Research on Security Education Method in Higher Vocational Colleges from the Perspective of Telecom Fraud

Chen Xiaorong

Chongqing Business Vocational College, Chongqing, 401331, China

Keywords: Telecom Fraud; Higher Vocational Colleges; Security Education

Abstract: The case of telecommunication fraud in Colleges and universities has seriously affected social order and posed a great threat to the property safety of College students. This paper summarizes the new characteristics of telecommunication fraud in Colleges and universities, expounds the harmfulness of telecommunication fraud, and puts forward the key problems of unclear judicial interpretation of telecommunication fraud in Colleges and universities. After a thorough understanding of the current situation of anti-fraud education for Higher Vocational students, this paper puts forward scientific, reasonable and effective countermeasures and measures. From the perspective of telecom fraud, this paper analyzes the current telecom fraud crimes, integrates the power of the whole society, proposes strategic countermeasures, and fundamentally curbs the rapid spread of telecom fraud. Innovative work mode, focus on cultivating students' awareness of online fraud prevention, and strengthen students' ability to screen for online fraud. Therefore, it fundamentally strengthens the students' awareness of telecommunications security, and then contributes to changing the current situation of students' telecommunications fraud cases.

1. Introduction

the development of network information technology and the popularization of smart phones, online shopping and chat have been generally accepted by students, which undoubtedly brings great convenience to students' study and life [1]. Register the fake company on the website, leave contact information, wait for the rabbit to carry out fishing fraud activities. This kind of fraud belongs to the self-entrainment network of the deceived. Like boiled frogs in warm water, the deceived students have fallen into the trap of the deceivers unconsciously [2].The public security organ shall instruct the competent educational department and the school to promptly remind prospective students and students in the school to be more vigilant and enhance the awareness of anti-fraud [3]. At the same time, they should be informed that they should report to the public security organ in time if they find that they have been defrauded [4]. In order to avoid the recurrence of the same type of cases, to protect college students from telecom fraud, it is necessary not only to strengthen students' own awareness of prevention, but also to explore the crimes of telecommunications fraud and corresponding measures in colleges and universities, to explore how to deal with telecommunications fraud crimes in colleges and universities, and to A healthy and safe learning environment [5].

Telecom fraud is a new type of crime of embezzlement, which has been growing rapidly in recent years. To a certain extent, it affects the current situation of crime in our country [6]. The prevention and control of telecommunication fraud is not only the key work of protecting people's property security and maintaining good economic and social order, but also the focus of criminology [7]. Especially, the phenomenon of locking in the victims of college students and inducing college students to commit crimes has become an important risk and threat to the health of campus environment. With the widespread infiltration of telecommunication fraud into colleges and universities in various regions, the number of college students suffering from telecommunication fraud is increasing in recent years [8]. Unfortunately, most students pay insufficient attention to cybersecurity, and a considerable number of students lack knowledge about cybersecurity, which has led to the frequent occurrence of telecom fraud cases among students [9]. Telecommunications fraud cases not only show a large number of situations, but also different in terms of fraud methods

  DOI: 10.25236/iwedss.2019.005

and fraud methods. This paper studies the safety education methods of higher vocational colleges from the perspective of telecom fraud. And further analysis, in order to provide a theoretical basis for the anti-fraud safety education in higher vocational colleges, and provide a basis for the countermeasures and methods of anti-fraud education in higher vocational colleges [10].

2. Materials and Methods

The high-tech and covert characteristics of telecommunication fraud force the investigative organs to have the sense of cooperation and abandon the old concept of "painting the ground as a prison and fighting with a single policeman". Break down all kinds of barriers hindering investigation, such as barriers between police categories, barriers to the territorial jurisdiction of cases, barriers to regional jurisdiction, etc. The organizers of Telecom fraud criminal groups need to rent at most a small office, prepare several telephones and computers, spend hundreds of yuan to buy personal data, and employ several "salesmen". The economic cost of investment is extremely low. Due to the lack of social experience and lack of awareness of safety and security, students are less alert to online fraud such as virtual part-time, virtual winning, and virtual refunds. In particular, some students have some incentives for “rich”, “high salary” and “winning”. There is a small and cheap psychology, which leads to a circle of “tubular thinking”. The survey of telecom frauds suffered by telecom fraud victims in a higher vocational college from 2016 to 2018 is shown in Table 1.

Table 1 Investigation on the Causes of Telecommunication Fraud Encountered by Victims of Telecommunication Fraud in a Higher Vocational College from 2016 to 2018

	Using phishing websites	Online shopping	Winning Online	Pretend to be an acquaintance	Other
2016	13	80	42	26	210
2017	16	120	51	36	314
2018	21	136	29	42	309

When the crime of fraud in telecommunication network is carried out, at the same time, there are cases of providing or making fraud schemes, or when there are criminal acts such as voice packages, terminology lists, key fraud information, etc., the crime of fraud in telecommunications shall be dealt with jointly. Because telecommunication fraud is non-contact, the victim and the suspect have no face-to-face contact process, so telecommunication fraud does not exist in the traditional crime of the dominant scene, which makes it difficult for investigators to obtain direct evidence. And set up a network security guards community, telecommunications anti-fraud consulting group and other student organizations, so that students change the network security knowledge from passive learning to active learning, establish a sense of ownership of security education propaganda. Build a bridge of knowledge interaction between the relatively decentralized security knowledge, and build a dynamic network to prevent telecom fraud in colleges and universities.

The reasons why the crime of network telecommunication fraud has been successful repeatedly include not only the weaknesses and shortcomings of students themselves, but also the social factors such as insufficient efforts to prevent and combat criminals. "Personal information leaks seriously belong to colleges and universities." I can find that some of the leaks are unconscious. Some parents attend some free lectures or tutorials before and after the exam, and the information they fill in is often collected and sold back by illegal elements. In addition, it is found that although the initial stage is only the victim, it is indirectly a member of the crime due to the inducement of criminal organizations. Such organizational development characteristics are also rare in the past, and are the main form of the formation of telecommunications fraud crimes in colleges and universities. In order to enhance the importance attached by school teachers to the prevention of telecom fraud knowledge, schools can incorporate the case into the performance appraisal of teachers and counselors. Effectively embedding the campus public safety management work into

the functions of the education full-time department, and playing the "information symmetry, resource sharing, and functional education" between the police schools, so that the entire system can be peaceful, stable, and upward development.

3. Result Analysis and Discussion

At the present stage in our country, reselling personal information has become a black industry chain, and criminal suspects can easily purchase information of specific groups. In this "black chain", there are not only suppliers, but also intermediaries to facilitate transactions. Information security education in Colleges and universities is to enhance students'ability to protect information. By standardizing students' correct use of information, it avoids such operations as registration on websites without security certification, and does not upload personal confidential information. Increase awareness of prevention, effectively avoiding telecom fraud cases caused by information disclosure. The propaganda is not enough, and the anti-fraud knowledge is fragmented and unsystematic. The network communication operation enterprises are full of loopholes, the relevant departments pay attention to the lack of, the judicial institutions are not enough to crack down on factors such as the network telecom fraud crimes have been expanding and spreading.

From the case of successful telecommunication fraud, the victim has the problem of weak or lack of awareness of prevention. Popularizing victim's knowledge is the basis of raising awareness of prevention. People who have not learned the common sense of the victim tend to think that the victim is innocent. Initially, the flow of small funds can quickly recover funds, while students relax their vigilance after receiving bonuses, and the amount of bills gradually expands, and the amount of funds advanced by students will also increase. When the criminal feels that the student’s payment balance has been completely drained, the contact will be cut off directly. As long as you overcome greed, resist the temptation, keep a clear mind and rational thinking, and abandon the idea of getting nothing, getting rich overnight and falling from the sky, then the criminals and fraud will lose the soil of existence. Students can't learn the knowledge about preventing telecom fraud in the classroom. They can only face the "sugar-coated shells" with great temptation in the society with the spirit of "dare to try and try." All of the above reasons have led to the frequent occurrence of telecom fraud cases in colleges and universities.

Establish a correct outlook on life and values to resist lure and seduction. Throwing out all kinds of temptations is a common trick used by telecom fraud criminals. Whether they can resist all kinds of temptations depends on their own outlook on life and values. The so-called "iron must depend on its own hard". When dealing with people, we should be disciplined and principled. When we do not fully understand each other, we should not trust others and easily disclose important information such as personal and family ID cards, bank cards, passwords and so on to others. This is the key to successfully preventing the safety of personal and personal property. Furthermore, after expanding the qualification punishment standard, the criminal law is strictly enforced, and relevant laws and regulations are used to make more accurate judgments and punishments on criminal facts, to lay the foundation conditions and social environment for strengthening the protection of college students' identity information, and to reduce college telecommunications. Fraud crime rate. The countermeasures for the prevention of telecommunications fraud in colleges and universities are shown in Table 2 and Figure 1. When using various payment methods, you should get a goodwill reminder from the financial service organization, and ask the remitter to repeatedly evaluate the relationship of the other party to prevent being deceived. The goodwill reminders of payment and financial services institutions can not only affect the proceeds of crime, but also increase the risk and cost of crime.

Table 2 Consideration on the Preventive Measures of Telecom Fraud Crime in Colleges and Universities

	Increase	Administration
Increase Campus Publicity	16.08	6.95
Preventing the Loss of Students'Information	17.15	7.12

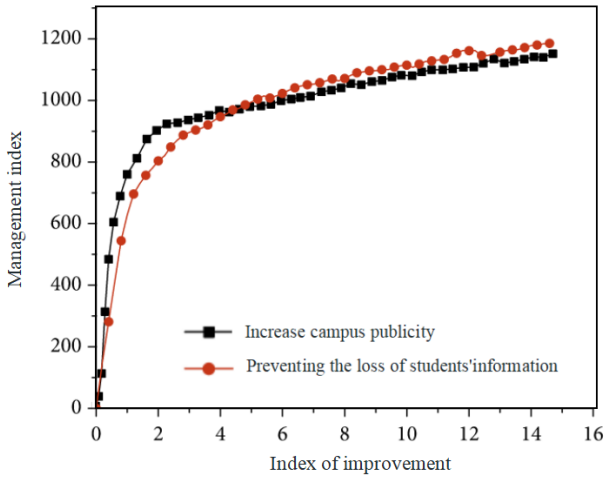

Fig.1. Consideration on the Preventive Measures of Telecom Fraud Crime in Colleges and Universities

4. Conclusion

This paper studies the security education method in Higher Vocational Colleges from the perspective of telecommunication fraud. As long as students understand its harmfulness and means of fraud, improve their awareness of prevention, grasp the necessary knowledge and methods of fraud prevention, and at the same time, social forces to increase propaganda and combat. It will certainly make the network telecommunications fraud have no foothold. Strengthen the screening ability of telecommunication fraud cases, improve the safety education system in Colleges and universities, from the perspective of knowledge popularization, take various educational means as an important grasp, and standardize the use of students' personal information. Improve students' awareness of network security and prevent collaboration with other departments such as the Ministry of Industry and Information Technology, banks, strengthen information exchange, and timely discover and dispose of numbers, serial numbers, and suspicious bank accounts involved in fraud cases. Give full play to the role of the network supervision department, long-term tracking, follow-up, and clean up the fraud gang hidden behind the virtual operators. Establishing an effective prevention and control system is a key link in the prevention and control of telecom fraud. Through the vigorous promotion of “point-to-face combination” and “stereo-precision”, the masses’ awareness of prevention is enhanced. Strengthen the prevention and control of deceived, deceived, and deceived to increase the intensity of technological upgrading. In order to fundamentally change the current situation of students' telecommunications fraud cases.

Acknowledgement

Supported by project of research innovation team of Chongqing Business Vocational College "Research Team of Higher Vocational Safety Education and Management"

References

[1] Farias, Mauricio, Sevilla, Maria Paola. Effectiveness of Vocational High Schools in Students’

Access to and Persistence in Postsecondary Vocational Education [J]. Research in Higher Education, 2015, 56(7):693-718.

[2] Park H S, Levine T R. The effects of truth–lie base-rates on deception detection accuracy in Korea [J]. Asian Journal of Communication, 2017, 27(5):1-9.

[3] Slantcheva-Durst, Snejana. Mechanisms of lifelong learning: the spread of innovative short-cycle higher education qualifications within national systems [J]. Higher Education, 2014, 68(1):87-102.

[4] Reflection on the Overlap of Youth's On-Line Victimization and Perpetration [J]. Deviant Behavior, 2016:1-16.

[5] Tran T T. Limitation on the development of skills in higher education in Vietnam [J]. Higher Education, 2013, 65(5):631-644.

[6] Basit T N, Eardley A, Borup R, et al. Higher education institutions and work-based learning in the UK: employer engagement within a tripartite relationship[J]. Higher Education, 2015, 70(6):1003-1015.

[7] Kim K N, Baker R M. The Assumed Benefits and Hidden Costs of Adult Learners' College Enrollment [J]. Research in Higher Education, 2015, 56(5):510-533.

[8] Hao Z. In search of a professional identity: higher education in Macau and the academic role of faculty [J]. Higher Education, 2015, 72(1):1-13.

[9] Garg V, Niliadeh S. Craigslist Scams and Community Composition: Investigating Online Fraud Victimization [J]. IEEE Cs Security & Privacy Workshops, 2013, 42(6):123-126.

[10] Levine T R, Clare D D, Blair J P, et al. Expertise in Deception Detection Involves Actively Prompting Diagnostic Information Rather Than Passive Behavioral Observation [J]. Human Communication Research, 2014, 40(4):442-462.