied electronic commerce research,2015,10(1) :19~34.

[12] Hilas C S, Mastorocostas P A. An application of supervised and unsupervised learning approaches to telecommunications fraud detection. Knowledge-Based Systems, 2008, 21(7):721~726.

[13] Xiao B, Benbasat I. Designing Warning Messages for Detecting Biased Online Product Recommendations: An Empirical Investigation. Information Systems Research, 2015, Forthcoming (4).

[14] Algarni A, Xu Y, Chan T, et al. Social engineering in social networking sites: how good becomes evil.Proceedings of The 18th PACIS 2014.2014.

[15] Ding Xiangli, Zhu Guoliang. Discussion on the rule of law education of college students in the "Internet +" era. The Party Building and Ideological Education in Schools,2017(15):63~65. (in Chinese).

[16] Kirlappos I, Sasse M A. Security Education against Phishing: A Modest Proposal for a Major Rethink. IEEE Security & Privacy, 2012, 10(2):24~32.

[17] Evers, J. Security Expert: User education is pointless[EB/OL]. [2017-12-30]. http: // news. com. com/ 2100-7350_3-6125213.html.

[18] Reyns B W, Henson B. The Thief with a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory. International Journal of Offender Therapy & Comparative Criminology, 2015, 60(10):1119.

[19] Shan Chunling, Zhao Hanyu. Analysis of Users' Forwarding Behavior of Business Information in Social Media—Based on Strong and Weak Relationship Theory. Journal of Modern Information, 2017, 37(10): 16~22. (in Chinese).