WEP Warwick Evans Publishing

International Journal of Social Sciences and Public Administration

ISSN: 3005-9836 (Print), ISSN: 3005-9585 (Online)
Volume 10, Number 8, Year 2026
DOI: https://doi.org/10.62051/ijsspa.v10n8.15

The Role of Immersive Murder Mystery Games in Preventing Telecom Fraud among College Students

Sirui Xu

Dalian Ocean University, Dalian, Liaoning, China

ABSTRACT

Telecom fraud represents a typical security risk on university campuses, severely undermining campus stability and safety. As fraudulent tactics continue to evolve, traditional anti-fraud models struggle to keep pace with the increasingly severe landscape. Exploring efficient anti-fraud education methods tailored to college students has thus become a priority for higher education institutions, with immersive murder mystery games offering a novel approach to innovating campus anti-fraud initiatives. Grounded in the practical dilemmas of current anti-fraud education and supported by situated learning and experiential education theories, this paper systematically analyzes the core advantages and mechanisms of applying immersive murder mystery games to anti-fraud education for college students. It elucidates their multi-dimensional educational logic and proposes diverse practical pathways for implementation in universities. The study demonstrates that immersive murder mystery games can effectively address the shortcomings of traditional anti-fraud education, enhance its quality and efficacy, and hold significant theoretical and practical value for innovating campus safety education models and strengthening anti-fraud defenses.

KEYWORDS

Immersive Murder Mystery Games; College Students; Telecom Fraud.

1. INTRODUCTION

In an era where online social networking is deeply embedded and digital technologies advance rapidly, college students have emerged as a primary target group for telecom fraud. Such crimes not only directly harm students' financial security and physical and mental well-being but can also trigger campus crises in extreme cases. Meanwhile, telecom fraud exhibits increasingly sophisticated characteristics: greater concealment, diversified typologies, precise targeting, and expanded scope of harm, posing unprecedented challenges to campus anti-fraud governance [1]. Current anti-fraud campaigns largely rely on one-way dissemination models, including lectures by police officers, poster displays, push notifications of anti-fraud articles, and screening of warning videos [2]. These approaches suffer from rigid formats, limited appeal, weak immersion, and unsustainable educational outcomes. Immersive murder mystery games, a popular experiential, interactive, and scenario-based entertainment and educational medium among young people, transform abstract anti-fraud knowledge into tangible, perceptible, participatory, and reflective experiences through role-playing, plot reasoning, scene reconstruction, and emotional resonance. This effectively resolves the persistent issue in traditional education where information "enters the ears but not the heart, reaches the eyes but not the mind."

2. THE HIGH INCIDENCE AND CURRENT STATUS OF TELECOM FRAUD TARGETING COLLEGE STUDENTS

With the widespread integration of mobile internet, big data, and artificial intelligence (AI) into campus life, students' academic pursuits, social interactions, consumption habits, and leisure activities have become fully digitized. In recent years, the proportion of telecom fraud victims aged 18–25 has risen steadily. Due to limited social experience, weak risk awareness, strong economic demands, and susceptibility to psychological manipulation, college students constitute a key demographic vulnerable to such crimes [3]. Perpetrators employ evolving tactics-including fake shopping services, online gaming virtual transactions, overseas high-salary job offers, academic credential enhancement schemes, "unsecured" low-interest loans, and AI face-swapping-leading to a year-on-year increase in victim numbers [4]. Some students suffer severe physical and psychological trauma after being defrauded, with certain cases even triggering campus crises that threaten institutional stability [5].

3. PRACTICAL DILEMMAS AND KEY SHORTCOMINGS OF TRADITIONAL ANTI-FRAUD EDUCATION

Universities nationwide prioritize anti-fraud efforts, incorporating them into campus safety management, ideological and political education, and legal education systems. Departments such as student affairs offices and security divisions organize activities including police lectures, case briefings, signed anti-fraud pledges, themed class meetings, and promotion of the National Anti-Fraud Center App. However, many students report having "heard, seen, and signed" yet remaining unable to "recognize, distinguish, or prevent" fraud in real scenarios [6]. Anti-fraud education finds itself in the awkward position of "comprehensive coverage in form but diminished efficacy in practice," manifesting five core shortcomings: excessive one-way indoctrination versus insufficient two-way interaction; rigid and monotonous formats lacking appeal; over-reliance on theoretical instruction at the expense of situational experience; frequent short-term intensive campaigns without sustained engagement; and broad educational reach coupled with inadequate precision. Collectively, these flaws result in the pervasive problem of information being "easy to see but difficult to internalize."

4. CORE ADVANTAGES AND THEORETICAL FOUNDATIONS OF APPLYING IMMERSIVE MURDER MYSTERY GAMES TO ANTI-FRAUD EDUCATION

(1) Core Advantages in Anti-Fraud Education

As a favored social activity among college students, murder mystery games inherently feature authentic scenarios, deep role immersion, high interactivity, and post-experience reflection. These attributes address the deficiencies of traditional education across experiential, emotional, and behavioral dimensions. By reconstructing the entire fraud chain-from "building rapport-setting traps-applying pressure-demanding transfers"-games allow students to viscerally experience tension, confusion, and decision-making pressure. Participants assume roles such as victims, fraudsters, police officers, or family members, facilitating perspective shifts through deep immersion to comprehend scam logic and truly grasp "tactics, harms, and boundaries." Interactive reasoning segments-such as distinguishing genuine from false information, analyzing clues, and making urgent decisions-compel students to apply anti-fraud knowledge proactively, converting theoretical understanding into practical competence. Furthermore, plots depicting post-fraud consequences-financial loss, credit damage, familial impact, and psychological distress-confront students with tangible repercussions, reinforcing psychological warnings and creating lasting cautionary memories. This "learning through play" model outperforms verbal instruction, easily diffusing across peer networks (e.g., dormitories, clubs) to foster a campus-wide anti-fraud culture with high student acceptance and dissemination potential.

(2) Theoretical Underpinnings

The application of immersive murder mystery games rests on robust theoretical frameworks: First, **Situated Learning Theory** posits that learning occurs within authentic contexts and practical participation. By recreating scam scenarios, these games facilitate "learning by doing," enhancing knowledge internalization through perceptual engagement. Second, **Experiential Education Theory** identifies "Experience–Reflection–Generalization–Application" as an effective pedagogical cycle for youth-a sequence perfectly mirrored in the structured flow of anti-fraud murder mystery games. Third, **Life-Oriented Ideological and Political Education Theory** emphasizes aligning education with daily life, reality, and youth interests. Leveraging murder mystery games as an entertaining medium for safety education achieves subtle, "moistening things silently" educational outcomes. Finally, **Behavior Change Theory** clarifies that the ultimate goal transcends performance or recreation; instead, the games aim to strengthen risk memory, catalyzing positive cognitive and behavioral shifts that improve real-world judgment and response capabilities.

5. MECHANISMS OF IMMERSIVE MURDER MYSTERY GAMES IN PREVENTING TELECOM FRAUD AMONG COLLEGE STUDENTS

(1) Cognitive Construction Mechanism: From "Awareness" to "Mastery of Tactics"

These games deconstruct prevalent campus scams-such as brush-order rebates, impersonated customer service, "pig-butchering" romance scams, fake loans, and AI fraud-into interconnected plot nodes, establishing a highly simulated "fraud scenario laboratory." Here, students transition from passive recipients to active reasoners and solvers. Tasks involving analyzing motives, identifying rhetorical inconsistencies, and tracing fund flows enable gradual reconstruction of scam chains. This "case-based reasoning" approach promotes structured, systematic cognitive development. For instance, in an "impersonated customer service" scenario, students begin with the initial hook ("parcel lost, compensation offered") and progressively uncover layered deceptions-including coerced screen sharing, phishing for verification codes, and falsified transfer screenshots. Role-playing ensures students internalize not merely the rule "refunds require official platforms" but also comprehend how scammers exploit the psychological drive for "gain and loss aversion." This establishes a "Scenario–Reasoning–Construction" pathway, transforming fragmented information into flexible, actionable knowledge frameworks and achieving a fundamental shift from merely "knowing fraud exists" to "understanding its mechanics."

(2) Emotional Awakening Mechanism: From "Indifference" to "Vigilance"

A persistent challenge is students' "It won't happen to me" mentality, rendering them psychologically immune to conventional warnings. Emotional vigilance deficits significantly contribute to flawed risk assessment. Immersive games counteract this through carefully engineered narrative tension, time constraints, moral dilemmas, and conflict scenarios that provoke deep emotional engagement. By embodying victims, bystanders, or even "accomplices," students vicariously experience the escalating pressure of scams. The visceral shock of realizing their credulity caused a "friend's" financial ruin or failing to prevent a "peer's" transfer proves far more impactful than didactic warnings. This embodied emotional experience converts abstract risks into potent affective memories-alarm, fear, anger, remorse. When encountering analogous real-world situations (e.g., unsolicited transfer requests, sudden loan appeals from friends), these ingrained "vigilance cues" activate instantaneously, triggering "déjà vu" risk alerts. This drastically reduces the latency between "information input" and "behavioral response," enabling students to "pull themselves back from the brink" during critical moments.

(3) Behavioral Training Mechanism: From “Comprehension” to “Competent Response”

Recognizing scams and feeling vigilant do not guarantee effective real-world responses. Many students, despite suspicion, falter due to panic, hesitation, or procedural uncertainty. Immersive games provide a low-risk, high-fidelity training ground through strategically placed decision points. Recurring “moments of truth”-Should I click this link? Transfer to a “safe account”? Report to police?-carry explicit consequences: incorrect choices lead to “successful scam” endings, while correct ones advance the narrative toward “scam thwarted.” Repeated cycles of “trial–error–correction–reinforcement” internalize standardized protocols-hanging up, ceasing operations, preserving evidence, dialing 96110, verifying via official channels-into near-instinctive behavioral patterns. Simulated time pressures and emotional interference further cultivate calm, methodical responses amidst chaos. Consequently, when facing actual fraud, trained students are more likely to react reflexively with appropriate actions rather than succumbing to panic-induced errors.

(4) Value Guidance Mechanism: From “Self-Protection” to “Collective Governance”

The ultimate objective extends beyond individual protection to dismantling the ecosystem enabling fraud. Alarmingly, many students lack clarity regarding the crime of “Assisting Information Network Criminal Activities” (AINCA), sometimes renting or lending bank cards/phone accounts for petty gains and inadvertently becoming accomplices [7]. Murder mystery games foreground this issue by embedding legal and ethical consequences within role-play. Assigning a student the role of someone who rents out bank accounts for profit-only to face criminal prosecution and academic ruin-delivers a far more visceral deterrent than statutory recitations. This fosters legal awareness, integrity, and accountability. Moreover, the collaborative nature of gameplay-requiring “information sharing, mutual reminders, and joint decision-making”-cultivates teamwork. Successfully thwarting a scam collectively generates a sense of efficacy that transfers to real-life contexts, building multi-layered defense networks spanning individuals, peers, classes, and the campus community. Thus, anti-fraud evolves from passive self-protection into proactive social governance. Students undergo a subtle identity shift from “anti-fraud learners” to “anti-fraud advocates and guardians,” crucial for establishing sustainable grassroots defenses and long-term governance.

6. PRACTICAL PATHWAYS FOR IMPLEMENTING IMMERSIVE ANTI-FRAUD MURDER MYSTERY GAMES IN UNIVERSITIES

(1) Collaborative Content Creation: Establishing Police–University–Community Script Development Mechanisms

High-quality scripts are foundational. Universities should establish cross-sector teams led by security and student affairs departments, collaborating with public security anti-fraud centers, procuratorates, and courts. Practitioners contribute real cases, emerging scam trends, and legal expertise, while universities handle pedagogical adaptation, narrative design, and value oversight. Scripts should adhere to principles of standardization, accessibility, and safety, focusing on prevalent campus scams to ensure authenticity, accuracy, and educational rigor. Dynamic updating mechanisms must integrate new fraudulent tactics promptly to maintain timeliness and relevance.

(2) Systemic Integration and Institutional Safeguards: Embedding within Education and Management Systems

Implementation should transcend extracurricular clubs, becoming institutionalized within the university’s educational framework. Specific measures include: integrating gameplay into mandatory freshman orientation as the “first lesson on anti-fraud”; incorporating it into regular class/league activities, legal education courses, and mental health curricula; and embedding it within “one-stop” student community initiatives as a key component of residential education. Institutionalization ensures universal student participation at least once during enrollment, preventing ad hoc or fragmented implementation.

(3) Infrastructure and Talent Development: Building Sustainable Support Systems

Infrastructure development should repurpose existing spaces-activity rooms, community lounges, library study pods, club venues-into fixed, reservable immersive experience hubs, reducing operational costs. Talent cultivation requires two core teams: (1) Faculty (counselors, class advisors) trained as game facilitators capable of organizing sessions, guiding narratives, and conducting debriefings; (2) Student leaders (class officers, psychological counselors, anti-fraud volunteers) forming a “faculty-led, student-driven” operational model. Inviting local police as guest facilitators can enhance authority and professionalism.

(4) Impact Assessment and Integrated Dissemination: Creating Closed-Loop Educational Ecosystems

A closed-loop “Assessment–Feedback–Optimization–Dissemination” mechanism prevents superficial gamification. Multi-dimensional evaluation should track: Participation Rates (attendance, sessions); Knowledge Retention (assessment scores); Behavioral Shifts (simulation accuracy); and Actual Fraud Rates (campus incident data). Integrated dissemination strategies leverage campus media-WeChat official accounts, short-video platforms, radio-to share exemplary scripts, highlights, and student reflections, amplifying reach. This cultivates a culture where “everyone participates in anti-fraud; everyone is a defender.” Online engagement should reciprocally reinforce offline activities, fostering a virtuous cycle of “Experience–Internalization–Dissemination–Re-experience” for sustained, ecological impact.

7. CONCLUSION

Anti-fraud education for college students is a long-term, systemic, and foundational endeavor vital to student welfare, campus harmony, and societal security. Introducing immersive murder mystery games represents both a breakthrough in traditional safety pedagogy and a practical manifestation of ideological and political education innovation-tailored to youth interests and needs. By relocating anti-fraud knowledge from textbooks to scenarios, shifting from didacticism to experiential learning, and transforming passivity into agency, these games empower students to recognize, prevent, and reject fraud. This provides valuable theoretical insights and practical references for constructing targeted, engaging, and effective campus anti-fraud systems. While this paper focuses on macro-mechanisms and implementation pathways, it lacks comparative data on efficacy across diverse regional universities. Future research should incorporate pilot program data to refine scripts and delivery models, promoting the normalized adoption of this innovative educational paradigm.

REFERENCES

[1] Zhao, L., & Chen, H. M. (2022). Research on influencing factors and formation mechanism of youth victimization in telecom fraud. *China Youth Social Science*, 41(3), 102–112. [In Chinese.]

[2] Xu, J. L. (2023). Research on effective domestic and international prevention strategies for college students against telecom fraud. *Legality Vision*, (3), 15–17. [In Chinese.]

[3] Zhang, X. X. (2023). Research on causes and prevention countermeasures of teenage telecom fraud in the big data era. *Industrial & Science Tribune*, 22(18), 25–27. [In Chinese.]

[4] Zhang, J. N. (2025). Current situation and risk prevention of telecommunication network fraud in higher vocational colleges. *Legality Vision*, (24), 166–168. [In Chinese.]

[5] Wang, J., Guo, C. C., & Zhang, F. (2021). Current situation and prevention countermeasures of telecom fraud cases in colleges and universities. *Journal of Lianyungang Technical College*, 34(4), 86–89. [In Chinese.]

[6] Xu, J. L. (2023). Research on effective strategies for college students to prevent telecom fraud—Taking Yunnan Normal University as an example. *Network Security Technology & Application*, (8), 84–86. [In Chinese.]

[7] *Anti-Telecom Network Fraud Law of the People's Republic of China*. (2022). People's Publishing House. [In Chinese.]