Digital Culture and Telecom Network Frauds: A Survey and Statistical Analysis in Colleges and Universities

Weishu Ye
School of Design, NingboTech University, Ningbo, 315000, China.
yws@nbt.edu.cn

Xin Jia
School of Design, NingboTech University, Ningbo, 315000, China.
zjgysj@nbt.edu.cn

Wenhui Yu*
School of Design, NingboTech University, Ningbo, 315000, China.
yuwenhui@nbt.edu.cn

Abstract: In an era dominated by rapid technological advancements, digital culture significantly shapes social interactions and vulnerabilities, particularly in the context of telecom network frauds in colleges and universities. This research undertakes a detailed survey and statistical analysis to uncover the specific characteristics and patterns of telecom frauds that are increasingly affecting college students. Utilizing data from a comprehensive big data platform, the study examines these frauds across several dimensions including the type of fraud, nature, gender of the victims, timing of incidents, and financial stakes involved. The analysis reveals distinct patterns and victim profiles, enabling the formulation of precise preventive measures. This paper proposes a dual approach combining digital cultural insights with empirical data to devise effective strategies and implementation pathways for managing and mitigating telecom network fraud risks in academic settings. The goal is to develop a scientifically grounded, culturally aware prevention and control mechanism that aligns with the digital realities faced by today's college students.
Keywords: Digital Cultural; Colleges and Universities; Telecom Network Fraud; Surveys Statistics

1. INTRODUCTION

Industries such as telecommunications, finance, e-commerce, and third-party payment platforms have developed more rapidly with the increasing prevalence of the Internet. People's daily behaviors and activities tend to be highly networked digital socialization. The youth, in the era of big data, have become the main group of people who use the Internet as a medium for convenient shopping, making friends, and acquiring various kinds of knowledge. The *50th Statistical Report on China's Internet Development,* released by the China Internet Network Information Center in September 2022,

showed that the number of Internet users in China was 1.051 billion, and the Internet penetration rate reached 74.4% as of June 2022. Internet users aged 10-19 and 20-29 accounted for 13.5 and 17.2%, respectively (Zamir & Wang, 2023). The number of mobile Internet users reached 1.047 billion, which accounted for 99.6 percent of the total Internet users (Valkenburg et al., 2006). The youth group has emerged as the predominant force in the realm of the Internet, with its proportion witnessing a steady annual growth. Fraudulent crime through telecommunication networks has become an increasingly serious social problem, particularly affecting college students who are frequent users of such networks (Liao et al., 2022). College students are at the early stage of psychological adulthood, with a simple social experience from the middle school campus to the college campus (Liu et al., 2021). It makes them weak in the early warning perception of social illegal and harmful information, including telecom network frauds in colleges and universities. The level of awareness regarding personal information security protection is relatively increasing the likelihood of falling victim to such crimes. The work used the big data platform for empirical research. A total of 2,830 telecom network fraud cases in 14 colleges and universities from January 1, 2017, to June 30, 2022, were taken as research samples (the big data platform in East China) (Tang & Wang, 2024). The focus laid on the data analysis of key case types, crime timing, victim gender, and platform involvement. The current laws and related characteristics of telecommunications network fraud in colleges and universities have been deeply explored (Shafiq, 2016). A scientific and effective education mechanism for the prevention and control of telecom network frauds in colleges and universities was constructed based on the perspectives of higher education, law, management, and crime prevention. Factual basis and reference were provided for effective countermeasures and methods to prevent and reduce such cases (Valkenburg & Peter, 2007).

2. RESEARCH OBJECT

2.1 Definition of Telecom Network Frauds in Colleges and Universities

Telecom network fraud is an act of defrauding significant public and private property through various information technology means such as telecommunications and networks, with the intention of illegal possession by distorting facts or concealing the truth (Liu et al., 2021). The concept of telecom network frauds in colleges and universities is defined as the occurrence of fraudulent activities targeting college students on campus

based on judicial practices and statistical requirements.

2.2 Data Source and Description

A total of 3,140 telecom network fraud cases were verified on the campuses of 14 colleges and universities in East China between January 1, 2017, and June 30, 2022 (Özmete & Pak, 2022). Data were based on the records from big data platforms of the judicial department and the university security department. The work took 2,830 cases as analysis samples for an empirical analysis of the current situation of telecom network frauds in colleges and universities to explore its significant characteristics and the law of occurrence (Moreira et al., 2021). Specific colleges and universities with cases located were not listed due to information desensitization and other related considerations.

3. CHARACTERISTIC ANALYSIS OF TELECOM NETWORK FRAUD CASES IN COLLEGES AND UNIVERSITIES

3.1 Characteristic Analysis

3.1.1 Diversity of Case Types

The criminals of telecom network frauds are skilled in combining fraud methods with the hot social phenomena of the Internet such as e-commerce, finance, social networking, and we-media (Kraut et al., 2002). Different false information is made up to trick people into being cheated. Criminals use various tactics and communication skills to lure college students into falling for their scams with the rapid development of related industries. Current telecom network frauds in colleges and universities mainly present 16 different types after classifying 2,830 telecom network fraud cases (Malecki & Demaray, 2003). They mainly include loan fraud, gambling fraud, rebate fraud, shopping fraud, dating fraud, naked chat and pornography fraud, impersonating public prosecution fraud, impersonating friends/leaders/acquaintances fraud, false information fraud, impersonating express fraud, click farming fraud, investment fraud, game and service transaction fraud, recruitment fraud, lottery fraud, and online banking theft (Hayes & Scharkow, 2013). These types show remarkable diversity. Frauds of shopping, impersonating friends/leaders/acquaintances, click farming, and game and service transaction are the most common through the classification and analysis of the above cases; they account for about 70% of the total number. Shopping fraud ranks first, accounting for 27.4% of the overall cases. Loan fraud,

dating fraud, and recruitment fraud occur frequently (Table 1).

Table 1: Frequency Distribution of Involved Types

Case Category	Frequency (Times)	Percentage (%)
Lottery Fraud	21	0.7
Dating Fraud	121	4.3
Impersonating Public Security Organs	46	1.6
Impersonating Leaders, Friends, or Acquaintances	511	18.1
Click Farming Fraud	511	18.1
Express Fraud	53	1.9
Investment Fraud	35	1.2
Employment Fraud	141	5.0
Game Trading Fraud	326	11.5
Online Banking Theft	3	0.1
False Information Fraud	63	2.2
Nude Chats and Porn Scams	25	0.9
Shopping Fraud	775	27.4
Loan Fraud	129	4.6
Gambling Fraud	2	0.1
Rebate Fraud	68	2.4
Total	2,830	100.0

There are 1,667 cases involving female victims, which represents approximately 58.9% of the total number. Similarly, 1,141 cases involving male victims, which accounts for about 40% of the total number. The gender of victims is unknown in another 22 cases. The work investigates the total number of students, the male-to-female ratio, and the gender disparity among victims in the selected universities. The probability of female college students being abused in telecom network frauds is higher than that of male college students(Table 2).

Table 2: Gender Frequency Distribution of Victims

Case Category	Frequency (Times)	Percentage (%)
Female	1,667	58.9
Male	1,141	40.3
Missing	22	0.8
Total	2,830	100.0

3.1.2 Different Case Types with Great Gender Differences

The similarities and differences of different gender-involved types can be found according to the data sample analysis. Shopping fraud, impersonating friends, leaders, or acquaintances, click-farming fraud, and

game trading fraud are among the most frequently encountered types regardless of gender (Hayes & Scharkow, 2013). The distinction lies in the fact that, for male individuals, there exists no statistically significant disparity in the proportion of the top three categories of engagement within the aforementioned ranking based on crime frequency (Cullen, 1994). The proportion of shopping fraud among female surpasses that of impersonating friends, leaders, and acquaintances and click farming fraud. These frauds are particularly prevalent among female and warrant heightened attention. The incidence rates of shopping fraud, dating fraud, false information fraud, and investment fraud among female students are significantly higher than those of male students (Cobb, 1976). The frequencies of shopping fraud and dating fraud are the highest among female, about twice those of male. The prevalence of false information fraud and investment fraud may not be significant (Chen et al., 2013). However, the incidence rate among female students is three times higher than that among male students, which warrants greater attention. Lottery fraud, impersonating public security fraud, impersonating friends, leaders, acquaintances, and express fraud are four types of cases, with a slightly higher incidence rate among male than female. The frequency of cases in female is significantly higher than that in male among the other 12 types of cases (Fig. 1).

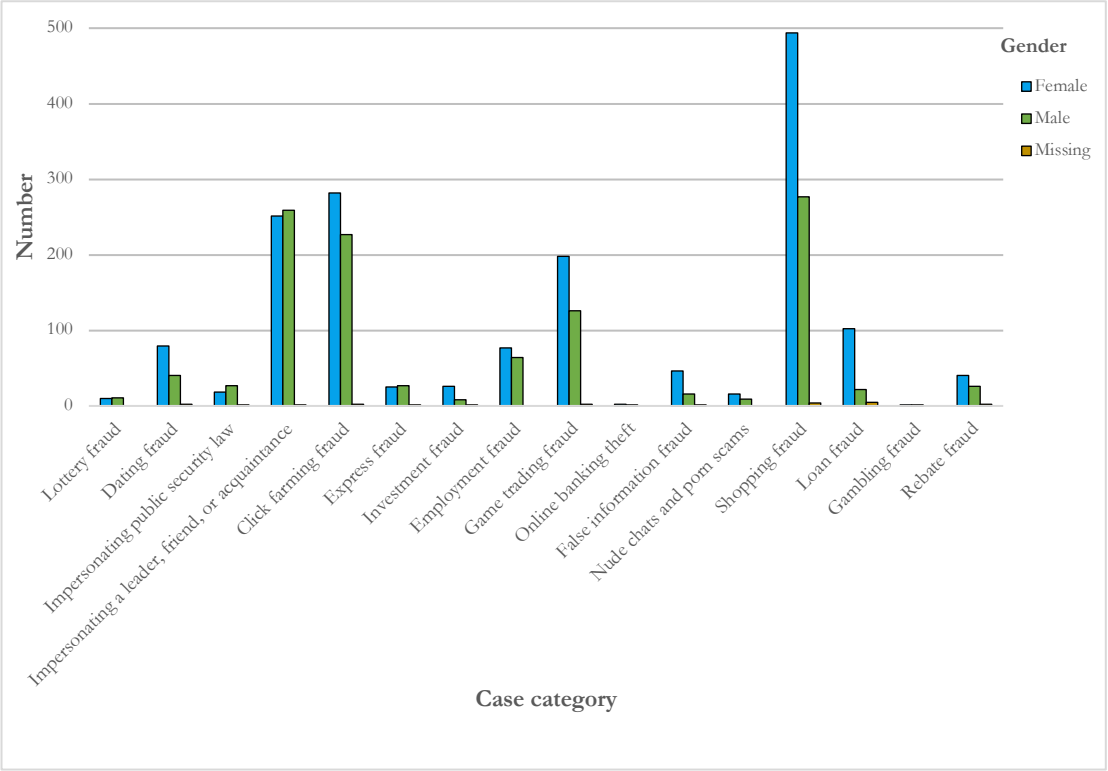


Figure 1: Victims of different genders and number of case types (I)

3.1.3 Significant Grade Stratification in Crime Incidents

Freshman students account for the highest number of cases, with a total of 1,081 cases, representing approximately 40 percent of the overall case count according to the sample data analysis. The number of cases (802 cases) in sophomore year has experienced a decline, which accounts for approximately 30% of the overall case count. Juniors are slightly less frequent than seniors.

The number of crimes shows a downward trend with the increased grade from the general trend. The number of cases in the junior and senior years has decreased significantly compared to the freshman and sophomore years. Nine cases in sample data occur at the graduate level. Data provided by the 14 colleges and universities cannot be used for analysis and reference due to the limited availability of graduate training programs (Table 3).

Table 3: Frequency Distribution of Telecom Network Fraud Cases in Colleges and Universities of all Grades

Crime Grade	Frequency (Times)	Percentage (%)
1	1,081	38.2
2	802	28.3
3	441	15.6
4	497	17.6
5	9	0.3
Total	2,830	100.0

Note: Five is the number code for graduate students.

3.1.4 Different Types of High-Incidence Cases in Each Grade

The freshman stage is the high incidence period of the case type of impersonating leaders, friends, or acquaintances through the data analysis of the case grade stage (Carranza, 2022). The most common type of case in the sophomore, junior, and senior years is mainly shopping fraud. The total number of telecom network fraud cases in the senior year decreases significantly compared with that in the freshman and sophomore years (Caplan, 2003). However, the frequency of loan fraud cases at the senior stage increases significantly, which exceeds the sum of such cases at the freshman, sophomore, and junior stages. The types of nude chats and porn scams account for a small proportion of the total number. The number of such cases increases significantly at the senior stage, which is about 2 times that of the freshman and sophomore stages and 3 times that of the junior stage.

3.1.5 Regularity in the Occurrence Month

The occurrence time (month) of telecom network frauds in colleges and universities is significantly influenced by the characteristics of academic semesters and holidays according to the analysis of the occurrence time of sample data (Bessière et al., 2008). The highest proportion of cases is about 13.7% in October; the lowest is about 1.3% in February. Significant differences exist in the number of cases from January to February, July to August, and winter and summer vacation compared to the spring and autumn semesters from March to June and September to December. The most frequent cases occur in March, April, and May and in October, November, and December (Table 4).

Table 4: Frequency Distribution in the Month of the Cases

Month Of Cases	Frequency (Times)	Percentage (%)
1	160	5.7
2	37	1.3
3	272	9.6
4	288	10.2
5	293	10.4
6	247	8.7
7	103	3.6
8	63	2.2
9	271	9.6
10	388	13.7
11	376	13.3
12	332	11.7
Total	2,830	100.0

3.1.6 Months of Concentration in Each Case Type

The data sample set analyzed in the work, spanning from 2017 to the first half of 2022 and with a capacity of 2830, reveals that shopping fraud emerges as the predominant case type across all months, except for February and October (Table 4). October witnesses the highest number of impersonating leaders, friends, or acquaintances throughout the year, which accounts for approximately 21% of the annual total. The largest proportion of shopping fraud is the highest in November of all the types involved, accounting for about 14% of the year (Table 5).

3.1.7 Medium Loss Mainly Constitutes the Amount Involved

A total of 2,830 telecom network fraud cases occurred in 14 universities between 2017 and the first half of 2022, which are divided into the low loss

(0-999 yuan), medium loss (1,000-9,999 yuan), high loss (10,000-49,999 yuan) and ultra-high loss (more than 50,000 yuan) according to the amount involved. The medium loss level of students who are cheated between 1,000 and 9,999 yuan is significantly high according to the data analysis, accounting for about 63% of the total. Students are cheated of less than 1,000 yuan in about 22% of cases. The cases of being cheated of 10,000 to 50,000 yuan account for about 13% of the total number, and the cases of being cheated of more than 50,000 yuan account for about 2%. The highest amount of money involved in the case is as much as 400,000 yuan (Fig. 2).

Table 5: Frequency Distribution of Cases in each Month

		Month												
		1	2	3	4	5	6	7	8	9	10	11	12	Total
Case Category	Lottery Fraud	0	0	0	1	2	2	2	1	4	2	3	4	21
	Dating Fraud	8	0	9	17	12	16	2	3	10	12	15	17	121
	Impersonating Public Security Organs	4	0	1	5	3	2	3	3	11	5	3	6	46
	Impersonating Leaders, Friends, or Acquaintances	30	8	43	28	52	40	14	10	51	105	68	62	511
	Click Farming Fraud	29	5	48	59	48	39	16	9	56	67	74	61	511
	Express Fraud	1	0	4	5	6	1	2	0	7	13	9	5	53
	Investment Fraud	3	3	0	4	0	6	1	2	4	5	3	4	35
	Employment Fraud	7	5	18	17	7	10	11	2	13	17	23	11	141
	Game Trading Fraud	14	5	39	54	35	18	4	4	23	43	37	50	326
	Online Banking Theft	0	1	0	0	1	0	0	0	1	0	0	0	3
	False Information Fraud	6	2	1	4	17	9	5	1	7	2	5	4	63
	Nude Chats and Porn Scams	2	1	2	2	2	4	0	3	3	1	1	4	25
	Shopping Fraud	40	6	92	66	91	74	35	18	67	93	110	83	775
	Loan Fraud	11	1	13	18	7	17	8	6	11	11	16	10	129
	Gambling Fraud	0	0	0	0	0	0	0	0	0	0	1	1	2
	Rebate Fraud	5	0	2	8	10	9	0	1	3	12	8	10	68
	Total	160	37	272	288	293	247	103	63	271	388	376	332	2830

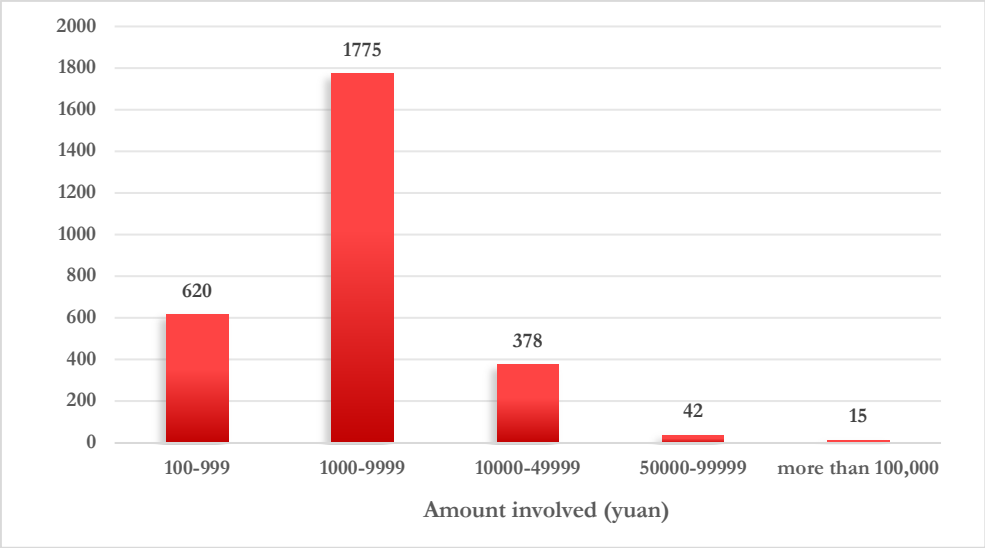
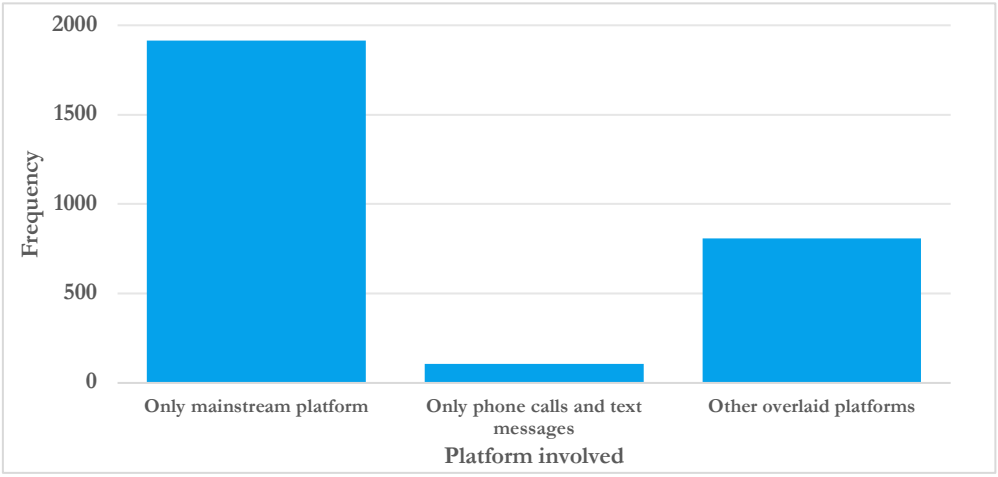


Figure 2: Amount Involved in the Telecom Network Fraud Cases in Colleges and Universities

3.1.8 Variability in the Platform Involved

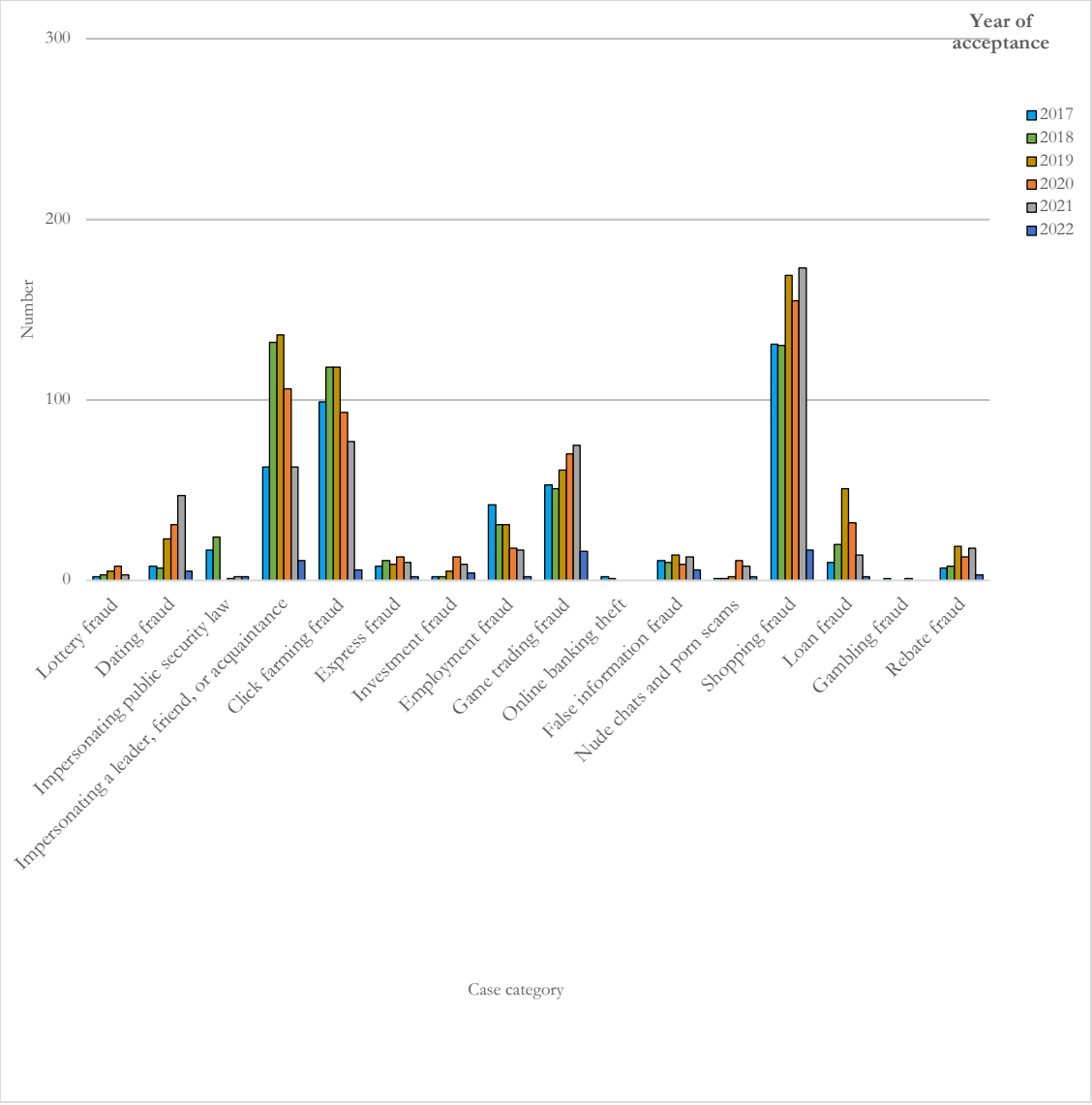
About 1,914 of the 2,830 telecom network fraud cases in the data sample set only involve formal, mainstream transaction payment, and social media single platforms, e.g., Taobao, online banking, Alipay, WeChat, Xianyu, Tmall, Pinduoduo, QQ, Weibo, Jingdong, Douyin, and Xiaohongshu, The proportion is 67.6%, almost 70% of the total. Only 107 cases involve phone calls and text messages alone, which account for less than 4%. Therefore, internet fraud is significantly higher than phone and SMS fraud. Besides, 28.6% of telecom fraud cases are outside the formal, mainstream transaction payment, and social media platforms mentioned above. One or more network telecom platforms of unknown origin are used for frauds (Fig. 3).



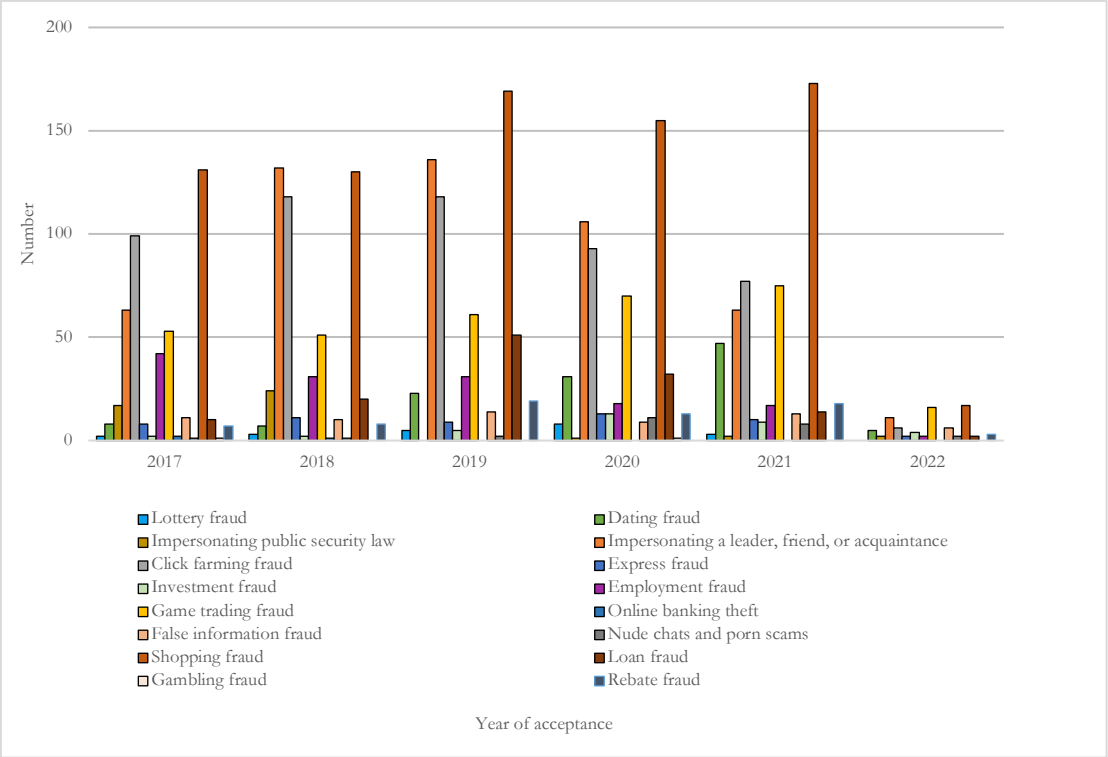
Figur 3: Platform Involved in Telecom Network Fraud Cases in Colleges and Universities

3.1.9 Trend Analysis of Case Types

The frequencies of shopping fraud, game trading fraud, and dating fraud show a significant upward trend from 2017 to 2021 among the 16 main case types during the sampling period by analyzing the sample data, with the peak occurring in 2021 (Table 8 and Figs. 11 and 12). The year 2019 is taken as the dividing line for the four categories of impersonating friends, acquaintances, or leaders, click farming fraud, loan fraud, and nude chats and porn scams take. It shows an upward trend before 2019 and a downward trend after 2019. The overall trend shows that the types of cases are approximately based on 2019 as the boundary point judging from the year of acceptance, with the distribution characteristics of rising first and then falling. Sample data, collected from January to June 2022, are not compared in the trend analysis of case types (Figs. 4).



(a): Types of Cases in Each Year



(b): Types of Cases in each Year
Figure 4: Types of Cases in each Year

4. PREVENTION MEASURES OF TELECOM NETWORK FRAUDS IN COLLEGES AND UNIVERSITIES

Telecom network frauds in colleges and universities are a specific form of social fraudulent crime (Beachum, 2018). They are different from common fraud cases in the aspects of publicity prevention, public security management, and disposal process due to the particularity of victims and fields. College students lack social experience, with weaker safety awareness and psychological resilience. The ability to perceive and discern various forms of misinformation is inadequate, which renders individuals highly susceptible to becoming targets of fraudulent criminals. College students have strong self-esteem and are usually unwilling to actively seek help from others after encountering telecom network frauds or causing losses. Colleges and universities lack the technical and personnel reserves to carry out real-time risk early warning and tracking and handling capabilities for telecom network fraud crimes. The comprehensive prevention and control measures of similar cases can be strengthened to manage telecom network frauds in colleges and universities (Aykanian, 2023). The promotion of the work system and mechanism innovation in colleges and universities is crucial for main responsibilities, particularly in the era of big data.

Enhanced measures should be taken to implement education, publicity, supervision, and management. Thus, a multi-level, comprehensive, highly collaborative, and efficient working mechanism can be established for the proactive prevention and education of telecom network frauds.

4.1 Construction of a Comprehensive and Multi-Dimensional Moral and Legal Literacy Education System

The report of the Party's 20th National Congress stressed that a nation will prosper only when its young people thrive. Young people are vanguard force in which the Party and the people have high trust and high hopes. The Party Central Committee, with Comrade Xi Jinping as its core, attaches great importance to cultivating socialist builders and successors. The colleges and universities, as institutions undertake the sacred mission of "educating individuals for the Party and the nation," should adhere to the fundamental educational task. Gambling fraud, nude chats and porn scams, click farming fraud, and rebate fraud are the most frequent cases among the 16 forms of college telecom network fraud through the analysis of sample data. The process of criminals luring victims with bait and engaging in fraudulent activities exhibits the inherent risk of self-entrapment, leading to acts that contravene legal statutes, public order, and societal norms. The cultivation of morality should be given greater prominence in colleges and universities, with an emphasis on enhancing the methodologies employed for ideological, political, and moral education of college students.

(1)The focus should be placed on the construction of an ideological and moral education curriculum system. Colleges and universities should fully leverage the pivotal role of ideological and moral education, legal education, mental health, and other courses to harness the teachers' subjective initiative. The typical cases and new developments of telecom network frauds in colleges and universities are explained in ideology and politics, social morality, psychological principles, and legal norms. College students' political awareness, online ethics awareness, sense of responsibility, and safety awareness should be cultivated to enhance the psychological knowledge literacy of online society. They possess the ability to discern the dichotomy between right and wrong, fame and profit, idealism and reality, thereby cultivating a robust set of consumption values and a sound social outlook on life. Individuals should enhance their moral judgment and decision-making abilities, eliminate reliance on chance, resist negative temptations, and regulate their words and actions. The prevention of telecom network frauds in colleges and universities should be prioritized from the origin of thought.

(2) The emphasis is placed on the establishment of a dedicated team for full-time and part-time ideological and political education staff. Colleges and universities should establish a proficient team, which has the political theory and is well-versed in the social morality of college students and network social psychology. This team is composed of ideological and political counselors, class teachers, full-time teachers, student backbone, and other full-time and part-time personnel. On the one hand, the guidance and early warning perception of college students' behaviors should be strengthened. On the other hand, the regular exploration of students' daily behaviors and relevant information is essential for a comprehensive understanding and grasp of their needs. Ideological and political education, psychological counseling, and other work should be carried out according to the personality and psychological characteristics of college students in the new era. College students' proactive ability is enhanced to identify and avoid falling into the traps of telecom network fraudsters.

(3) The objective is to establish a conducive cultural milieu on campus. Colleges and universities should strengthen the investment in the construction of campus cultural infrastructure, especially the development of an ecological environment for spiritual civilization. College students should be educated and guided to participate in healthy and upward sports and sports activities. The construction of experiential venues for campus safety culture should be aligned with the current situation to enhance teachers' and students' intuitive understanding of telecom network fraud prevention. Thus, the safety precautions abilities of teachers and students can be improved. The characteristics of college students' online behavior should be given more attention, in conjunction with Campus Safety Month and other promotional and educational activities. Students' cognition of network media, network social morality, and network security can be improved by constructing ideological and political work websites that fit with the characteristics of college students. Students' ability to network technology applications, network participation, and collaboration should be improved for self-development with the network.

4.2 Construction of Multi-Level, Highly Coordinated, and Fraud-Free Campuses

Colleges and universities should engage in continuous exploration, innovation, and practical application to further advance innovation. This will promote the prevention system and mechanism innovation of telecom network frauds on campus. Colleges and universities, as the main body of telecom network fraud prevention, have an inescapable responsibility for

preventive education. The concrete implementation of preventive measures requires enhanced communication among all departments and secondary colleges in preventive education efforts. Besides, supports from families and relevant government departments are needed.

(1) Colleges and universities should give full play to the role of safe-campus leading groups. The publicity, student, security, logistics, and other relevant departments should be coordinated to strengthen communication and cooperation with the secondary colleges. Safety education forms can be continuously innovated by integrating resources and working. Safety education platforms and carriers should be expanded to enrich education forms. The propaganda and education operation mechanism of telecom-network-fraud prevention and control coordinated inside and outside universities and colleges is established by integrating traditional media propaganda and self-media propaganda, media propaganda and anti-fraud full coverage activities layout, anti-fraud full coverage activities and daily dynamic early warning, the anti-fraud propaganda of the police, and the experience of teachers and students in the public security anti-fraud center. Then the pertinence and effectiveness of anti-fraud publicity and education can be improved.

(2) Colleges and universities should analyze the effectiveness and shortcomings of publicity and education in the past according to the characteristics and laws of the occurrence and development of telecom network frauds. The granularity of establishing a fraud-free campus should be enhanced to enforce safety publicity and education responsibilities at all levels. Secondary colleges should establish the consciousness of main responsibility and further promote the creation of fraud-free colleges and universities. The full coverage of anti-fraud activity is included as a topic in the important topics of the class teacher meeting and the student leader assembly at the beginning of each semester. The head teacher and the monitor organize all students in the class to learn the relevant knowledge of telecom network fraud prevention in the form of a thematic class meeting. The construction of fraud-free classes is essential to achieve full coverage of both anti-fraud classes and groups and anti-fraud knowledge content. The dormitory as the smallest unit cell should be fully utilized to ensure safe-campus operations and promote the establishment of a fraud-free living environment. The precision of prevention and control should be improved to make the prevention and control of telecom network frauds comprehensive and accurate.

(3) Colleges and universities should attach importance to the contact with students' parents and other family members. Relevant safety education

propaganda materials including anti-telecom network frauds should be regularly or irregularly pushed to parents as home-school safety collaborative education content. Students and parents should read carefully to improve their awareness of the main types and hazards of college network frauds. Prevention publicity and education for frequent and high-incidence cases can be enhanced with greater accuracy. Colleges and universities should keep in close contact with the public security anti-fraud center, the local police station, and other departments to grasp the latest telecommunications network fraud cases. The types and developing trends of telecom network frauds should be detected. The dynamic early warning should be well implemented based on the actual level of anti-fraud propaganda and education knowledge mastered by teachers and students.

4.3 Fosus on the Multi-Channel, Wide Publicity of Personal-Information Security Prevention

The freshman stage is the most prevalent phase for telecom network frauds, such as impersonating leaders, friends, or acquaintances, based on the analysis of sample data. The transition from primary education to college typically signifies the induction of young students into a wider social sphere, encompassing their involvement in online communities upon entering as freshmen. The social experience during this stage is simple, while individuals tend to exhibit a natural curiosity towards novel stimuli from a psychological perspective. Moreover, their self-assurance is heightened, albeit accompanied by a tendency to place trust in others easily. Their awareness regarding frauds and other illegal activities is insufficient, and their ability to identify fraudulent means is also inadequate. Criminals exploit these characteristics of freshmen to illicitly obtain personal information when freshmen register information and create new service or platform accounts. Finally, accurate frauds can be carried out through the Internet, telephone, SMS, and other communication tools. Most students can realize the hazards caused by telecom network frauds in colleges and universities through the anti-fraud and anti-fraud education received on campus. However, some people have obvious deficiencies in the mechanism of telecom network frauds, anti-fraud awareness, and coping ability. The social activities of college students have become more diverse and personalized due to the enrichment of college life, learning activities, and social practice. There are many channels for requesting individuals to fill in identity information and collect electronic data. The personal information of college students can be easily compromised if apps and website platforms (e.g., games, e-commerce, job search, and intermediaries)

lack robust security systems in the presence of asymmetric information. This will allow criminals to take advantage. Relevant departments of colleges and universities should take the initiative to understand and investigate the channels that college students are susceptible to information leakage. Education, intervention, and correction measures should be promptly provided in view of the above situation. Warning floating windows should be set up on the campus network. Banners and posters can be placed in stores, supermarkets, logistics points, ATMs, and other places where personal information is likely to leak. The ways that can easily cause personal information disclosure are shown to prevent students from inadvertently exposing information to various virtual and real environments. Thus, the chance and probability of criminals obtaining college students' personal information can be reduced from the source.

About 28.6% of telecom network frauds occur outside of formal, mainstream transactions, payment platforms, or social media according to data samples. The criminals use one or more online telecom platforms such as apps to commit frauds. Colleges and universities should strengthen early warning education for students to identify non-mainstream Internet platforms, apps, and illegal websites during prevention and awareness campaigns in view of this remarkable feature. The objective is to enhance students' awareness regarding unknown network links or APP platforms. Students should be educated to exercise caution when clicking on unfamiliar network links and refrain from downloading APP platforms of unknown origins. They can identify frauds in time, wake up quickly, and avoid losses when interacting with others online.

4.4 Improvement of the Dynamic and Innovative Anti-Fraud Early Warning System On Campus

The frequency of telecom network frauds in the freshman and sophomore years is significantly higher than that in the junior and senior years according to sample data. March, April, and May of the spring semester as well as October, November, and December of the autumn semester are the most frequent periods for telecom network frauds in colleges and universities. Colleges and universities should grasp the behavioral cognition characteristics of students according to the occurrence and development of telecom network frauds. The existing "anti-fraud" propaganda and education strategy should be adjusted in time to do a good job in the safety law and discipline education of freshmen. Anti-fraud and anti-corruption knowledge is seamlessly integrated into the practical activities of college students (e.g., self-education, self-

management, and self-service) by leveraging the diverse characteristics exhibited by students at different stages. The establishment and enhancement of the anti-fraud working mechanism on campus should be achieved through the organization of college student volunteers dedicated to promoting social practice during winter and summer vacations as well as in their daily activities. The key measures for prevention, control, education, and response should be implemented targeting specific periods, population types, and characteristics prone to the occurrence of cases. Volunteers can experience and participate in the daily work through contact and cooperation with the Anti-Fraud Center of the public security department. Anti-fraud personnel can provide on-site telephone advice and other assistance to potential victims who may fall victim to telecom network frauds. The research activities on anti-fraud propaganda should be conducted extensively in street communities, towns, and villages. Thus, college student volunteers can intuitively realize the reality and urgency of the anti-fraud work task. The combination of volunteers' work experience and their accumulated expertise in anti-fraud volunteer service will enhance the enthusiasm and initiative to actively participate in the promotion of campus anti-fraud education. The anti-fraud publicity and education activities on campus should be carried out according to seasons, groups, types, and focus. The primary focus should be directed towards targeted prevention of shopping fraud, express fraud, and click farming fraud before the extensive promotional campaigns conducted by e-commerce shopping platforms in November and December, as these represent prevalent forms of online shopping deception. The campus should foster an anti-fraud working environment where individuals are held accountable as the primary guardians against fraudulent activities. The sense of responsibility and mission of students should be strengthened through a series of measures to resist the temptation of misinformation and prevent and reduce the likelihood of telecom network frauds in colleges and universities. The analysis of students' grades and cases should be enhanced by colleges and universities to carry out targeted prevention. The graduating seniors believe that they have gained significant social experience during their four years of college life, and the academic burden they carry is more substantial compared to the earlier years. Individuals often exhibit a heightened desire for social recognition when preparing to enter society, which leads to increased fluctuations in their self-esteem and vanity compared to previous stages. Some people may have the phenomenon of psychological satisfaction through comparison with each other. Most of the students' financial resources are still from their parents'

regular remittance of living expenses, with narrow channels for obtaining funds. The insufficiency of available funds to satisfy one's desires, coupled with the reluctance to easily seek financial assistance from parents, may lead individuals to fall victim to meticulously prepared fraudulent schemes orchestrated by scammers. Special prevention education for high-incidence cases should be strengthened, such as shopping fraud, loan fraud, nude chats, and porn scams in the senior stage. Female students should focus on shopping fraud and more prevalent dating fraud as well as specialized prevention education on false information fraud and investment fraud. Prevention education in male groups should be strengthened to address cases such as lottery fraud, impersonating public security organs, impersonating leaders, friends, or acquaintances, and express fraud.

5. CONCLUSION

The work started from the needs of campus security construction and social stability based on the background of the big data era. The sample data of telecom network frauds in 14 colleges and universities in East China from 2017 to the first half of 2022 were empirically analyzed. Outstanding features were comprehensively analyzed such as the occurrence time, involved people and amount of money, and laws in current colleges and universities. The preventive measures and implementation paths of college telecom network frauds were put forward based on this. Results offer a crucial reference framework and practical guidance for establishing a scientific and efficient mechanism to prevent and control telecom network frauds in colleges and universities. Thus, a secure and stable campus environment can be fostered. The socio-economic development of mainland China is unbalanced, with large cultural differences between different regions. Telecom network frauds in colleges and universities are multifaceted, and aforementioned research mentioned in the work may not provide a comprehensive depiction of the entire landscape of telecom networks in colleges and universities in the new era. The campus is the main place for college students' activities, which undertakes the sacred mission of cultivating people. Colleges and universities should attach importance to the advantage of academic resources and strengthen education and research on the prevention of telecom network frauds. The telecom network fraud prevention work should be integrated into teaching, scientific research, local services, and other activities. The full potential of cultural communication in colleges and universities should be harnessed to

provide intellectual support and academic references for social gatherings, thereby enhancing crime prevention. Colleges and universities should play the main role in the prevention and control of telecom network frauds and use big data platforms for detection. The collection and analysis of information on telecom network fraud cases should be enhanced, while education management and internal prevention and control systems need to be improved. The active participation of the entire society should be mobilized to prevent and mitigate instances of telecom network frauds on campus. An advanced model is provided for the community to prevent and reduce the occurrence of such cases.

6. ACKNOWLEDGMENT

The work is the phased result of the Special-Task Project of Humanities and Social Science Research of the Ministry of Education (College Counselor Research), "Research on the Construction of Telecom Network Fraud Prevention and Control Mechanism in Colleges and Universities under Big Data" (Grant No. 22JDSZ3176).

Data Availability Statement

Data will be made available upon request/reasonable request.

References

Aykanian, A. (2023). A qualitative exploration of frontline homeless service worker experiences during the COVID-19 pandemic. *Journal of Social Service Research*, *49*(1), 67-78.

Beachum, F. D. (2018). The Every Student Succeeds Act and multicultural education: A critical race theory analysis. *Teachers College Record*, *120*(13), 1-18.

Bessière, K., Kiesler, S., Kraut, R., & Boneva, B. S. (2008). Effects of Internet use and social resources on changes in depression. *Information, Community & Society*, *11*(1), 47-70.

Caplan, S. E. (2003). Preference for online social interaction: A theory of problematic Internet use and psychosocial well-being. *Communication research*, *30*(6), 625-648.

Carranza, M. (2022). The cost of "A better life": children left behind—Beyond ambiguous loss. *Journal of Family Issues*, *43*(12), 3218-3243.

Chen, Y., Zhu, L., & Chen, Z. (2013). Family income affects children's altruistic behavior in the dictator game. *PloS one*, *8*(11), e80419.

Cobb, S. (1976). Social support as a moderator of life stress. *Psychosomatic medicine*.

Cullen, F. T. (1994). Social support as an organizing concept for criminology: Presidential address to the Academy of Criminal Justice Sciences. *Justice Quarterly*, *11*(4), 527-559.

Hayes, A. F., & Scharkow, M. (2013). The relative trustworthiness of inferential tests

of the indirect effect in statistical mediation analysis: does method really matter? *Psychological science*, *24*(10), 1918-1927.

Kraut, R., Kiesler, S., Boneva, B., Cummings, J., Helgeson, V., & Crawford, A. (2002). Internet paradox revisited. *Journal of social issues*, *58*(1), 49-74.

Liao, K., Liu, Z., & Li, B. (2022). The effect of psychological capital and role conflict on the academic entrepreneurial intents of chinese teachers in higher education: A study based on the theory of planned behavior. *Frontiers in Psychology*, *13*, 793408.

Liu, F., Vadivel, B., Rezvani, E., & Namaziandost, E. (2021). Using games to promote English as a foreign language learners' willingness to communicate: Potential effects and teachers' attitude in focus. *Frontiers in Psychology*, *12*, 762447.

Malecki, C. K., & Demaray, M. K. (2003). What type of support do they need? Investigating student adjustment as related to emotional, informational, appraisal, and instrumental support. *School psychology quarterly*, *18*(3), 231.

Moreira, A. L., Yunes, M. Â. M., Nascimento, C. R. R., & Bedin, L. M. (2021). Children's subjective well-being, peer relationships and resilience: An integrative literature review. *Child Indicators Research*, *14*(5), 1723-1742.

Özmete, E., & Pak, M. (2022). Life course parent–child Relationships: Associations between childhood trauma experiences and filial piety among young adults in Turkey. *Journal of Social Service Research*, *48*(4), 561-576.

Shafiq, M. R. (2016). *A forward genetic approach to isolate Arabidopsis mutants altered in the regulation of the ALDH7B4 gene* Universitäts-und Landesbibliothek Bonn].

Tang, J., & Wang, J. (2024). Relationship Among Internet Use, Social Support and Financial Well-Being: Based on the Empirical Survey. *Journal of Social Service Research*, 1-14.

Valkenburg, P. M., & Peter, J. (2007). Internet communication and its relation to well-being: Identifying some underlying mechanisms. *Media Psychology*, *9*(1), 43-58.

Valkenburg, P. M., Peter, J., & Schouten, A. P. (2006). Friend networking sites and their relationship to adolescents' well-being and social self-esteem. *CyberPsychology & behavior*, *9*(5), 584-590.

Zamir, S., & Wang, Z. (2023). Uncovering Covid-19, distance learning, and educational inequality in rural areas of Pakistan and China: a situational analysis method. *Humanities and Social Sciences Communications*, *10*(1), 1-13.