Academic Education Publishing House

Economic Society and Humanities Vol. 3 No. 3, 2026

The Generative Logic and Prevention Mechanism of Telecommunications Network Fraud in Universities in the Era of Intelligent Media

Yiping Li

School of Journalism and Communication, Jiangxi Normal University, Nanchang, Jiangxi, China.

Abstract: In the era of intelligent media, technologies including big data, artificial intelligence and algorithmic recommendation are reshaping the pattern of information communication at the underlying logic, which promotes the iterative upgrading of telecommunications network fraud toward intelligence, precision and covertness. Fraudsters leverage digital intelligence tools to accurately capture the psychological and behavioral characteristics of target groups, constructing personalized and scenario-based fraud systems, thereby significantly increasing the level of risk. University students, who are psychologically immature, lack social experience and rely heavily on the Internet, have become the primary targets of fraud. Traditional anti-fraud publicity in universities is inconsistent with communication principles, and can hardly address the logic of emerging fraud and the psychological dilemmas such as cognitive biases of university students, resulting in unsatisfactory preventive effects. At present, it is urgent to adopt a communication studies perspective to systematically analyze the generative logic and practical dilemmas of university telecommunications network fraud in the intelligent media environment, and explore a fraud prevention mechanism suitable for university students' psychological characteristics and digital scenarios, so as to provide theoretical support and practical approaches for enhancing the effectiveness of anti-fraud efforts and safeguarding campus security.

Keywords: Era of Intelligent Media; Communication Studies; Universities; Telecommunications Network Fraud; Generative Logic; Prevention Mechanism

1. Introduction

The popularization and application of digital intelligence technologies have restructured the ecology of information dissemination, opening up new pathways for telecommunications network fraud. This has driven the continuous iteration and upgrading of fraudulent methods while expanding their scope of infringement, posing a severe threat to social stability and campus security [1]. Article 8 of the Anti-Telecom Network Fraud Law of the People's Republic of China explicitly stipulates that relevant departments shall strengthen anti-fraud publicity and education. As a core base for cultivating young talents, universities bear an important responsibility in safeguarding students' property safety and strengthening the anti-fraud line of defense [2]. University students are in a transitional period of psychological maturity, exhibiting prominent psychological traits such as profit-seeking, fluke mentality, blind trust and conformity [3]. Meanwhile, as they remain highly active on various online social platforms, they are highly vulnerable to being precisely targeted and preyed upon by fraudsters through digital and intelligent technologies. Currently, anti-fraud education in universities is still constrained by the traditional one-way indoctrination communication paradigm [4], resulting in a structural misalignment between its communication logic and the laws of information dissemination in the era of intelligent media, as well as the psychological acceptance mechanism of university students. This "sender-centered" model can hardly resist fraudulent offensives that leverage algorithmic precision distribution and iterative situational simulation, nor can it facilitate the in-depth encoding and internalization of anti-fraud information at the cognitive level of the receiver. Consequently, it falls into the paradoxical phenomenon of "full coverage of publicity yet frequent occurrence of fraud victimization". Based on communication theories and against the background of the era of intelligent media,

this study sorts out the generative logic of telecommunications network fraud in universities, analyzes the practical dilemmas of anti-fraud communication, and constructs targeted prevention mechanisms. It aims to help universities improve the effectiveness of anti-fraud efforts and safeguard the physical and mental health as well as property safety of young students.

2. The Generative Logic of Telecommunications Network Fraud in Universities in the Era of Intelligent Media

In the era of intelligent media, technological empowerment has rendered the generative logic of telecommunications network fraud in universities more systematic and manipulative. Fraudsters accurately perceive and leverage the psychological traits of university students, integrate digital intelligence technologies into the entire fraud process while leveraging the characteristics of campus social scenarios, constructing a progressive and interlocking fraud induction system (see Figure 1). This has significantly enhanced the deceptiveness and success rate of fraud, and also brought brand-new challenges to anti-fraud practices in universities.

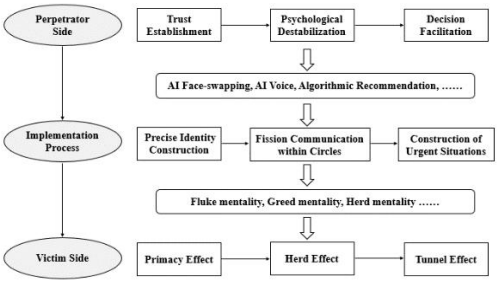

Figure 1. Generation Logic Framework for the Whole Process of Student Fraud Victimization

2.1 Trust Establishment: Precise Identity Construction and Strengthening of the "Primacy Effect"

In the information-overloaded intelligent media environment, university students often lack sufficient time to screen massive amounts of information, making information they encounter for the first time more likely to leave a deep impression on their cognition. The core of the "primacy effect [5]" lies in the notion that "first impressions determine subsequent cognition", and the widespread application of digital intelligence technologies has further amplified the influence of this effect. Compared with the crude and single identity disguise in traditional fraud, digital intelligence technologies have provided perpetrators with more sophisticated tools, enabling them to build "targeted personas" around target groups, gain initial trust from university students rapidly at the first contact, and lay an important foundation for the advancement and expansion of subsequent fraud chains.

By integrating cutting-edge technologies such as AI face-swapping, real-time voice synthesis, and big-data user profiling [6], fraudsters can deeply capture students' social networks, academic anxieties, job-seeking needs, and daily life scenarios. Based on this information, they craft virtual identities that closely align with the target's cognitive expectations, significantly enhancing the credibility of their disguises. Furthermore, through techniques such as intelligent generation of fake credentials, replication of standardized official language templates, and intelligent simulation of immersive scenarios, they further reinforce the authority and authenticity of their identities, greatly blurring the boundary between the real and the fake.

Contemporary university students, who have limited social experience and are still in a stage of incomplete psychological development, generally exhibit a low threshold for trusting others, making them more susceptible to favorable first impressions. Exploiting this psychological characteristic, fraudsters use multiple channels such as campus social communities, targeted SMS messaging, and mainstream social media platforms to deliver digitally packaged disguised identities directly to targeted students. By leveraging the "primacy effect", they create a preconceived positive perception that quickly breaks through students' psychological defenses. Once such a preconceived perception is established, students unconsciously lower their guard and develop a sense of identity and psychological dependence on the fraudster. Later, when faced with so-called benefits or urgent task instructions, they are more likely to lose rational judgment, readily believe and spread false information, and ultimately fall into the carefully designed trap.

2.2 Psychological Destabilization: Fission Communication within Circles and Amplification of the "Herd Effect"

With the deep penetration of digital intelligence

technologies into campus scenarios, platforms such as WeChat communities, short-video platforms, and campus-specific mobile applications have become the primary channels through which university students access information and engage in interactive communication. As a result, the characteristics of campus circle-based communication have become increasingly prominent. The essence of the "herd effect [7]" is that "group behavior influences individual decision-making", and the era of intelligent media has provided a natural carrier for this effect through circle-based communication. Fraudsters exploit digital intelligence technologies to amplify group influence, achieve fission-style dissemination of fraudulent information, and expand the scope of victimization.

Campus circles are primarily formed around classes, student clubs, dormitories, and interest groups, characterized by high levels of mutual trust among members and efficient information transmission. These closed and tightly-knit circles make fraudulent information more readily accepted by students. Fraudsters precisely exploit this feature by employing algorithmic recommendation technologies [8] to accurately push "fake profit-making cases" and "screenshots of group participation" to students within targeted circles. They also use AI to generate a large number of fake accounts, creating an illusion of widespread participation and collective benefit within campus communities. Through channels such as short videos and WeChat Moments, they rapidly disseminate fraudulent information, fostering a communication dynamic wherein the entire circle appears to be discussing the scheme.

University students possess a strong sense of belonging to their circles and exhibit pronounced herd behavior. They have relatively limited social experience, weak risk prevention awareness, and a strong desire for economic independence through "low-cost gains". These psychological and behavioral traits are precisely exploited by fraudsters. By means of digital intelligence tools, fraudsters disseminate the "participation scenarios" and "profit screenshots" of victimized students within their respective circles, leading other students to adopt the cognitive bias that "if everyone is doing it, it cannot be problematic". Even when some students harbor doubts, they may abandon rational judgment under group pressure and blindly follow the trend.

Furthermore, fraudsters leverage algorithmic recommendation technologies to continuously capture the browsing preferences and interaction traces of students within these circles. They repeatedly push fraudulent information involving group participation to other students in the same circles, thereby further amplifying the "herd effect", achieving fission-style dissemination of fraudulent information, substantially expanding the reach of fraud, and significantly increasing the likelihood of students becoming victims.

2.3 Decision Facilitation: Construction of Urgent Situations and Triggering of the "Tunnel Effect"

With the rapid iteration of digital intelligence technologies and the widespread adoption of tools such as AI, big data, and instant messaging, university students have become a prime target for fraudsters. The frequent occurrence of various digitally intelligent fraud cases poses serious threats to students' financial security and physical and mental well-being. At the heart of the "tunnel effect [9]" is that "urgent situations constrain cognitive resources", that is, when individuals face a sudden emergency, their attention becomes narrowly fixated on the immediate problem, as if observing the world through a tube, perceiving only a partial view while overlooking holistic information and rational judgment. Technological advancements in the era of intelligent media enable fraudsters to rapidly construct immersive emergency scenarios, compressing students' space for deliberation and trapping them in a tunnel state, ultimately leading to irrational decision-making.

Using AI voice synthesis and instant messaging tools, fraudsters can quickly convey urgent messages to students, such as "account frozen", "suspected involvement in illegal activities", "family member in danger", or "limited quotas". The lifelike tone and realistic scenario reproduction make it difficult for students to distinguish authenticity at first glance. Through big data analysis [10], fraudsters precisely identify students' anxiety points and tailor-make emergency contexts. Leveraging intelligent interactive scripts, they adjust their conversational pace in real time based on students' responses, continuously reinforcing a tense atmosphere and leaving no time for students to verify information.

University students, whose cognitive abilities are still developing and who possess weak risk awareness, are prone to having their cognitive resources heavily occupied in emergency situations. The hyper-realistic emergency environments created by digital intelligence technologies further amplify panic responses, deepening their immersion in the "tunnel effect". In such states, students' attention becomes exclusively fixated on resolving the immediate crisis, rendering them incapable of critically evaluating information authenticity or proactively contacting family, instructors, or authorities for verification. This cognitive constriction may even lead to the neglect of fundamental common-sense judgments. Ultimately, under the stepwise manipulation of fraudsters, students engage in irrational behaviors such as transferring money, disclosing personal information, or providing verification codes, becoming victims of fraud.

3. Communication Dilemmas in Preventing Telecommunications Network Fraud among University Students in the Era of Intelligent Media

Telecommunications network fraud can leverage digital intelligence tools to precisely capture individual psychological vulnerabilities, thereby deepening the "technology-psychology" dual-driven communication model and significantly enhancing the deceptiveness and behavioral manipulation capability of fraudulent information. Based on the "5W" theoretical [11] framework in communication studies, combined with the emerging characteristics of fraud communication in the era of intelligent media and the psychological traits of contemporary university students, this study systematically analyzes the dilemmas in current anti-fraud communication efforts in universities across five dimensions: communicator (who), message (says what), channels (in which channel), receivers (to whom), effect (with what effect). It aims to provide theoretical references and practical approaches for constructing a targeted and effective anti-fraud governance system in universities.

3.1 Communicators (Who): Formalization of Multi-agent Collaboration and Suspension of Trust in Anti-Fraud Relationships

The degree of synergy and the level of expertise among communicators directly determine the overall quality of anti-fraud communication. In terms of subject composition, on-campus administrators and full-time counselors have long served as the core force in anti-fraud communication in universities. The participation of multiple entities such as public security departments, cyberspace administrations, campus communities, parents, and student autonomous organizations remains extremely low. A stereoscopic collaborative communication framework featuring "university-led, departmentally linked, family-school coordinated, and student-involved" has yet to be established. Although some universities have attempted to collaborate with off-campus entities in anti-fraud publicity, such efforts are mostly temporary and ceremonial, lacking sustained coordination mechanisms and clear responsibility division. Consequently, the professional anti-fraud resources of public security departments, the advantages of family supervision from parents, and the community-based dissemination efficacy of student organizations remain significantly underutilized, resulting in a severe deficiency in the synergistic force of anti-fraud communication. In terms of professional competence, anti-fraud personnel within universities typically undertake this work on a part-time basis. They have neither received systematic training in communication psychology or practical anti-fraud methods, nor do they possess the necessary skills to apply digital intelligence technologies. Consequently, the anti-fraud publicity initiatives they design often fail to align with the psychological characteristics and receptivity habits of university students. Meanwhile, universities generally lack compound anti-fraud talent with integrated expertise in communication literacy, psychological knowledge and digital intelligence skills, making it difficult to employ digital intelligence technologies for precision-oriented anti-fraud communication. This has created a considerable competence gap compared with the targeted induction implemented by fraudsters relying on professional teams and digital intelligence tools. Such deficiencies in the professional competencies of relevant subjects directly result in anti-fraud communication remaining extensive and indoctrinatory, which fails to meet the practical needs of fraud prevention in the era of intelligent media, and further undermines overall communication efficacy.

3.2 Message (Says What): Homogenization of Knowledge Production and Unmet Cognitive Demand for Anti-Fraud

The targeted nature and adaptability of communication content directly influence receiver receptivity, and more importantly, determine whether anti-fraud communication can truly resonate with and internalize in the receiver's consciousness. At present, anti-fraud communication in universities is generally plagued by prominent problems of homogeneity, templating, and obsolescence. Such communication is inadequate to cope with the customized, scenario-based, and precision-oriented communication offensive of fraudulent content in the era of intelligent media, thereby significantly undermining the actual effectiveness of anti-fraud publicity. First, there is an insufficient innovation in content. Current anti-fraud communication in universities mainly consists of simple case enumeration, legal provisions preaching, and risk warnings. Anti-fraud content across different universities and scenarios is highly similar, largely characterized by stereotyped publicity rhetoric and fragmented case stacking. It fails to design personalized content in light of university students' grade characteristics, major differences, and daily life scenarios, thus being unable to meet their personalized information needs or stimulate their active attention and emotional resonance. Second, there is an insufficient sense of the times. With the iteration of digital intelligence technologies, new fraudulent methods such as algorithmic fraud and virtual identity fraud are constantly emerging. However, the content of anti-fraud communication in universities is updated in a lagging manner, with inadequate and unspecific interpretations of the operational logic and identification techniques of such new frauds, and a lack of operable countermeasures. Consequently, it fails to provide effective anti-fraud guidance for university students, rendering the communication content bereft of practical application value, making it difficult to help students resist the precise infiltration of digital intelligence fraud.

3.3 Channels (in Which Channel): Mismatch of Media Contexts and Obstruction of Anti-Fraud Experience Channels

The precision of communication channels directly affects communication efficiency. Currently, there is a serious misalignment between the anti-fraud communication channels used in universities and the media habits of university students, resulting in anti-fraud information failing to achieve effective reach and thus being unable to form an effective counterbalance against fraudulent communication. On the one hand, traditional communication channels account for an excessively high proportion, and the communication model is relatively extensive. Anti-fraud publicity in universities still mainly relies on conventional channels such as themed class meetings, campus posters, banners and slogans, and offline lectures. Such channels are not only inefficient in communication and limited in coverage, but also tend to be rigid and unappealing in form, which easily trigger resistance and perfunctory attitudes among university students. This is seriously inconsistent with university students' media usage habits of "frequent internet use and reliance on new media", making it hard to realize efficient delivery of anti-fraud information. On the other hand, digital intelligence communication channels are underutilized and operated irregularly. Although some universities have attempted to deploy new media channels frequently used by university students, such as short-video platforms, campus communities, and WeChat official accounts, they generally suffer from problems including untimely content updates, a serious lack of interactivity, and insufficient precision of algorithmic recommendation. These channels have not been truly integrated into university students' online social circles, nor can they leverage digital technologies such as big data and algorithms to achieve targeted push of anti-fraud information. In contrast, digitally intelligent fraud has long occupied core online channels for university students, realizing fragmented and full-coverage information dissemination through algorithmic recommendation and circle-based fission. As a result, anti-fraud information from universities is overwhelmed by massive volumes of online content, eventually forming a passive situation where "anti-fraud publicity is ignored while fraudulent information is unavoidable", which further weakens the overall effectiveness of anti-fraud communication.

3.4 Receivers (To Whom): Solidification of Cognitive Biases and Pervasiveness of a Fluke

Mentality in Anti-Fraud

The cognitive level, psychological state, and willingness to participate of communication receivers directly affect the effectiveness of communication and are crucial to whether anti-fraud communication can achieve tangible results. As the core receiver for anti-fraud communication in contemporary universities, students characterized as "digital natives", exhibit profound contradictions between their psychological traits and the dissemination logic of fraud in the era of intelligent media. These contradictions hinder the practical implementation of anti-fraud communication information, preventing the formation of effective self-protection barriers. First, cognitive biases are prominent and identification capabilities are insufficient. Although university students have generally been exposed to basic anti-fraud information, their understanding of the communication logic and psychological induction mechanisms underlying digitally intelligent fraud remains vague. They lack the ability to identify common psychological tactics employed by fraudsters and to distinguish emerging fraudulent methods, making them susceptible to the precise manipulation of fraudsters and thus prone to falling into fraud traps. Second, psychological defenses are weak and easily breached. University students are in a transitional stage of psychological maturity, and their psychological vulnerabilities can be precisely targeted and exploited by fraudsters. Even after receiving anti-fraud information, they often fail to uphold their psychological defenses due to inherent psychological weaknesses, resulting in a disconnect between cognition and behavior - namely, "knowing anti-fraud knowledge yet still being defrauded". Third, initiative participation is low and collective communication synergy is inadequate. Affected by traditional anti-fraud communication formats that are monotonous and content that is disconnected from their needs, university students generally exhibit resistance and perfunctory attitudes toward anti-fraud communication. They lack the awareness and willingness to actively acquire and learn anti-fraud knowledge, as well as to disseminate anti-fraud information, which prevents the formation of a campus-wide anti-fraud atmosphere and further weakens the overall efficacy of anti-fraud communication.

3.5 Effects (With What Effect): Hollowing out of Feedback Mechanisms and Rupture of the Closed Loop in Anti-Fraud Communication

The conversion efficiency and long-term effectiveness of anti-fraud communication directly determine the practical value of anti-fraud efforts. At present, the effects of anti-fraud communication in universities remain limited, making it difficult to fundamentally improve the quality of university anti-fraud governance. First, insufficient effect conversion leads to a disconnect between cognition and behavior. Anti-fraud communication in universities largely remains at the superficial level of "information transmission", failing to effectively guide students toward cognitive upgrading and attitudinal change regarding fraud prevention. As a result, although students possess basic anti-fraud knowledge, they remain unable to quickly identify fraud traps or respond rationally when actually confronted with digitally intelligent fraud. This gives rise to the phenomenon of "knowing anti-fraud principles yet still falling victim to scams", meaning the practical value of anti-fraud communication is not fully realized. Second, the absence of a sound feedback mechanism leaves strategy optimization without empirical support. Anti-fraud communication in universities generally lacks well-established feedback channels for communication effectiveness. Feedback from receivers is often collected through rudimentary methods such as simple questionnaires or oral surveys, which fail to accurately capture students' acceptance of anti-fraud communication content and channels, nor do they effectively track students' psychological changes and actual needs. Consequently, shortcomings and issues in the communication process cannot be identified in a timely manner, and the optimization of anti-fraud communication strategies lacks a scientific basis. Third, inadequate long-term mechanisms result in formalism. Anti-fraud communication in universities has not established a dynamic optimization mechanism. Communication strategies remain rigid for extended periods, failing to adjust content, channels, and methods in real time in response to the iterative evolution of digital and intelligent fraud tactics, as well as changes in students' psychological states. This has led to a problematic focus on "form over substance", making it difficult to achieve sustained and precisely targeted anti-fraud communication.

4. Construction of Prevention Mechanisms for Telecommunications Network Fraud in Universities in the Era of Intelligent Media

Universities shoulder the important mission of nurturing talents for the new era. Faced with the complex challenges posed by the spread of telecommunications network fraud in the era of intelligent media, they should base their efforts on the psychological development characteristics of university students and the generative logic of fraud, and take coordinated actions across the four dimensions of "cognition, emotion, volition and action". Taking "cognition" as the foundation, "emotion" as the bond, "volition" as the support, and "action" as the goal, this approach can precisely resolve the current communication dilemmas in anti-fraud publicity in universities, effectively enhance the accuracy, effectiveness and long-term sustainability of anti-fraud communication, prevent and defuse the risks of telecommunications network fraud among university students at the source, and help universities fulfill their responsibilities in cybersecurity education.

4.1 Cognition: Addressing Cognitive Biases, and Consolidating the Cognitive Foundation for Anti-Fraud

As the fundamental prerequisite for anti-fraud efforts, it is necessary to focus on the knowledge gaps that make university students vulnerable to fraud. In the context of the iterative characteristics of fraud tactics in the era of intelligent media, this requires systematically disseminating anti-fraud knowledge, emerging fraud patterns, and prevention techniques to help students establish a clear anti-fraud cognitive framework and discern the underlying logic of fraud. At the same time, targeted interventions should be implemented to overcome students' entrenched cognitive biases and weak identification abilities. Through precision-based and differentiated cognitive cultivation, students can fully grasp the key points of fraud prevention and solidify their cognitive defense line against fraud.

First, optimize the supply of cognitive content to break the homogeneity of knowledge production. In line with the iterative evolution of digitally intelligent fraud, systematically sort out the criminal logic and key identification points of emerging fraud types such as AI face-swapping and algorithmic fraud. Integrate interpretations of psychological mechanisms including the "primacy effect", "herd effect", and "tunnel effect", striking a balance between professionalism and accessibility, while avoiding simplistic legal preaching and the mere piling up of cases.

Second, precisely match communication channels to resolve media-context mismatches. Leverage intelligent channels frequently used by university students, such as short videos, campus communities, and official WeChat accounts, to deliver anti-fraud knowledge accurately through formats such as situational simulations, case deconstructions, and engaging science-based content. Meanwhile, traditional channels including offline lectures and themed class meetings should be retained to accommodate the reception habits of diverse student groups.

Third, implement hierarchical and classified precision cultivation. Strategies should be tailored according to students' grade, major, and psychological characteristics. For freshmen, emphasize the dissemination of foundational anti-fraud knowledge. For upperclassmen, focus on scenario-based knowledge covering part-time job fraud and online loan fraud. For students facing financial difficulties, strengthen guidance to reduce the tendency toward greed-driven risks. This approach aims to resolve the problem of idle cognitive needs.

4.2 Emotion: Bridging Emotional Alienation, and Forging Emotional Consensus on Anti-Fraud

It is essential to break through the limitation of "one-way indoctrination" in traditional anti-fraud publicity and align with the emotional needs of university students. Emotional connections can be established through campus-based cases and empathetic expressions, so as to reduce the rigidity of publicity and enhance the appeal and affinity of anti-fraud content. Meanwhile, targeted measures should be taken to address the insufficient emotional connection and prominent resistance among students in anti-fraud communication. With emotional empowerment to build resonant scenarios, students can be guided to emotionally identify with anti-fraud concepts, thus transforming anti-fraud publicity from "passive reception" to "active acceptance".

First, establish scenario-based emotional resonance carriers, abandon rigid preaching modes, and combine high-frequency scenarios in

university life, such as campus activities, part-time work, further education, and employment, to create anti-fraud short dramas, real-case interviews, and family reminder videos that closely align with students' lived experiences. These forms can evoke emotional resonance among students and weaken their resistance.

Second, strengthen emotional linkage among multiple subjects, break the formalistic dilemma of multi-party collaboration, and promote joint efforts among universities, public security departments, parents and student organizations. Public security police share frontline anti-fraud stories, parents, send family anti-fraud reminders, and student organizations carry out anti-fraud themed community interactions, so as to build an anti-fraud atmosphere of "emotion + responsibility" and resolve the issue of suspended anti-fraud trust relationships.

Third, integrate negative emotional warnings with positive emotional guidance. On one hand, use real fraud cases to convey the harms of fraud and evoke vigilance. On the other hand, disseminate positive narratives, such as deeds of anti-fraud volunteers and successful fraud-avoidance stories, to strengthen students' confidence in fraud prevention. This dual approach helps build an emotional consensus of "everyone participating in fraud prevention".

4.3 Volition: Overcoming Fluke Mentality, and Reinforcing Volitional Support for Anti-Fraud

Fraud schemes often exploit human weaknesses. Therefore, anti-fraud efforts should be made to cultivate university students' anti-fraud willpower and moral character, guiding them to develop a rational judgment, enhancing their ability to identify fraudulent information and resist temptation, and enabling them to maintain firm anti-fraud convictions when confronted with fraudulent traps, avoid being misled by false information, and build a solid ideological defense against fraud. Meanwhile, targeted measures should be taken to address the prevalent fluke mentality and weak psychological defense among university students. Through volitional reinforcement training, university students can be assisted in strengthening their anti-fraud beliefs, resisting fraudulent inducements, and forming a firm resolve characterized by "rejecting fraud and taking proactive precautions".

First, strengthen psychological intervention and guidance. In view of university students' psychological vulnerabilities such as greed, fluke mentality, and herd mentality, the university psychological center carries out anti-fraud psychological counseling and group psychological activities to interpret the psychological induction logic of fraud, helps students recognize their psychological deficiencies, improves psychological defense capabilities, and solves the problem of solidified cognitive bias.

Second, construct regular scenarios for tempering willpower. Through anti-fraud knowledge competitions, scenario simulations, commitment signing and other activities, university students can strengthen their anti-fraud willpower in practice and abandon the fluke mentality that "fraud is distant".

Third, establish an anti-fraud incentive mechanism. Commend anti-fraud volunteer propagandists and students who have successfully avoided fraud. By setting role models in fraud prevention, positive reinforcement strengthens students' anti-fraud willpower. This promotes the internalization of anti-fraud awareness in the heart and externalization in action, and solves the problem of weakened willpower caused by blocked access to anti-fraud experience.

4.4 Action: Integrating Knowledge and Action, and Achieving Implementation of Anti-Fraud Behavior

Transform anti-fraud cognition, emotional identification, and firm volition into practical actions by guiding university students to take the initiative in learning anti-fraud knowledge, participating in anti-fraud publicity, and avoiding fraud risks. Meanwhile, universities should be encouraged to establish anti-fraud practice platforms, enabling students to consolidate their anti-fraud capabilities through practice. Furthermore, targeted interventions should be adopted to tackle the dilemmas of insufficient translation of anti-fraud effects and the disruption of communication closed loops, so as to drive university students to shift from "being aware of fraud prevention" to "practicing fraud prevention" and fundamentally prevent and resolve the risks of telecommunications network fraud among university students.

First, establish a precise behavior guidance system. For various fraud scenarios, operable methods for fraud avoidance and loss prevention

will be provided, including skills for verifying unfamiliar information, transfer early-warning procedures, and help-seeking channels after falling victim to fraud, enabling university students to respond quickly and rationally when encountering scams.

Second, the feedback and optimization mechanism will be improved to overcome the problem of overly vague feedback mechanisms. By integrating online-offline multi-channel feedback pathways, this mechanism systematically collects students' insights on anti-fraud communication, enabling real-time adjustments to content, channels, and methods. This dynamic optimization ensures the continuous improvement of anti-fraud dissemination strategies.

Third, build a practice platform for anti-fraud with full participation, encouraging university students to become anti-fraud volunteers and participate in campus anti-fraud publicity, community anti-fraud promotion, and other activities, thereby fostering a practical atmosphere in which "everyone propagates anti-fraud, everyone guards against fraud". At the same time, collaborate with public security departments and communities to extend anti-fraud practice beyond the campus, normalize anti-fraud behaviors, and ultimately solve the problem of the broken communication loop in anti-fraud dissemination.

5. Conclusion

The essence of preventing and combating telecommunications network fraud on university in the era of intelligent media is an information dissemination counter-campaign that follows the laws of digital-intelligent communication and precisely aligns with the psychological needs of university students. The traditional anti-fraud communication model not only deviates from the core logic of communication science but also fails to adapt to the development trend of digital intelligence communication, resulting in its inability to effectively respond to the precise and diversified communication offensive of new types of fraud and to give full play to the actual effectiveness of anti-fraud communication. In view of the new challenges confronting anti-fraud efforts in universities during the era of intelligent media, it is imperative to adopt a core communication studies perspective, accurately assess the psychological characteristics and cognitive patterns of university students, and establish a systematic, digital-intelligent, and targeted anti-fraud communication and prevention mechanism. Such a mechanism should achieve the precise delivery of anti-fraud information, comprehensively fortify students' psychological defenses against fraud, and foster the autonomous cultivation of fraud-prevention behaviors. In the future, universities should continuously keep pace with the advancement of digital-intelligent technologies, persistently refine their anti-fraud communication strategies, and with sustained efforts, build a robust campus security barrier against fraud, thereby effectively safeguarding young students' property security and promoting their healthy development.

Acknowledgments

This paper was financially supported by the fund of 2024 Annual Project Titled "Research on Behavioral Characteristics and Intervention Strategies of university Student Victims in Fraud Cases" of Jiangxi Provincial University Ideological and Political Education Research Association (No. XSGZ24202), 2024 Annual Research Project Titled "Research on the Construction of a Safety Education System for University Students from the Perspective of the Holistic Approach to National Security" of the National Training and Research Center for University Ideological and Political Work Teams (Jiangxi Normal University), 2025 Annual Special Task Project of Humanities and Social Sciences Research Titled "Exploration on the Construction and Practical Pathways of University-Family-Society Collaborative Education Consortium under the Overlapping Influence Domain Theory" of the Ministry of Education (Research on University Counselors) (No. 25JDSZ3091).

References

[1] Wu Dan. Research on the Generation Mechanism and Governance Construction of Telecommunications Network Fraud Crimes in the Digital Intelligence Era. Journal of Wuhan Public Security Cadre's College, 2025, 39(4): 16-20.

[2] Hou Jiangbo. Research on the Construction of Prevention Mechanism for Telecommunications Network Fraud in Universities under the Background of New Media. Journal of News Research, 2024, 15(12): 161-163.

[3] Wu Zhenghao, Weng Tianfu, & Cheng

Ziliang. A Brief Analysis of the Psychological Characteristics and Prevention Mechanisms of College Students Victimized by Telecommunications Network Fraud. Youth of the Times, 2025, (10): 120-122.

[4] Yang Jianguang, & Chen Si. Research on Problems and Countermeasures of Publicity and Education for Preventing Telecommunications Network Fraud in Universities in the Era of Big Data. Journal of Kunming University of Science and Technology (Social Sciences), 2023, 23(3): 136-142.

[5] Wang Chaoyang, Ye Zichen. Primacy Effect and Cross-Cultural Community Cognition: A Comparative Experiment of Two News Forms from the Perspective of Cultural Dimensions. Journalism & Communication Review, 2023, 76(2): 56-69.

[6] Zheng Zhen. Current Situation, Causes, and Prevention Pathways of University Students Victimized by Telecommunications Network Fraud in the AI Era. Journal of Hunan University of Humanities, Science and Technology, 2025, 42(5): 104-112, 120.

[7] Wang Le, Wang Luyao, Zhang Ziqiong, et al. Research on the Enhancement and Reversal Mechanisms of the Intention and Behavior of Disclosing Others' Privacy in the Social Media Environment. Chinese Journal of Management Science, 2024(3): 1-14.

[8] Li Yeqiang. Thoughts and Countermeasures on the “Information Cocoons” Effect under Algorithmic Push Mechanism. News Tribune, 2020, 34(4): 40-43.

[9] Bai Xiaoli, Jiang Yongzhi. Does Money Shortage Accelerate Mental Depletion? Tunnel Effect under Scarcity Mindset. Psychology: Techniques and Applications, 2025, 13(08): 494-502.

[10] Tao Manjing. Logical Dimensions, Realistic Dilemmas, and Promotion Paths of the Connotative Development of Ideological and Political Education in Universities Driven by Digital Intelligent Technology. Studies in Ideological Education, 2025, (12): 117-121.

[11] Chen Jiyin, & Jia Chaoran. Research on the Challenges and Countermeasures of ChatGPT Technology to National Security: From the Perspective of Communication Studies. Qinghai Social Sciences, 2023, (3): 127-131.