

Study on Telecommunication Fraud from a Student's Perspective

Shen Shiyang

People's Public Security University of China, Beijing, China

Abstract: With the rapid development of the information society, the structure of crime has undergone significant changes, and traditional crime has continued to decline, in contrast to which the new type of cybercrime represented by telecommunication network fraud has become the current major form of crime. In the public's perception, most of the victims of telecommunication network fraud are elderly people who are not familiar with the network, middle-aged people who are frequently involved in financial investment and the financial market, or young people who have just entered the workplace and are in urgent need of stability. However, students, who seem to have nothing to do with money, are becoming a new target for fraudsters. Part of the reason is because of the students a large number of personal information has been improperly collected, use, another part of the reason is that the students just because there is no source of money, but in the face of temptation has no resistance, especially for the students who have been addicted to online games, excessive consumption, almost unable to resist a variety of deception.

Keywords: Telecommunication fraud, Victims of students, Upgrading technical means

1. Introduction

In recent years, telecommunication network fraud has been a problem that cannot be ignored. Every year, many compatriots have their families broken up because of telecommunication network fraud. Nowadays, the target group of electric fraud has been expanded to students, many students are not familiar with the world, too simple, has become the "hardest hit" by electric fraud. As the future of our country and the hope of our families, we should pay attention to this issue and focus on solving the problem of students being cheated, in order to provide a healthier environment for the physical and mental development of children.

2. The current situation of victimization of student groups in telecommunication network frauds

2.1. The effectiveness of China's prevention and control of telecommunication network fraud in recent years

In response to the telecommunication network fraud crimes that have continued to show an upward trend in recent years, on October 10, 2020, the State Council held a meeting and decided to carry out card-breaking actions nationwide, and since the implementation of the card-breaking actions, as of mid-June 2021, the national public security organs in conjunction with the courts, procuratorates, finance, communications and other departments have cracked down on a total of "two-card " illegal and criminal gangs 15,000, seized 3,733,000 fraud-related phone cards, 566,000 bank cards, remediation of non-compliant industry outlets, institutions 18,000, the right to curb the high incidence of telecommunication network fraud crimes from the source. According to statistics, in the first half of 2021, the number of cases prosecuted for crimes committed by minors, the number of cases in which crimes were committed using the Internet was 945, involving 1,594 people, and the number of cases in which crimes were committed using telecommunications was 577, involving 1,114 people, and it can be seen from the data that there is a trend of more frequent cases of telecommunication network fraud involving minors. The Ministry of Foreign Affairs, the Supreme Court, the Supreme Procuratorate and the Ministry of Public Security jointly deployed a "nail-pulling" operation, which succeeded in apprehending 240 leaders and backbones of wire fraud syndicates. Although Operation Broken Card has severely cracked down on telecommunication network fraud, resulting in a continuing downward trend in the number of telecommunication network fraud cases nationwide after 2020, the form of the

crime is still serious and complex, and in particular we should continue to see the victimization of students in telecommunication network fraud as well as the crime situation [1-3].

2.2. Victimization of student groups by telecommunication network frauds

On June 22, 2021, the Supreme People's Court, the Supreme People's Procuratorate, and the Ministry of Public Security jointly issued the Opinions on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Telecommunications Network Fraud and Other Criminal Cases (II), which makes several references to minors and school students. In reality, telecommunication fraud cases show a trend of younger criminal subjects and younger victim groups, and many cases often involve such groups. During the epidemic, telecommunication fraud also gave rise to some new manifestations. For example, during the epidemic, the vast majority of students at home online classes, criminals take advantage of this to take targeted fraud. In fact, online education has gradually become a daily mode of education, children have more access to the network, it is easier to be deceived and exploited by those who have the intention to become a victim or victim of telecommunication fraud, the opportunity is greater. In addition, criminals will be "double-decrease policy" for the elaborate design of the scam, a variety of fraud can not be defended.

In the course of my internship at the police station, I received many cases of underage students being defrauded. For example, in April 2023, a junior high school student in order to buy a birthday gift for his mother, added a "seller" of WeChat, after knowing that the other group is a student, the "seller" seized the student does not have sufficient funds, with a low price to induce the student to buy products. Purchase of products, after the purchase, the "seller" asked the deceived person to add its QQ number, to participate in the lottery, of course, the deceived person drew the first prize, the first prize of 2000 yuan in cash and a pair of sneakers, but the "seller" asked the deceived person to first remit 3,000 yuan as a deposit, and then the "seller" asked the deceived person to first remit 3,000 yuan as a deposit. However, the "seller" required the victim to remit 3,000 yuan as a deposit before the prize could be released to the victim. Because the deceived person is only a junior high school student, no extra cash, will be the mother's bank card of 3,000 yuan transferred to the "seller", the mother found that the bank card was swiped out of 3,000 yuan after asking the deceived person, the deceived person to inform the mother of this matter, and then the mother will be brought to the police, even if the police, the loss is also Even if they came to the police, the loss would be difficult to recover. In fact, during my internship, I found that there were more cases of youth and elderly people being cheated than other age groups.

360 digital science released the "financial telecom network fraud analysis report" pointed out that financial telecom network fraud showed a trend of centralization, in which the cancellation of the campus loan account type of fraud accounted for 9%, ranking high in the forefront. The object of this type of scam is mostly just graduated college students, its cheating reason for students to register loan accounts during college will affect the personal credit, in order to intimidate the borrower will account for the amount of withdrawals, and transferred to the bank account in order to "cancel the account". The actual silly brother ah during the registration of online loan accounts and will not affect the personal credit, the borrower will withdraw the online loan amount is borrowing behavior, belong to the personal liabilities if not timely repayment will affect the personal credit. In addition to cancel campus loans, there are many other types of fraud on campus, such as online loans, part-time brush single, posing as an e-commerce customer service, idle fish "margin", buying and selling game accounts, QQ (WeChat) posing as a friend or relative, investment and finance, and so on. A few years ago, Xu Moyu case is the epitome of the harm of telecom fraud students, telecom fraud caused Xu Moyu physical and mental damage to death[4-6].

3. Students as Perpetrators in Telecommunication Network Frauds

At the same time, the number of cases in which young students become perpetrators of telecommunication fraud is also on the rise, with some students taking part in or helping to commit telecommunication network fraud for reasons such as being misled, and thus embarking on the path of crime. According to a report by the Supreme Prosecutor's Office in 2022, the suspects of the crime of helping information network criminal activities are mostly low-income and low-education groups, with 66.3 percent of them having less than junior high school education. The crime of helping the letter has become the third most prosecuted crime, after dangerous driving and theft, and has the highest incidence rate among information network crimes. However, with the constant updating and iteration of the means and technology of telecommunication network fraud, the criminal form of the crime of

helping the letter is also becoming more and more high-tech, and college students with undergraduate education or above have gradually become the group of the crime of helping the letter. In the case of telecommunication fraud, due to the lack of social experience of students, easy to be lured by others, compulsion, to the lawless elements to provide personal bank cards and cell phone cards, step by step into the telecommunication network fraud criminal activities of the "tool man". In addition to the "two cards", young students are also prone to become a contact tool between criminals and victims, that is, using their QQ number to add fraudsters, in accordance with the instructions of the fraudsters, take turns to use their own cell phones to dial the phone number provided by criminals, will be open with the fraudsters QQ voice of the cell phone and their own and the victim's phone call Cell phones together, so that fraudsters even outside the country, but also through the student's cell phone to talk to the victim, thus, the students fell into the victim. And some students studying IT majors to participate in the development of software, provide technical support is also a noteworthy criminal behavior in the crime of helping the letter.

4. Exposure to telecommunication network fraud in countries around the world

After 2012, with the popularization of the Internet, computers and smartphones, telecommunication fraud began to show an upward trend. Although I did not find any data or information on students becoming victims of telecommunication fraud in various countries on major search engines, telecommunication fraud has been active in various countries, and the following is the data on telecommunication fraud in various countries.

4.1. United States

In March 2023, the FBI released a report showing that Americans lost \$10.2 billion to various types of telecom fraud last year, the most in nearly five years. In terms of fraud types, one of the most prevalent types was phishing, in addition to data breaches and nonpayment scams, which were the second most common Internet scams in the United States. In terms of victim groups, seniors are the primary victims of internet fraud, with older Americans losing a total of \$3.1 billion to internet fraud in 2022, the most of any age group, and the most common scams among the older victim group are emails or phone calls posing as the IRS. In fact, in the U.S., Indians are the main group of people committing fraud, and since cybercrime is under the control of the FBI, but the FBI is only in charge of what happens within the U.S. and does not have foreign law enforcement authority to go abroad and make arrests, and foreign operations are under the control of the CIA, but the CIA does not have access to the victims, telecom fraud in the U.S. makes it almost impossible to recover losses.

4.2. Korea

Korea's telecommunication network fraud cases in 2018-2022 amounted to 227,126,000 cases, with a victimization amount of 16,645 trillion won (about RMB 8.82 billion). From the type of fraud, loan fraud accounted for as high as 60.1%, impersonation of authorities accounted for 22.8%, in addition to chat tool fraud in recent years showed a trend of continuous increase. From the age point of view, who also the higher the age, the greater the amount of money involved.

4.3. Japan

The Japan Police Agency released data saying that in 2018, Japanese people were cheated about 100 million yen per day on average due to telecommunication fraud, which is about 6.06 million yuan, and the economic loss caused by telecommunication fraud in Japan in 2018 was 36.58 billion yen, which is about 160 million yuan. In terms of the distribution of victims' age groups, those over 65 years old accounted for 78% of the total number of victims. Meanwhile, the Japan Police Agency also said that a total of 2,747 suspects suspected of telecommunication fraud were arrested or questioned by the police in 2018, of which 754 were minors, accounting for 27.4% of the total number of suspects. Although the number of telecommunication fraud cases has declined, the proportion of teenagers among fraudsters has increased significantly.

4.4. France

A total of 423,000 cases of telecommunication network fraud were registered in France in 2021, a

15% increase year-on-year, according to official data released by the country. The Bank of France released the "Report on Secure Transactions in France in 2020", which shows that 7.8 million fraudulent transactions occurred in France in 2020, resulting in a loss of 1.28 billion euros, which accounted for more than two-thirds of Internet platforms as well as cross-platform telecommunication network fraud.

5. Responses to telecommunication network fraud in countries around the world

In the Internet era, the incidence of telecommunication network fraud remains high, and in order to cope with the huge losses caused by telecommunication fraud to the people of various countries, governments are also endeavoring to introduce various policies and take a variety of countermeasures to prevent and combat telecommunication fraud, and I will introduce the countermeasures of various countries in the following aspects[7-8].

5.1. Strengthening legislative guarantees

The fight against online telecommunication fraud needs to be preceded by legislation, so as to lay a good legal foundation for the management of fraud. Countries around the world have introduced a variety of legislation against telecommunications network fraud. In order to combat telecommunications network fraud, the United States government introduced the Telephone Consumer Protection Act and other regulations and policies. According to the provisions of the French Penal Code, the maximum penalty for defrauding others by means of fraudulent, unfair or illegal collection of personal information is five years' imprisonment and a fine of 300,000 euros. In Japan, it is stipulated through the Penal Code that a person who deceives a person into delivering property shall be punished by imprisonment of not more than ten years." "Eliminate the trouble that has not yet arisen, cure the disease that has not yet fallen ill, and heal before nothing happens", China, on December 1, 2022, also formally enforced the "Anti-Telecommunications Network Fraud Law of the People's Republic of China".

5.2. Establishment of specialized agencies

First, in response to the proliferation of scams, the French Government has further strengthened the functions of specialized agencies by establishing, under the Directorate-General for Combating Information Technology and Communications Crime, which is part of the French National Police Directorate-General, a subdirector for combating cybercrime with more detailed responsibilities, which is responsible for investigating cyberfraudulent activities under new technologies. Secondly, the French government has also launched a specialized service website, which aims to help users effectively block spam calls and where users can also report fraudulent calls. In addition to the website, the French government has also launched a hotline and a cross-operator platform. Abu Dhabi, on the other hand, has created a platform called AMAN, which provides a 24/7 service to the public.

5.3. Upgrading technical means

According to a report by Brazil's Economic Values newspaper, Brazil's major banks have decided to complete the technical upgrades to their banking applications as soon as possible, such as requiring face recognition and fingerprint identification for each transaction to improve the security of bank accounts. In addition, Brazil's central bank previously adjusted the use of the instant payment system PIX rules, such as coloring the upper limit of night transfers, strengthen the single transfer amount to change the application of the audit. Meanwhile, 2022, China's Ministry of Public Security has continued to push warning instructions to various regions through the establishment of a graded and categorized warning and dissuasion mechanism. The National Anti-Fraud Center, according to the public security organs in possession of the cases involved in the good, the use of big data, artificial intelligence and other technical means to analyze the potential victims of the masses, may be smashing encountered telecommunication network fraud clues pushed to the public security organs around the country, by the national public security organs to carry out early warning and dissuasion work.

5.4. Focus on key populations

In 2018, Germany set up a special investigation team to target telecommunication network fraud

against the elderly, and launched the "Seniors informing seniors" program, which recruits retired police officers as volunteers to target telecommunication network fraud crimes against the elderly with precision.

5.5. Strengthening social monitoring and publicity

In order to enhance the ability of the public to prevent fraud, the United States, the United Kingdom, Germany, Russia, Japan and other countries have released on their official websites recent common methods of telecommunication network fraud and preventive measures. In China, public security organs across the country are publicizing the recent new fraudulent methods to the public every day through door-to-door meetings, telephone contacts, SMS reminders, etc., and for the people who are being defrauded, various ways are being used to make them see the criminals' schemes clearly.

6. Reasons for and solutions to students becoming a target group of telecommunication network frauds

6.1. Reasons why students are targeted by telecommunication frauds

In the face of the rising trend of underage fraud cases, we need to see why minors will become the tools and victims of fraud cases. Today's minors grow up in the Internet era, belong to the Internet era of the aborigines, for the Internet contact time is longer, and minors have a strong curiosity for new things, but due to the world is not yet deep, shallow social experience, immaturity, no economic income and other characteristics, resulting in a poor resistance to traps, easy to be compelled by others. For example, minors who are addicted to online games, high reward, high recharge, excessive consumption, etc., will easily and unconsciously walk into traps when faced with the temptation of receiving many cool skins and high-level equipments free of charge, as well as the possibility of interest-free loans, etc. In addition, poor, violent, and anorexic minors who are not familiar with online games will be easily and unconsciously trapped. In addition, poverty, violence, anorexia, neglect and other problems are also the reasons why underage students become a target group, and the aforementioned reasons, combined with online reasons, are also the main reasons why students become targets.

6.2. How the student population can be freed from the shackles of telecommunication network frauds

The relevant person in charge of the Criminal Investigation Bureau of the Ministry of Public Security said that "telecommunication network fraud is a product of the Internet era, which is not only a simple problem of social security, but also a complex problem of social governance". Students to prevent telecommunication network fraud, especially college students, is the main content of the future work of students in colleges and universities, in order to protect the property safety and physical and mental health of college students, telecommunication fraud must be unremitting.

First of all, from the students personally, students should raise their awareness of the rule of law, strengthen their own concept of the rule of law, and improve vigilance. Although the fraudulent techniques vary greatly, but all changes are the same, are through the information network to get in touch with you, to take a variety of ways to cheat your trust, so that you pay first, more money out of pocket. Nowadays, the public security organs have also done a lot of anti-fraud propaganda, students should keep the awareness of anti-fraud in mind, download the "National Anti-fraud Center" app, pay attention to the "National Anti-fraud Center", and always tighten the anti-fraud and anti-fraud strings. If you have unfortunately been cheated, you must first call 110 or to the nearest police station to call the police for help, apply for a stop payment, and keep a good record of relevant information to cooperate with the public security organs to investigate the work.

Secondly, from the family point of view, parents should be the first responsible person, parents are the most trustworthy people of college students, but also the university set up communication and exchange of crime close to the object, so the parents as a communication channel to the college students to prevent fraud propaganda can be more college students to accept. Parents should teach minors knowledge of fraud prevention, fraud prevention awareness, such as informing the child to remember the "three not one more" principle, that is, remember the unknown links do not click, unfamiliar callers do not gullible, personal information does not disclose the principle. For middle school and high school students, parents should also pay attention to their children's mental health and

behavior, keep their bank account information and cell phone payment passwords, and do not let their children use their payment accounts at will.

Once again, from the perspective of social governance, public security organs at all levels should strengthen the importance of anti-fraud propaganda, so that anti-fraud awareness is deeply rooted in people's hearts. However, the governance of telecommunications fraud can not fight alone, public security and inspection authorities around the world to deepen communication and collaboration with the local education sector, according to the local crime situation, in-depth development of telecommunications network fraud governance within the campus and around the campus, the introduction of anti-fraud measures that fit the characteristics of students.

In short, telecommunication network fraud to students is not only the loss of property, but also the damage to the mind, in the prevention of telecommunication network fraud, students are extremely vulnerable link, for the protection of students is not a person's responsibility, political and legal organs, relevant government departments and parents should be co-management, and jointly build a strong prevention and control line, the school and parents to strengthen as much as possible on the supervision of the students, the formation of the correct guidance to students, and establish healthy values. In dealing with the issue of minors involved in telecommunication network fraud, we should adhere to the principle of "education as the mainstay, punishment as a supplement", deepen the rule of law education for minors, crack down on criminal gangs using minors to commit fraud, and strengthen the supervision of the network, in order to maximize the protection of the rights and interests of minors.

7. Conclusions

Anti-fraud is a long way to go, and requires a two-pronged approach of combating and publicizing, especially for the student population. In addition, we can also learn from the relevant experience of other countries in the world. For students, anti-electro fraud is not only the society and the school, parents should also assume the corresponding responsibility, multi-cooperation, attention to the physical and mental health of students, to escort their healthy growth.

References

- [1] Xu Jialai. *Research on effective prevention strategies of college students against telecommunication fraud at home and abroad*[J]. *Legal Expo*, 2023, No. 899(03):15-17.
- [2] LIU Yinheng, HAN Yang, XIAN Luanjie. *How to prevent young people from becoming "knife passers"intelecomfraud*[N]. *ChinaYouthDaily*,2023-03-15(007).DOI:10.38302/n.cnki.nzgn.2023.000825.
- [3] Zhao Xiaojing. *Research on the path of cultivating college students' awareness of telecommunication fraud risk prevention in the era of "Internet+"*[J]. *Legal Expo*, 2023, No.900(04): 160-162.
- [4] YANG Jianguang, CHEN Si. *Research on the problems and countermeasures of propaganda and education for preventing telecommunication network fraud in colleges and universities in the era of big data* [J/OL]. *Journal of Kunming University of Science and Technology (Social Science Edition)*: 1-7 [2023-06-12].<https://doi.org/10.16112/j.cnki.53-1160/c.2023.03.153>.
- [5] Wu Linhua. *"Post-90s" and "Post-00s" become the main victim groups of telecom network fraud* [N]. *Jiefang Daily*,2021-08-27(010).DOI:10.28410/n.cnki.njfrb.2021.004786.
- [6] *State Internet Information Office exposes a batch of typical cases of telecommunication network fraud involving minors*[J]. *China Anti-counterfeiting Report*, 2023, No. 268(01):75-76.
- [7] TAO Tianyi. *Governance and prevention of minors' involvement in telecommunication network fraud* [J]. *Youth Rule of Law Education*, 2022, No. 68(11):5-11.
- [8] YIN Xiaotong, YE Meng. *Dilemmas and Countermeasures Facing the Governance of Telecommunication Network Fraud Crimes Committed by Minors*[J]. *Journal of Hubei Normal University (Philosophy and Social Science Edition)*,2022,42(03):50-55.