Global Science Publishing

大数据时代大学生陷入网络电信诈骗的原因与对策

何隽恺，唐佳怡，邵明浩
江苏大学京江学院，江苏镇江

摘要：在大数据时代背景下，网络电信诈骗案件频发，大学生作为特定群体，因其独特的心理特质及行为习惯，已成为诈骗犯罪分子的主要攻击目标。通过剖析大学生易受网络电信诈骗影响的成因，深入探讨了心理、技术和社会层面的因素，并据此提出了针对性的防范策略。研究结果表明，大学生网络安全意识的缺失、对网络信息的过度信任以及个人信息保护意识的不足是其受骗的主要因素。针对上述问题，建议从强化网络安全教育、完善相关法律法规、增强技术防护能力等维度出发，制定相应对策，以期提升大学生的防范意识，有效降低网络电信诈骗事件的发生率。

关键词：大数据时代；大学生；网络电信诈骗

Reasons and Countermeasures for College Students Falling Prey to Online and Telecommunication Fraud in the Big Data Era

Junkai He, Jiayi Tang, Minghao Shao
Jingjiang College, Jiangsu University, Zhenjiang, Jiangsu

Abstract: Against the backdrop of the big data era, online and telecommunication fraud cases occur frequently. College students, as a specific group, have become the main targets of fraudsters due to their unique psychological traits and behavioral habits. By analyzing the causes of college students' vulnerability to online and telecommunication fraud, this paper delves into the psychological, technical, and social factors and proposes targeted prevention strategies accordingly. The research results show that the lack of cybersecurity awareness, excessive trust in online information, and insufficient awareness of personal information protection are the main reasons for college students being deceived. To address these issues, it is suggested that corresponding countermeasures be formulated from the dimensions of strengthening cybersecurity education, improving relevant laws and regulations, and enhancing technical protection capabilities, with the aim of enhancing college students' prevention awareness and effectively reducing the incidence of online and telecommunication fraud.

Keywords: Big Data Era; College Students; Online and Telecommunication Fraud

1 大数据时代网络电信诈骗的特征与趋势

1.1 核心特征

以数据驱动的精准诈骗画像为核心，诈骗者通过非法手段获取网购记录、社交数据、定位信息等，构建详尽的受害者画像，实现定制化诈骗。例如一名高校学生因频繁搜索“兼职信息”，接收到伪装成“知名企业线上实习”诈骗邮件，导致个人信息泄露。诈骗者利用朋友圈动态定向推送“教育退费”“快递理赔”等诈骗链接。同时，AI技术的滥用在合成熟人语音、视频进行诈骗。2023年，浙江某高校发生诈骗者“AI换脸冒充辅导员”案件，涉案金额超过10万元。

1.2 发展趋势

在技术对抗方面，诈骗者使用“对抗生成网络”绕过人脸识别系统，而防御方则研发了深度伪造检测工具，元宇宙空间渗透、数字资产交易、虚拟身份认证成为新目标。2023年，某元宇宙平台发生“虚拟土地诈骗案”，200多名大学生损失超过300万元。

1.3 数据佐证

根据公安部数据，2020-2023年大学生受骗案件年均增长率为23.7%，远高于其他群体(全体人群增长率为15.2%)，2023年校园诈骗涉案总金额达到47.8亿元，人均损失从2019年的6320元上升至13500元。根据2024年中国信息通信研究院研究显示，78%的诈骗案件涉及大数据分析工具，43%使用AI技术。

大数据时代，网络电信诈骗已从“随机偶发”转变为“技术驱动、精准打击”的系统性风险，其特征表现为数据化、智能化、链条化，发展趋势指向技术对抗升级、场景全域渗透、犯罪隐蔽性增强。防范此类诈骗需构建“数据治理-技术防御-法律惩戒”全链条防护体系，特别需关注元宇宙、量子计算等前沿领域可能催生新型犯罪形态[1]。

2 大学生陷入网络电信诈骗的成因分析

2.1 主体因素

教育部《2023年大学生数字素养调查报告》显示，仅36%的学生能准确识别钓鱼网站特征，58%的学生对“HTTPS加密协议”防护意义缺乏认知。某高校学生因轻信“免费WiFi”连接，导致社交账号被盗，诈骗分子借此向好友群发“紧急借款”信息，造成连环诈骗。大学生隐私保护意识薄弱，调查显示83%的大学生在社交平台公开真实姓名、学号、定位信息，65%的学生使用“弱密码”[2]。

2.2 高频网络行为增加暴露风险

大学生日均使用移动支付6.8次，参与网络游戏、直播打赏、二手交易等场景占比达79%。虚拟货币交易、NFT数字藏品投资等新兴领域成为诈骗新温床。在大数据与AI技术的双刃剑效应下，数据滥用导致了精准诈骗，如通过爬虫技术非法获取学生网购记录、学生社交关系等信息，形成精准“诈骗剧本”。

2.3 环境因素，防护体系的漏洞与滞后

高校教育体系中，网络安全课程缺失，反诈教育多停留在“横幅标语”宣传，缺乏情景模拟训练，管理存在盲区。校园WiFi、工作系统存在安全漏洞，大多数院校系统未启用双因素认证，学生心理辅导体系未涵盖反诈心理建设，受骗后极少数学生会主动寻求帮助。

大学生受骗的本质是“技术漏洞，心理弱点，环境缺陷”三维风险叠加，技术维度是大数据与AI技术被犯罪工具化，突破传统防御边界，教育、法律、平台治理多重滞后提供犯罪温床。破解这一困局需构建涵盖“认知重塑（教育），技术对抗(防御)，制度补位(治理)”的协同防护体系。

3 多维协同防范体系的构建路径

3.1 教育赋能：构建“认知-技能-实践”一体化培养体系

将网络安全与反诈教育纳入通识教育必修课程，实现从入学到毕业全周期覆盖。课程内容涵盖网络诈骗类型识别、个人信息保护、法律维权途径等关键模块。教学模式可采用“MOOC+情景模拟”相结合的方式，通过案例分析提高学生的参与度[3]。南京某高校实施试点后，学生反诈知识测试

的平均分数从62分提升至85分，诈骗案件发生率下降了38%。

3.2 朋辈教育机制

组建反诈志愿者团队，选拔并培训学生骨干，开展“案例复盘”、“反诈剧本杀”等特色活动。通过模拟诈骗场景，提升学生应对能力。同时，通过线上社群运营，建立反诈知识分享群，定期推送最新诈骗案例与防范技巧。

3.3 制度保障：完善法律与服务体系

通过立法强化与执法优化，推动《反电信网络诈骗法》实施，明确平台数据保护责任。建立跨境反诈协作机制，打击境外诈骗服务器与资金洗白网络。设立校园反诈心理咨询站，对受骗学生进行创伤后应激干预；提供免费法律咨询与诉讼支持，降低学生维权成本。开通反诈举报热线与线上平台，鼓励公众提供诈骗线索。

4 实证分析与成效验证

4.1 实证分析

广西师范大学钟晓媚与秦素琼副教授在研究中指出，大学生网络社会支持以及心理资本水平较高，而网络人际信任以及网络利他行为水平偏低，有待提高。正是由于一系列网络心理原因诱发大学生被网络信息吸引，导致网络诈骗频发。

信阳学院冯慧、李静和李海丽通过研究得出，高校学生防范诈骗意识薄弱的原因基本包括社会(网络)环境、高校教育工作及学生自身意识等三个方面[4]。中国刑事警察学院匡荟霖研究得出，由于互联网普及、社会节奏加快，很多青年婚恋交友由线下转变为线上，以网络婚恋交友的诈骗手段日渐丰富，严重影响了和谐社会建设和公共安全，尤其是受骗人经济和感情的双重损失，降低了幸福感，这也成为了社会治理重要问题之一。

云南师范大学桑锦霞和雷希研究得出，电信网络诈骗是互联网商家无视公民个人信息隐私权，伦理正当性及挑战社会安全性所造成的结果。贵州师范大学的张素娟、潘弘、唐林研究得出，判断取款行为成立诈骗罪还是掩饰、隐瞒犯罪所得罪，需要从主观和客观两个方面进行综合判断。

4.2 成效验证

针对上述问题，我国信息通信行业积极开展了行业源头治理工作。工业和信息化部作为国务院打击治理电信网络诈骗新型违法犯罪工作部际联席会议工作单位和行业主管部门，全面贯彻党中央、国务院有关决策部署，在工信部网安局指导下，信息通信行业相关企业单位深入落实主体责任，纵深推进防范治理工作，形成了全链条多层次的治理格局。

针对当前诈骗治理重点难点，工信部网安局多次组织指导相关专题会议，部署督导人工智能诈骗治理相关工作，确保治理工作有效推进。同时，为保障促进人工智能在安全领域应用，工信部发布《促进新一代人工智能产业发展三年行动计划》，构建完善以法律法规、监管政策、技术标准、监督执法为核心的人工智能安全监管体系。

5 未来展望与持续改进

5.1 应对新型诈骗形态

针对校园网络安全基础设施的升级，建议构建元宇宙空间行为监测系统，并开发相应的虚拟身份认证工具。同时，推动建立国际反诈数据交换机制，实现诈骗黑名单与犯罪线索的共享[5]。建议与国际网络安全机构进行合作，共同研发AI反诈工具和深度伪造检测技术。此外，应制定校园数据采集与使用准则，以明确反诈监测的合法界限。利用机器学习技术分析诈骗趋势，动态调整防范策略。建立高校、企业与政府的联动机制。高校负责反诈教育、提供心理支持及执行数据监测任务，企业提供技术工具与数据支持，政府则需完善相关法律法规，并协调跨境执法协作。

5.2 构建可持续反诈生态

大学生网络诈骗未来防范策略应着重于“技术前沿布局”、“国际合作深化”以及“伦理边界界定”三大关键领域。通过实施“数据驱动优化”、“多主体协同”以及“长效评估反馈”持续改进机制，构建可持续发展的反诈生态系统。该系统核心目标在于实现反诈工具智能化与前瞻性，形成多

方协同的高效治理模式，在确保安全的同时充分尊重学生隐私与权益。

通过持续创新与优化，旨在实现“零诈骗校园”的长远愿景，为数字时代人才培养提供坚实的安全保障，为大学生打造健康绿色的网络环境平台，尽可能减少网络诈骗事件对校园安全稳定和良好秩序的负面影响，致力于使网络诈骗现象在校园内无迹可寻。

参考文献

[1] 冯慧, 李静, 李海丽. 新形势下大学生防范网络电信诈骗有效路径研究[J]. 中国新通信, 2023, 25(07): 122-124+133.

[2] 郝思舜. 电信诈骗议题报道中“受骗者”的媒介形象建构研究——以中国大陆地区综合性报章为例(2016-2022)[D]. 上海: 华东师范大学, 2023. 6.

[3] 张素娟, 潘弘, 唐林. W市电信网络诈骗协同治理的困境和对策研究[D]. 咸阳: 西北农林科技大学, 2023. 6.

[4] 李娜. 网络环境下大学生防范电信诈骗安全意识现状及管理研究[J]. 法制博览, 2023(07): 25-27.

[5] 匡荟霖. 网络婚恋交友类型诈骗侦查对策研究[J]. 网络安全技术与应用, 2024(02): 157-159.