Scientific and Social Research, 2024, Volume 6, Issue 11
https://ojs.bbwpublisher.com/index.php/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

A Study on the Evolution of the Deceived Mode of Young Victims of Telecom Network Fraud

Feifei Mao*

Department of Investigation, Jiangsu Police Institute, Nanjing 210031, Jiangsu Province, China

Corresponding author: Feifei Mao, maofeifei@jspi.cn

Abstract: At present, the crime of telecommunication network fraud is still frequent and the crime situation is still severe and complex. With the emergence of new Internet technologies and new forms of business, youth groups have been impacted the most by telecommunications network fraud crimes. The victim group is characterized by the majority of young victims, with obvious differences in gender, education, and occupation, and the type of deception is highly related to age and gender. In the past three decades, the youth victim group has experienced the evolution of three modes of being cheated, from general netting to precise customization to incubation and operation. Analyzing the reasons for being cheated in specific crime situations from the perspective of victims is conducive to better predicting the potential victims of telecommunications network fraud crime and implementing more effective and accurate crime prevention.

Keywords: Telecom network fraud crime; Young victims; Deceived mode; Evolution

Online publication: November 29, 2024

1. Introduction

Since the 21st century, with the rapid development of the information society, the structure of crime has undergone significant changes, and traditional crimes have continued to decline. New types of network crime, represented by telecommunications fraud, have become the most prominent illegal activities with the highest number of cases, the greatest losses, and the strongest public response. In criminology, crime and victimization are two sides of the same problem. In-depth research on the characteristics of victims of fraud crimes can infer the motives, habits, and markings of criminals, improve the structural level of fraud crime research, and enrich the connotation of fraud crime research culture. In particular, by studying the evolution of the victim's fraud mode, researchers can fully understand the reasons for the victim's fraud and the reasons why the perpetrator chooses certain specific groups to commit fraud and how to lock in the victim, which is conducive to analyzing the causes of fraud crime from the specific crime situation. These studies are conducive to better predicting the potential victims of the telecommunications network fraud crime, and finding the loopholes in the prevention and control system of such

crime, to implement more effective and accurate crime prevention from the perspective of potential victims.

2. The research status of this problem

The research on the crime of telecommunication network fraud, with the keywords of "telecommunication", "fraud", "network", and "fraud" respectively, has found more than 4000 relevant research papers through the document retrieval of the full-text database of CNKI. The earliest research began in 1996 with the introduction of five common network fraud techniques in the United States. Relevant research began to increase in 2011 and grew rapidly in 2016. According to the literature search, the analysis of the crime of telecommunication network fraud from the perspective of the victim is relatively small, with only a dozen relevant studies. Based on some cases or case materials, and with the help of some theory or some statistical method, the existing research has summarized some demographic or statistical characteristics of the victims and analyzed the psychology of the victims and the formation process of the victims. The research object involves the elderly, college students, and other special groups.

Some representative studies include: Zhang Zhi et al. analyzed the demographic characteristics, victimization characteristics, and the acceptance of anti-fraud propaganda of the victims of telecommunications network fraud through the analysis of report notes, telephone return visits, and questionnaires surveys, and found that there were obvious differences in the demographic characteristics of the victims [1]. Based on the motivation theory of individual information behavior, Li Hui conducted empirical analysis and data processing on 1398 victims' survey samples and used the logical framework of the "motive opportunity ability" model to study the mechanism of different influencing factors in the process of victims' acceptance of fraud information and their sharing of fraud information [2]. Tianyu Wang et al. studied the investigation process and countermeasures of telecom network fraud through big data technology. This paper introduced the characteristics of big data and put forward the clustering algorithm and specific steps based on big data. Based on the clustering analysis of telecommunication network fraud based on big data, the experimental results showed that through the information age of big data, as long as big data are used rationally, it can effectively suppress telecommunications fraud and reduce it by 80% [3]. He Jingqiu takes the telecommunications network fraud crime of false investment and wealth management as an example and proposes the construction of a comprehensive time and space victim prevention system of "pre-prevention, mid-blocking, and post-tracking"[4]. Sun Chenbo and Zhao Guifen conducted in-depth interviews with post-90s victims of telecommunications fraud crimes and found that the personality and trust tendency of the victims are the mediating conditions of the victim process, incomplete experience is the strategic interaction condition of the victim, and interpersonal isolation is the key context of the victim [5]. Wang Chunmei and Wang Yiming used NVivo12 qualitative research software to conduct text analysis on 51 interview materials of victims of telecommunications network fraud crimes. They found that victims of telecommunications network fraud have psychological manifestations of depression and decline, traumatic stress, resentment, and vicious transformation after being deceived [6].

3. Research method

This paper mainly uses the qualitative research method to analyze and summarize 152 inquiry records of young victims of telecommunications network fraud crime from a certain region of J province, as well as research materials from some key areas of the country's telecommunications network fraud crime. Based on a macro summary of the typical characteristics of the youth victim group, it focuses on the evolution of the pattern of

young victims' being cheated in the past two decades with the rapid development of telecommunications network fraud crime, to achieve the purpose of accurate warning.

4. Typical group characteristics of young victims of telecommunication network fraud

According to the analysis of the survey data, the main victims of the current telecommunications network fraud crime show the following characteristics.

4.1. Young victims are the majority

At present, telecommunication network fraud mainly relies on the Internet to implement fraud, and the people who use the Internet are mainly young. From the perspective of the age composition of victims, the proportion of young people under 40 years old is as high as 79%, which is the main victim group of telecommunications network fraud. From the perspective of the proportion of each age group, the proportion of people aged 18–25, 26–29, and 30–40 is the largest, and the sum of the three reaches 75%, close to 3/4.

4.2. Significant gender difference

In the group of young victims of telecommunications network fraud, men account for 61%, while women account for 39%, meaning the number of male victims is significantly more than women. The proportion of men and women is about 6:4, with a large difference in number. Men are undoubtedly the target of fraud. This shows that men have poor awareness of prevention and a higher risk of being cheated, especially since some men have their own prevention loopholes when being cheated.

4.3. Significant differences in education and occupation

There are educational differences among the victims, and most of them have low educational backgrounds. The number of deceived groups with junior high school education is the largest, and the number of people with primary school and college education is the least. From the perspective of occupational distribution, ordinary occupational victims are relatively common. Among them, temporary workers, staff, farmers, waiters, ordinary workers, small businessmen/self-employed, unemployed, and other conditions are more common.

4.4. The type of cheating is highly correlated with age and gender

The group under the age of 20 are mostly school students or young people who have just entered society. They are prone to fall into the trap of fraud such as false shopping service transactions and part-time order swiping, among which the rebate fraud of order swiping accounts for 22.3%. The age group of 20–29 years old has a relatively large proportion in various scenarios such as identity fraud, brushing orders for rebates, online loans, and online marriage and dating. The mature group aged 30–39, with a stable economy, is relatively easy to be caught by swindlers such as "pig butchering scams", impersonating public security officers and the law, government agencies, leaders, acquaintances, and so on.

In addition, there are also significant differences between young men and women in the types of cheating. Men are more likely to be cheated in online marriage, making friends, online prostitution, pornography, loans, and online game product false transactions, while women are more vulnerable to the infringement of fake logistics customer service, part-time order swiping, "pig butchering scam" and other methods. Among them, male victims

account for 93% of pornographic fraud and 86% of online marriage and dating fraud. Among the victims of "pig butchering scam", the proportion of women is significantly higher than that of other types of fraud, and the proportion of victims aged 40 who are in the marriageable stage is as high as 43%, becoming the key target of fraud.

5. Evolution of the pattern of young victims of telecommunication network fraud

The evolution of the victimization mode of the youth victim group is closely related to the continuous updating of the ways of committing crimes by fraudsters. On the one hand, the updating of the ways of committing crimes directly "benefits" from the change in communication network technology. On the other hand, it is a typical performance of "one foot higher than the other." With the three stages of fixed, semi-mobile, and mobile communication network technology, the fraud mode has gone through three iterations, and the victimization mode of young victims has also gone through three evolutions.

5.1. Universal netting mode

Since 2000, mobile communication developed rapidly, and mobile phones have gradually become the main tool for people's daily communication. During this period, the fraudsters were in the active attack state, the fraud mode was large-scale and random, and the "general net" was carried out to the non-specified crowd through random group calls and SMS group sending. In particular, early fraudsters in Taiwan region claimed that the victims had won grand prizes such as scratch and horse betting by issuing leaflets and using the "Wang Ba Card" phone (the phone card with a fake application), but they had to send a certain amount of tax before receiving the prize. After the victim remitted the first sum of money, the fraudster asked the victim to remit money again and again in the name of a lawyer's fee, handling fee, notarial fee, etc., until the victim realized or all the money was drained. In addition, "Guess who I am", "PS photo" fraud and so on are common cheating techniques in this period, which can be called the 1.0 era of fraud.

5.2. Precision customization mode

After 2000, the Internet has gradually formed a new means of communication. The combination of short messages and the Internet has gradually formed a new form of online fraud, which is promoted by telephone and short messages in the initial stage of the drainage phase and "attention-drawing" in the later stage through short videos, web pages, and dating platforms. Since 2015, precision fraud has been implemented with the help of big data. Especially due to the rise of black and gray industries that steal public and private information data, the phenomenon of "precise customization" appears in the selection of fraud targets. The fraudsters can accurately find the victim's name, gender, home address, occupation, hobbies, and even recent concerns and current status. With the "August 19, 2016, Xu Yuyu Telecom Fraud" as a sign, it entered the 2.0 era of fraud. In the precise customization mode, the target of fraud is selected accurately, and the fraud script is "customized" according to the characteristics of different groups. The fraud is more targeted and the fraud success rate is high.

5.3. Incubation business model

With the development of mobile Internet in China, especially the iterative updating of 3G to 5G technology, various applications on the mobile end emerge endlessly. The constantly enriched applications have become the new favorites of fraud criminals. At present, the combination of traditional short messages and mobile internet

has created a mixed form. Criminals often use text messages to attract victims, click on false links, or log in to special websites, and then use mobile terminals (Internet-based applications) to commit fraud. This makes it easy for criminals to gain the trust of victims, and often the success rate of fraud is very high. In recent years, the widespread "pig butchering scam" fraud can be said to mark the entry of the 3.0 era of telecommunications network fraud. With the help of all kinds of social software, in the name of making friends, scammers can obtain the trust of victims through a certain period of "emotional investment" before fraud, that is, "pig butchering scam", which is an incubation business model.

Although the pattern of being cheated by young victims has undergone three changes, in each pattern of being cheated, the criminal is always in the active position, and each fraud is the criminal's premeditated attack. At this time, the victim is in a passive defense state and actively cooperates with the implementation and completion of the criminal's fraud without being aware of it [7]. In the process of fraud, the young victims interact with the perpetrators. They are not only the bearers of the consequences of the fraud crime, but also the young victims play a role in promoting or promoting their victimization in many of the above specific crime situations. It is because of the interaction between young victims and offenders that the final pattern of fraud crime is formed. This requires researchers to analyze the relationship between the victim and the offender from a dynamic perspective, and correctly understand the role of the victim in the whole process of crime, to eliminate the factors that induce or promote crime from the perspective of the victim, and thus more effectively prevent crime.

6. Conclusion

Strengthening targeted publicity and education, as well as prevention and early warning, is an important practical experience in the fight against telecommunications network fraud. This requires researchers to innovate anti-fraud mechanisms, explore the formation of a new anti-fraud model of "reverse search for potential victims based on involved element information" and carry out precise publicity and prevention. Researchers should actively promote the transformation of anti-fraud propaganda from "general public propaganda" to "key group propaganda" and then to "precise individual propaganda", and focus on improving the anti-fraud awareness and ability of potential key youth groups who have been deceived. By combining external anti-fraud propaganda with internal proactive anti-fraud measures, people can effectively protect the rights and interests of potential victims and achieve precise prevention of telecommunications fraud crimes.

Funding

The educational reform project of Jiangsu Police Institute "Data Empowerment and Criminology Teaching Design and Practice in the Perspective of High-Quality Development" (No.2021B07).

Disclosure statement

The author declares no conflict of interest.

References

[1] Zhi Z, Feng C, 2021, Research on the Propaganda Countermeasures of Telecom Network Fraud Prevention-Empirical

Analysis Based on the Characteristics of Victims. Journal of Guangxi Police Academy, **2021(2):** 41–49.

[2] Hui L, 2021, Research on the Victim's Willingness to Accept and Share Fraud Information in the Context of Telecom Fraud. Library and Information Work, **2021(7):** 90–102**.**

[3] Wang TY, Yang B, 2022, Countermeasure of Telecom Network Fraud Investigation Based on Big Data. Scientific Programming, 2022(7219080): 1–13.

[4] He JQ, 2023, Governance Dilemma and Optimization Approach for Prevention of Victims of Telecom Network Fraud Crimes — Empirical Investigation based on False Investment and Financing Cases. Journal of the People's Public Security University of China (Social Science Edition), **2023(4):** 83–96.

[5] Sun CB, Zhao GF, 2024, Research on the Process of Post-90s Victims in Telecom Network Fraud. Journal of the People's Public Security University of China (Social Science Edition), **2024(2):** 52–66.

[6] Wang CM, Wang YM, 2024, Characterization Analysis and Repair Path Research on Psychological Hidden Damage of Victims of Telecommunications Network Fraud Crimes: A Qualitative Analysis of NVivo based on 51 Victim Interview Materials. Journal of Zhejiang Police College, **2024(1):** 91–110.

[7] Zhang YH, 2020, Criminology (Fourth Edition). China Renmin University Press, Beijing, 82–84.