Vol.5 Iss.3 2024 Communication & Education Review
https://doi.org/10.37420/j.cer.2024.036

On the Exploration and Practice of the Anti-Fraud Work System of College Students under the Perspective of "Three-Fully Education" —— Take Shenzhen Polytechnic University as an Example

Jingkang Pang [1], Jidong Chen[2], Hong Chen[3], Xiaobing Li[4]
School of Architectural Engineering, Shenzhen Polytechnic University, Guangdong, China
***Corresponding author,E-mail:lixiaobing@szpu.edu.cn**

Abstract:
In recent years, college students have suffered from frequent Internet fraud incidents. Criminals make use of students' vanity, petty profit, and simple mentality, taking a variety of fraud means, resulting in some students bearing huge property losses and mental pressure. Telecom fraud has gradually evolved into a serious social problem, and now domestic colleges and universities have become the hardest hit areas of telecom network fraud, and many problems exposed behind it deserve our deep reflection. The paper has analyzed college students' telecom fraud types and situation, the characteristics of telecom fraud, called on the concept of "three-fully education", which explores the problem by "fully improving ideological understanding", "fully accurate classification management," "fully intensifying governance" to fight fraud work, and improve college students' telecom fraud awareness and self-protection ability.

Keywords:
College students; Telecom fraud; Anti-fraud; Anti-fraud work system

1. Introduction

In recent years, the rapid growth of the Internet in China has significantly enhanced the convenience of people's lives. The utilization of the Internet not only improves the efficiency of information reception and processing but also introduces transformative shifts in people's lifestyles. As per the 50th "Statistical Report on the Development of China's Internet" published by the China Internet Network Information Center (CNNIC) in Beijing, the number of Internet users in China had surged to 1.051 billion by June 2022, marking an impressive internet penetration rate of 74.4%. The advancement of the Internet industry plays a pivotal role in expediting the establishment of a development framework emphasizing "domestic circulation as the core and the dual circulation of domestic and international markets" in China.

Telecom fraud represents a novel form of deceitful schemes orchestrated by criminals through communi-

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

cation channels such as mobile messages, telecommunications, and the Internet. With the swift advancement of China's economy and telecommunications industry, illicit activities exploiting telecom technology for fraudulent purposes have proliferated rapidly, akin to a contagion. Despite the conveniences brought about by the Internet, it has also spawned a host of adverse effects, with telecom fraud standing out among them. This form of fraud not only inflicts financial harm on individuals but also triggers a cascade of detrimental outcomes. It disrupts the normal order of life, impacts social cohesion, and gravely undermines individuals' pursuit of a better life. Consequently, the prevention and containment of telecom fraud have emerged as pivotal components of current security endeavors.

Studies indicate that college students constitute a primary target of telecom fraud. Despite having greater exposure to anti-fraud information and the effectiveness of anti-fraud campaigns within universities, students' inadequate vigilance, inclination to trust, and heavy reliance on the Internet render them particularly susceptible to the perils of telecom scams. When students fall prey to such fraud, the repercussions extend beyond financial losses, plunging them into difficulty and psychological distress, potentially fostering feelings of societal mistrust and existential fear. Hence, universities must discern the evolving patterns and traits of telecom fraud and implement tangible preventive measures to safeguard the well-being of college students.

2. Current Status of Telecom Fraud in Domestic Universities

2.1 Analysis of Characteristics of Telecom Fraud in Domestic Universities

According to statistics, by the end of 2021, telecom network fraud cases in China accounted for over 75% of all reported crimes, inflicting serious financial losses on residents. The characteristics are as follows: Firstly, the criminal tactics have shifted from traditional telephone scams to internet-based fraud and from widespread targeting to more focused schemes. Secondly, telecom fraud crimes progressively adopt centralization, internationalization, organization, and professionalism traits. Thirdly, the complexity of solving cases has escalated. Fourthly, the forms of telecom fraud are evolving rapidly, with an increasing probability of recurring deceptions.

According to Tencent's "2021 Telecom Network Fraud Governance Research Report", individuals aged "20-29 years old" represented the largest victims at 41%, indicating that college students are at high risk for falling prey to telecom fraud.

2.2 Overview of Fraudulent Cases in Our University

Currently, there is a noticeable uptick in fraudulent cases in society, characterized by diverse and evolving methods of crime, posing challenges to prevention efforts. Data reveals that between January 1 and April 9, 2023, our university encountered 38 fraud cases involving students, with total losses amounting to tens of thousands of yuan.

Regarding the types of these frauds, prevalent occurrences within our university include rebate-related click farming (11 cases, constituting 28.95%), impersonation scams such as fraudulent customer service (6 cases, making up 15.79%), online scams linked to the purchase of concert tickets (6 cases, accounting for 15.79%), and scams related to the trading of online game accounts and equipment (5 cases, representing

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

13.16%).

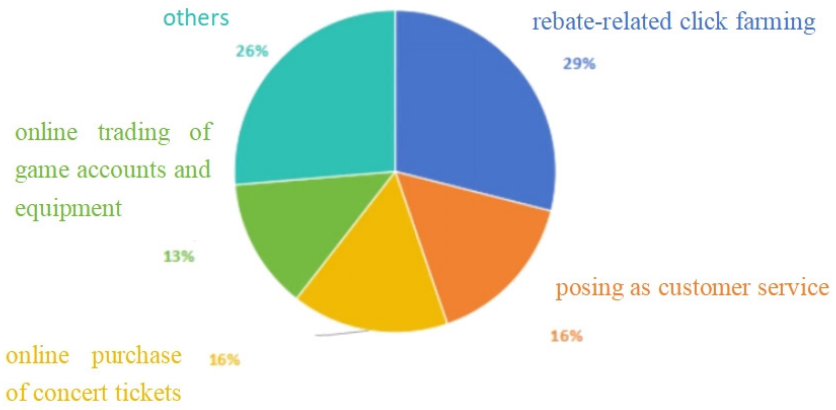


Figure 1: Types of Fraud

When examining the demographics of the victims, while the majority are students, there is a noticeable uptick in faculty and staff falling prey to scams as well. Analysis of data from student residences across various campuses reveals 22 cases at Liuxiandong Campus, 8 cases at Xilihu Campus, 5 cases at Guanlongshan Campus, and 3 cases at Wangtang Apartments. Regarding the gender distribution of student victims, it was evenly split between males and females. A closer look shows that out of 19 female victims, 11 were deceived due to misplaced trust, comprising 57.89% of the total. All 6 instances of falling victim to online concert ticket scams involved females, accounting for 100%. Among the 19 male victims, 8 were duped due to misplaced trust, making up 42.10% of the total, while 6 were enticed by the allure of quick monetary gains, constituting 31.58%. Six cases of being deceived by click farming were males, accounting for 54.55%, while all 2 cases deceived by false sexual enticement were males, accounting for 100%.

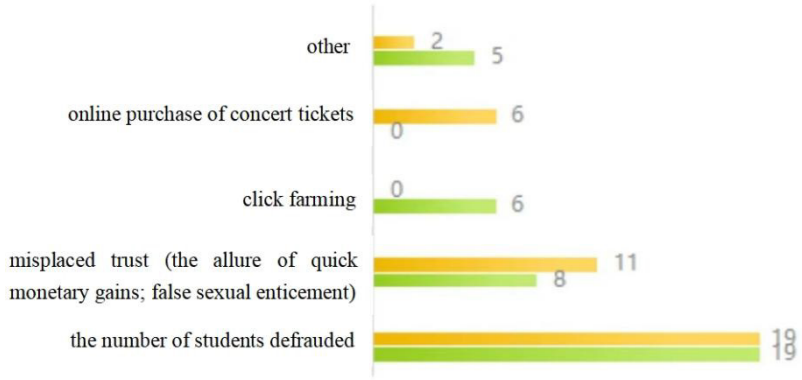


Figure 2: Types of Fraud

Regarding the mediums used by fraudsters, 16 cases involved scams through QQ or QQ groups, accounting for 42.11%, 12 cases were through third-party platforms, making up 31.58%, and 6 cases were through WeChat or WeChat groups, representing 15.79%.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

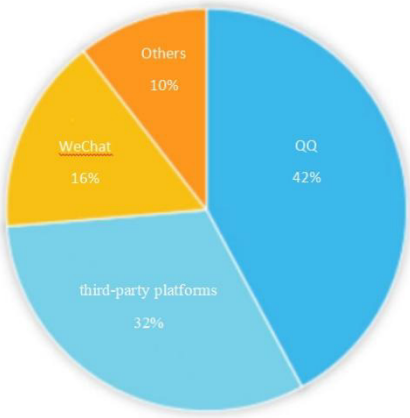


Figure 3: Fraudsters' Contact Mediums

Regarding the fraudulent techniques, fraudsters enticed students to download illegal apps by sharing unknown links out of 15 cases, accounting for 39.47%. Fraudsters obtained students' personal information, such as bank card details and passwords, by screen sharing in 4 cases, making up 10.53%.

Feedback gathered from follow-up interviews with the defrauded students reveals that most acknowledged receiving fraud prevention education from their university or school. However, 14 students displayed a sense of overconfidence, believing they were immune to falling victim to fraud, resulting in a lack of vigilance. Two students mentioned that despite receiving education, they still lacked clarity on the specific methods and tactics employed in various scams. One student highlighted that the constantly evolving strategies of fraudsters surpassed their knowledge, leaving them ill-equipped to counter the deceptive language used by scammers.

2.3 Analysis of the Causes of High-Incidence Fraud Cases

2.3.1 Insufficient Prevention Awareness

In telecom fraud cases, perpetrators primarily capitalize on college students' limited social exposure and inadequate prevention consciousness. Some students desire quick profits and are enticed by trivial gains. Schemes like "click farming" and "lottery scams" ensnare individuals with misleading information, prompting them to interact with fraudsters in pursuit of illusory benefits actively, ultimately falling prey to deceit. Scams such as "impersonating acquaintances" or "posing as customer service" thrive due to a lack of critical thinking and a deficiency in discerning authenticity. Instances like "online shopping refunds" and "express refunds" ensnare individuals, even without losing goods, driven by a craving for minor gains. Frauds like "online purchase of concert tickets" and "trading game accounts and equipment" arise from a lack of social exposure and unwarranted trust in others.

2.3.2 Insufficient Relevance and Engaging Education

The cornerstone of fraud prevention lies in effective awareness campaigns and education. However, in post-scam interviews with students, nearly half admitted that despite receiving anti-fraud education, they still felt invincible. It suggests that educational initiatives have not deeply resonated with students, as they may grasp

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

the concept of fraud but struggle to apply it to their daily lives, particularly in realms like online shopping and social media interactions.

2.3.3 Varied Scam Types and Rapid Evolution of Methods

Cyber scams are evolving into more covert, diverse, and intelligent forms, with fraudsters often well-versed in systematic scamming techniques. Operating in organized networks, they employ tailored tactics based on the age, identity, gender, and location of their targets, making it arduous for victims to fend off attacks. Without timely insights into the latest scamming methodologies, individuals in campus settings lack the robust capacity to identify and thwart emerging fraud schemes.

3. The "three-fully education" Anti-Fraud Initiative

To tackle the issue of students' limited awareness in preventing emerging illicit activities on telecommunications networks at the root and to consistently elevate the ethos of "never let one's guard down" and the urgency of "time waits for no one", concerted efforts are underway to bolster comprehensive governance and expedite the establishment of an enduring framework to combat telecommunications fraud effectively. A campus-wide alert is in effect to heighten anti-fraud consciousness, strengthen defense mechanisms to protect assets and personal safety and uphold campus security and stability. In alignment with the university's practical initiatives and the ethos of "three-fully education", a customized anti-telecommunications network fraud prevention strategy tailored to the university's context is being devised.

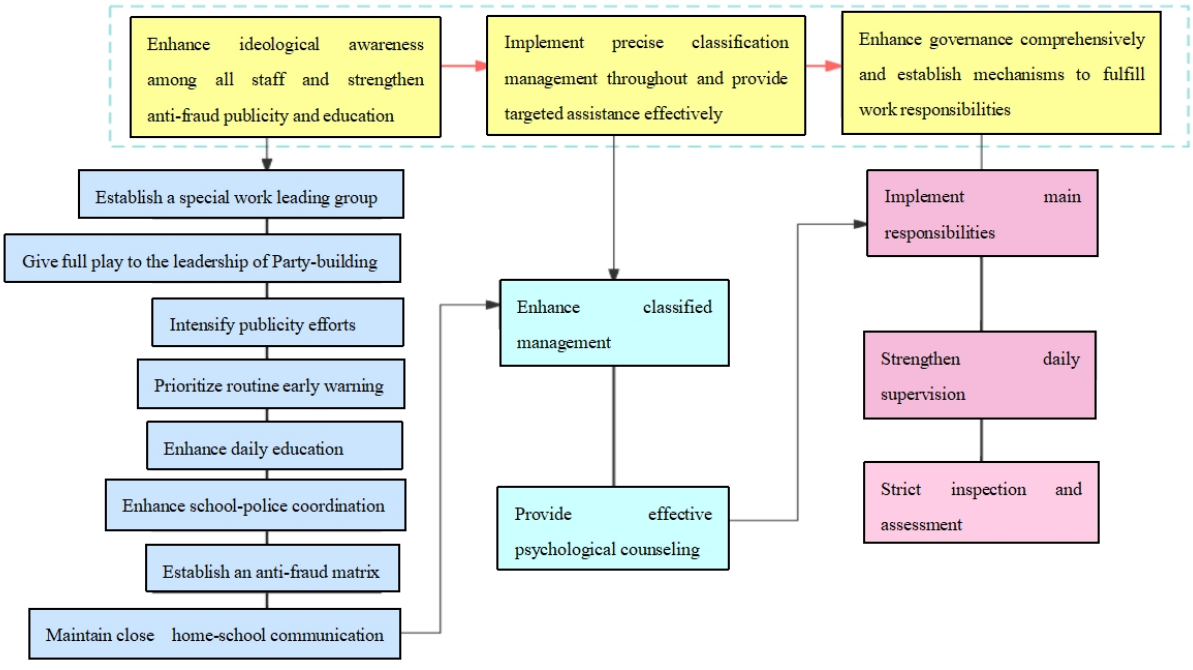


Figure 4: Anti-fraud Work System Based on the concept of "three-fully education"

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

3.1 Enhancing Ideological Awareness Among All Staff, Strengthening Anti-Fraud Propaganda and Education

3.1.1 Establishment of a Special Task Force, Maximizing the Role of Party Building

To fully harness the leadership influence of party building, bolster unified guidance, ensure the effective execution of anti-fraud initiatives within the university, and uphold the normalcy of educational operations, a specialized task force for combating and preventing telecommunications fraud is being instituted. Each secondary school will form a leadership team dedicated to anti-fraud efforts, with top party and government officials serving as leaders, deputy secretaries overseeing student affairs as deputy leaders, and members including heads of comprehensive management offices, student affairs offices, youth league committee secretaries, and counselors. Furthermore, an appointed anti-fraud commissioner will oversee student anti-fraud activities, organizing the planning and execution of anti-telecommunications fraud measures within the unit. This leadership team coordinates and oversees anti-telecommunications fraud prevention efforts, fostering collaboration to establish a coordinated "university-school-class-dormitory" grid network with relevant departments and the School of Architectural Engineering.

Aligned with themed party events, ensure that grassroots party units comprehensively cover anti-fraud knowledge acquisition. All school party members are expected to study and implement anti-fraud messaging diligently. Heighten party members' sense of mission and duty, capitalize on the strength of party units and exemplary members, and assign party-affiliated teachers in each secondary school to deliver anti-fraud education in classes or dormitories at least once per semester. Depending on circumstances, designate student party members to maintain regular contact with 1-3 student dormitories, ensuring continuous dissemination of anti-fraud information and promptly notifying relevant counselors and class instructors of any irregularities.

3.1.2 Boosting Public Awareness, Prioritizing Routine Early Warning

Leverage various platforms, including campus websites, office systems, WeChat official accounts, QQ groups, WeChat groups, electronic displays, promotional boards, banners, campus broadcasts, and promotional brochures to disseminate essential anti-fraud information. The university should actively promote the study of the People's Republic of China Anti-Telecommunications Fraud Law and integrate it into the curriculum. Conduct concentrated promotional activities and learning sessions at least once per semester, mandating the attendance of all staff and students at an anti-fraud lecture to ensure a thorough grasp of anti-fraud concepts and advance anti-fraud education. Increase the adoption of the "National Anti-Fraud Center" app among teachers and students to enhance their defense mechanisms against telecommunication fraud, thereby reducing fraud occurrences and fortifying campus anti-fraud defenses comprehensively.

To address evolving scam tactics, reinforce anti-fraud measures through daily risk alerts, weekly case analyses, and monthly evaluations. The security office should issue daily alerts on scam risks to facilitate risk identification and provide real-time warnings. Weekly case analyses should present typical scam scenarios to bolster the effectiveness of anti-fraud messaging. Monthly telecommunications fraud alerts should be circulated to middle-level leaders and administrators, detailing incidents, patterns, amounts involved, and the handling of fraud cases within the institution.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

3.1.3 Enhancing Daily Education, Strengthening School-Police Collaboration

Utilizing a comprehensive student community management platform, the school conducts awareness campaigns and educational sessions on cyber-security, financial literacy, personal data protection, and responsible spending habits, focusing on prevalent scams such as click farming, job scams, gaming equipment sales, and loan frauds that students are susceptible to. Moreover, the university hosts annual anti-fraud initiatives, including safety education for first-year students, fraud awareness assessments, training for anti-fraud ambassadors, lectures on student safety literacy, microfilm competitions on fraud prevention, anti-fraud knowledge contests, dormitory visits for anti-fraud education, anti-fraud poster design competitions, and "Unity Against Fraud" essay contests, all aimed at instilling a deep-rooted understanding of anti-fraud measures among students.

Enhance collaboration with the Shenzhen City Public Security Bureau, Nanshan District Sub-bureau, and Xili Subdistrict Police Station to gather typical cases and prevention strategies, thereby enhancing the targeted impact and efficacy of educational campaigns, raising awareness of laws among faculty and students and fostering a conscious resistance to fraudulent schemes. Establish a campus anti-fraud consultation platform involving officers from the local police station, security office, institute, and departmental anti-fraud representatives to share updates on anti-fraud efforts regularly, discuss typical cases, offer consultation services, assist students in identifying fraud schemes, and prevent victimization. Simultaneously, establish a swift communication channel with campus police to promptly notify the Xili Subdistrict Police Station of cases involving student fund transfers for immediate freezing, minimizing student losses.

3.1.4 Establishing an Anti-Fraud Network, Enhancing Home-School Collaboration

Our university has implemented several initiatives in response to the escalating issue of campus fraud. Firstly, we have formed a campus anti-fraud task force comprising anti-fraud commissioners from secondary schools and volunteers from various departments. They diligently monitor campus fraud activities daily, swiftly identifying and addressing issues. Additionally, we have assembled a team of college-level anti-fraud commissioners appointed by secondary schools to ensure thorough and expert execution of anti-fraud measures within the colleges. Secomdly, to bolster anti-fraud awareness and education, our university has also established a group of dedicated anti-fraud volunteers, including passionate faculty and students committed to the anti-fraud cause. Collaboratively, they deliver anti-fraud education and awareness campaigns in classrooms and dormitories through lectures, distribution of materials, and on-site explanations, equipping students with the knowledge of fraud tactics and prevention strategies.

Moreover, to guarantee the effective implementation of anti-fraud measures, each class has formed a grid management team with counselors as supervisors, class committee members as team leaders, and dormitories as units. This structured approach ensures clear responsibilities and systematic management, ensuring the comprehensive execution of anti-fraud initiatives in every class and dormitory. Through these endeavors, we aim to construct a comprehensive, multi-tiered anti-fraud defense system to protect every student and staff member adequately.

By fortifying the home-school communication channel and disseminating informative letters to parents, such as A Letter to Parents and Anti-Fraud Information for All Students at Shenzhen Polytechnic University,

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

parents are encouraged to enhance education, supervision, and dialogue with their children. They are advised to vigilantly monitor any unusual activities related to their children's bank cards, phone numbers, WeChat accounts, and bank transactions, establishing a robust home-school communication framework to promptly address any concerns and prevent students from falling prey to fraudulent schemes.

3.2 Rigorous Classification Management, Effective Implementation of Key Support Measures

3.2.1 Enhancing Classification Management

Given the prevalence of various types of fraud, it is imperative to heighten our vigilance. These fraudulent activities encompass rebate fraud in online shopping, deceptive online investment and financial schemes, fraudulent online loans, impersonation scams involving e-commerce logistics customer service, and posing as public security, procuratorate, and judicial officials. Other prevalent fraud types include false credit information scams, deceptive shopping and service frauds, impersonation of leaders and acquaintances, fraudulent transactions involving online gaming products, and scams related to marriage and dating. For students, special attention should be directed towards preventing rebate fraud in online shopping, ticket transfer scams for events like concerts, fraudulent transactions in online gaming products, deceptive online shopping schemes, refund scams (posing as customer service), and false social networking scams based on real-life scenarios. Additionally, it is crucial to be mindful of the legal risks associated with the purchase, sale, rental, or lending of mobile phone cards, bank cards, Alipay accounts and other third-party payment accounts, as well as social media accounts such as WeChat and QQ.

3.2.2 Provision of Psychological Counseling

The university significantly emphasizes anti-fraud initiatives and has established a detailed work log. Comprehensive records are maintained for each student who has fallen victim to deception, documenting the circumstances of the fraud, their family background, and the origin of the deceived funds. To effectively support deceived students, the university offers psychological counseling and assistance to ensure they do not endure further harm from telecom fraud, safeguarding their overall well-being. During follow-up sessions with deceived students, the school assesses their financial status. In cases where a student is experiencing significant financial hardships, the school promptly reports this information to relevant authorities of the university to secure temporary financial aid on campus for the affected student, aiding them in overcoming immediate challenges.

3.3 Comprehensive Enhancement of Governance Efforts, Establishing Mechanisms to Ensure Work Responsibilities

3.3.1 Implementation of Primary Responsibilities

As the key entity tasked with combating telecom fraud, secondary schools are responsible for safeguarding the financial security of all faculty and students. In their capacity as the primary decision-makers, the top leadership of these schools must take on leadership roles, personally overseeing and implementing measures to ensure that anti-fraud initiatives on campus are given due attention and effectively executed. To bolster

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

anti-fraud endeavors, each secondary school has set up two communication channels for anti-fraud activities: one between school leaders and anti-fraud experts and another involving counselors, class teachers, and students. These channels facilitate seamless information dissemination, ensuring prompt access to the latest fraud intelligence and swift implementation of preventive measures.

3.3.2 Reinforcement of Routine Supervision

Bi-weekly anti-fraud meetings are held by secondary schools with the security department and police office, where the total number of telecom fraud cases across the entire school is reported monthly. Teachers handling high incidence rates receive supervisory feedback, and those overseeing persistently high-incidence cases must present reports on corrective actions taken during safety meetings and elucidate the situation to school leaders. All counselors must conduct face-to-face anti-fraud education sessions with students each academic year.

3.3.3 Rigorous Inspection and Evaluation

Secondary schools conduct specialized anti-fraud assessments actively every semester. These assessments consider the quantity and scale of fraud cases and comprehensively assess the efficacy of student anti-fraud endeavors. Assessment outcomes serve as a vital benchmark for collective appraisals of student performance at the school. Teachers who have not encountered student fraud cases throughout the year are acknowledged as a form of encouragement and appreciation. This system of rewards aims to enhance the effectiveness of student anti-fraud initiatives, ensuring that students can better safeguard themselves and steer clear of the perils of fraud.

4. Conclusion

This paper examines the current situation at Shenzhen Polytechnic University, integrating the concept of "three-fully education" to approach anti-fraud initiatives from three perspectives. Specifically, it is crucial to intensify anti-fraud publicity and education to boost students' self-preventative consciousness. Moreover, tailored support should be extended to students vulnerable to telecom fraud. Lastly, mechanisms must be established to ensure the fulfillment of work responsibilities, with individuals being answerable and implementation being meticulous at every stage. Anti-fraud activities in universities entail cultivating a campus environment free from fraud and necessitates students enhancing their personal anti-fraud consciousness. Only through a collective commitment to adhering to safety protocols and fortifying self-preventative awareness can we collectively foster a "fraud-free campus". Hence, sustained efforts are imperative to ramp up publicity and education, elevate students' anti-fraud awareness and capabilities, and collaboratively construct a secure and harmonious campus milieu.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)

Author Contributions

Overall planning	Pang Jingkang
Main concept writing and data collection, status data collection and writing	Chen Hong, Chen Jidong
Theory writing and data analysis.	Li Xiaobing
Topic design	Chen Jidong, Li Xiaobing
Data summary	Pang Jingkang, Chen Hong

Acknowledgments

The authors would like to acknowledge the generous support of Jin Xing (MTI candidate) and Dr. Sun Jicheng at the School of Foreign Languages, Shandong University of Technology, for their wonderful English translation of this essay and special thanks for their invaluable feedback and insights during the development of this essay.

References

[1] Luo Zhao (2022). Research on the Construction of a System for Preventing Fraud in Universities—Taking the Anti-Fraud Work of Peizheng College in Guangdong as an Example [J]. Qin Zhi, 2022, (10): 15-17.

[2] Zhu Jiayu, Zhang Duan (2023). Constructing a New Campus Anti-Fraud Model Based on the Characteristics of Universities [J]. Journal of Civil Aviation Flight College of China, 2023, 34(01): 69-71.

[3] Xie Chong Xiaohan (2023). Analysis and Study on Preventing Telecom Fraud Cases in Universities [J]. Journal of Civil Aviation Flight College of China, 2023, 34(02): 64-67.

[4] Zhang Yongjie (2022). Exploration of Innovative Paths for Anti-Fraud Education and Promotion in Universities—Taking the New Media Anti-Fraud Promotion Work of Zhejiang University of Technology as an Example [J]. Educational Progress, 2022, 12(11): 4769-4774.

[5] Huang Lifeng, Zhao Penghui (2023). Enhancing Students' Awareness of Anti-Fraud to Strengthen the Anti-Fraud Defense Lines in Universities [J]. Safe Campus, 2023(12): 45-48.

[6] Yao Dongsheng (2020). Decoding the Dilemma of Combating and Preventing Telecom Fraud in Universities—Taking Shanghai as an Example [J]. Journal of Hubei Police College, 2020, 33(02): 111-116. DOI: 10.19828/j.issn1673-2391.2020.02.012.

© 2024 by the author(s); licensee Mason Publish Group, this work for open access publication is under the Creative Commons Attribution International License (CC BY 4.0). (http://creativecommons.org/licenses/by/4.0/)