

大数据背景下大学生电信网络诈骗风险 评估与干预体系研究

李荣霞

重庆工商大学, 重庆 400067

摘要: 本研究聚焦大数据背景下大学生电信网络诈骗风险, 通过对多维数据特征的分析, 构建了“经济拮据—寻求兼职型”“社交孤独—渴望情感型”“消费冲动—热衷网购型”三类典型高风险学生画像。在此基础上, 设计了分级干预体系, 针对低、中、高风险群体分别实施普遍性预防、针对性预警与精准性阻断措施。同时, 本文构建了包含“风险识别、干预过程、结果产出”三个维度的评估指标体系, 以客观衡量干预体系的实施效果。

关键词: 大数据; 大学生电信网络诈骗; 风险评估; 分级干预; 效果评估

0 引言

近年来, 我国数字化进程持续加速, 移动互联网、第三方支付等技术的普及极大地便利了社会生产生活, 但也为电信网络诈骗提供了滋生的土壤。大学生群体因金融知识储备薄弱、社会经验不足、风险防范意识欠缺, 成为诈骗分子重点攻击的目标。资料显示 2024 年, 全国高校范围内报告的大学生电信网络诈骗案件就达 1.2 万起, 平均每起案件造成学生财产损失超 8000 元, 部分案件甚至引发学生心理危机、家庭经济困境等连锁问题, 严重影响“平安校园”建设。

当前针对大学生的反诈工作仍以普适性宣传教育为主, 多采用讲座、海报、宣传单等传统形式, 缺乏基于数据驱动的前瞻性风险评估和个性化干预手段, 导致反诈工作精准度不足、预警时效性差, 难以有效遏制诈骗案件的发生。在大数据背景下构建大学生电信网络诈骗风险评估模型, 设计精准干预策略, 成为当前亟待解决的关键问题。

1 核心概念

1.1 电信网络诈骗

电信网络诈骗是指犯罪分子利用电话、短信、互联网等通信技术手段, 编造虚假信息, 设置骗局, 对受害人实施远程、非接触式诈骗, 骗取受害人财物的违法犯罪行为。其主要类型包括刷单返利诈骗、冒充客服诈骗、虚假交易诈骗、“杀猪盘”诈骗、校园贷诈骗等。其中, 刷单返利诈骗以“低投入、高回报”为诱饵, 吸引大学生参与虚假刷单任务, 后期以“任务未完成”“账户冻结”等理由拒绝提现; “杀猪盘”诈骗则通过社交平台伪装成“高富帅”“白富美”, 与大学生建立情感关系后, 诱导其参与虚假投资、赌博等活动, 最终骗取钱财。

1.2 风险评估

本研究中的风险评估是基于多维度数据,

对大学生个体或群体遭受电信网络诈骗的可能性进行量化和等级划分的过程。其目的是识别高风险学生群体, 明确不同学生的风险等级, 为后续干预策略的制定提供数据支持。与传统风险评估相比, 基于大数据的风险评估具有覆盖范围广、评估精度高、动态性强等优势, 能够实时跟踪学生风险变化, 提升评估的时效性。

1.3 干预策略

干预策略是指基于风险评估结果, 为降低大学生电信网络诈骗风险而采取的预防性、警示性和阻断性的措施。根据学生风险等级的不同, 干预策略可分为普遍性预防、针对性预警和精准性阻断三类, 旨在通过差异化措施, 实现对不同风险群体的有效干预, 降低诈骗案件发生率和财产损失。

2 大学生电信网络诈骗风险的多维数据特征分析

2.1 风险数据源的构成与整合

2.1.1 线上行为数据

线上行为数据是评估大学生电信网络诈骗风险的核心数据来源, 主要包括 App 使用时长、网络浏览记录、社交媒体活跃度、搜索关键词等。其中, App 使用时长可反映学生对不同应用的依赖程度, 如频繁使用兼职类、社交类 App 的学生, 面临刷单返利、“杀猪盘”诈骗的风险较高; 网络浏览记录中, 若学生经常访问不明兼职网站、虚假投资平台等, 可能存在潜在诈骗风险; 社交媒体活跃度和搜索关键词则能体现学生的需求和关注点, 如频繁搜索“兼职赚钱”“快速致富”等关键词的学生, 更容易成为诈骗分子的目标。

2.1.2 个人属性与消费数据

个人属性数据包括学生的年级、专业、性别等基本信息, 消费数据则涵盖月消费水平、消费结构(如网络游戏充值、直播打赏支出占比)等。从个人属性来看, 低年级学生因刚进入校园, 社会经验不足, 风险防范意识较弱, 更容

易遭受诈骗;从消费结构来看,月消费水平较低、经常进行网络游戏充值或直播打赏的学生,可能因经济压力或消费习惯,面临更高的诈骗风险,如容易被“低价充值”“打赏返利”等骗局吸引。

2.1.3 心理与认知数据

心理与认知数据通过量表测量获取,主要包括风险偏好、从众心理、财务状况认知、防骗知识水平等。风险偏好较高的学生,更愿意尝试“高风险、高回报”的项目,容易陷入虚假投资诈骗;从众心理强的学生,可能因盲目跟随他人参与刷单、投资等活动,遭受集体诈骗;财务状况认知不足、防骗知识水平低的学生,对诈骗手段的识别能力较弱,难以察觉骗局的破绽。

2.1.4 校园环境数据

校园环境数据包括所在学校及周边区域的诈骗案发率、接受的防骗宣传教育频率与形式等。学校及周边区域诈骗案发率高的学生,面临的外部诈骗威胁更大;接受防骗宣传教育频率低、形式单一的学生,防骗知识储备不足,风险防范意识较弱,更容易遭受诈骗。

2.2 基于大数据的风险特征提取与量化

2.2.1 行为特征

行为特征是反映大学生电信网络诈骗风险的重要指标,主要包括夜间活跃度、非常规金融操作频率、访问风险网站的频次等。夜间活跃度高的学生,可能因夜间判断力下降,更容易被诈骗分子诱导;非常规金融操作频率,如频繁进行跨地域转账、向陌生账户大额汇款等,可能是遭受诈骗的信号;访问风险网站的频次越高,学生接触诈骗信息的机会越多,遭受诈骗的风险越大。通过对这些行为特征进行量化,如将夜间活跃度划分为高、中、低三个等级,非常规金融操作频率按次数统计,可构建行为风险指标体系。

2.2.2 社交特征

社交特征包括社交网络广度、与已知风险账号的关联度等。社交网络广度窄的学生,可能因社交孤独,更容易被诈骗分子通过社交平台建立情感关系,进而遭受“杀猪盘”诈骗;与已知风险账号(如被标记为诈骗账号的微信、QQ账号)关联度高的学生,可能已陷入诈骗陷阱或面临较高的诈骗风险。通过计算学生社交网络中好友数量、与风险账号的互动频率等,可量化社交特征风险。

2.2.3 心理特征

心理特征通过冲动性得分、轻信度得分等指标进行量化。冲动性得分高的学生,在面对“高回报”“限时优惠”等诱惑时,容易做出非理性决策,进而遭受诈骗;轻信度得分高的学生,对他人提供的信息缺乏辨别能力,更容易相信诈骗分子编造的虚假信息。通过心理量表对学生进行测试,可获取冲动性得分和轻信度得分,

为风险评估提供心理层面的数据支持。

2.2.4 环境特征

环境特征主要通过所处环境的诈骗威胁指数来量化。诈骗威胁指数综合考虑学校及周边区域的诈骗案发率、涉诈人员密度、诈骗手段更新速度等因素,指数越高,学生面临的诈骗风险越大。通过收集公安部门、高校保卫处的诈骗案件数据,可计算出不同学校及周边区域的诈骗威胁指数,为环境特征风险评估提供依据。

2.3 高风险学生群体的初步画像

综合上述多维数据特征,可初步勾勒出三类典型的高风险学生画像:

2.3.1 “经济拮据—寻求兼职型”

此类学生多为低年级学生,月消费水平较低,经济压力较大,频繁搜索“兼职赚钱”“快速赚钱”等关键词,经常使用兼职类App,访问不明兼职网站的频次较高。他们风险偏好较高,防骗知识水平低,容易被“刷单返利”“足不出户赚钱”等骗局吸引,遭受刷单返利诈骗的风险极大。

2.3.2 “社交孤独—渴望情感型”

这类学生社交网络广度窄,社交媒体活跃度低,从众心理强,内心渴望情感关怀。他们经常使用社交类App,容易被伪装成“理想伴侣”的诈骗分子吸引,与陌生账号互动频繁,部分学生甚至与已知风险账号存在关联。此类学生轻信度得分高,对情感关系的需求远高于对风险的警惕,是“杀猪盘”诈骗的主要目标群体。

2.3.3 “消费冲动—热衷网购型”

该类学生消费冲动性得分高,经常进行网购、网络游戏充值和直播打赏,月消费支出中娱乐消费占比高。他们对“低价商品”“充值返利”“打赏抽奖”等活动兴趣浓厚,容易被冒充客服的诈骗分子以“订单异常”“商品质量问题”“退款赔偿”等理由诱导,遭受冒充客服诈骗或虚假交易诈骗的风险较高。

3 基于风险等级的分级干预策略

针对低风险群体,以“提升整体防骗意识”为核心,开展普遍性预防措施,具体包括三类举措。一是常态化防骗宣传教育:高校每月通过校园公众号、班级群推送反诈知识,内容结合近期高发诈骗案例(如新型“AI换脸”冒充亲友诈骗、“游戏账号交易”诈骗),采用短视频、漫画、情景剧等学生喜闻乐见的形式,避免传统文字宣传的枯燥性;每学期组织1-2次反诈主题讲座,邀请公安反诈民警、受害学生(匿名)分享案例,增强宣传感染力。二是防骗知识测试与积分激励:开发线上防骗知识测试平台,学生每月完成1次轻量化测试,激发学生主动学习防骗知识的积极性。三是环境风险管控:高校联合通信运营商,对校园网内的恶意网址、涉诈APP进行自动拦截;在校园

周边商铺、快递点张贴反诈海报,联合商户开展“反诈宣传志愿者”活动,营造“校园内外联动反诈”的环境氛围。

中风险群体多存在“某类风险特征突出但未达高风险阈值”的情况(如频繁使用社交类APP但未与风险账号关联、消费冲动性较高但无异常消费记录),需开展针对性预警干预,核心是“及时提醒+行为引导”。一是个性化预警通知:通过校园APP推送个性化预警消息,内容结合学生具体风险特征,如对“消费冲动-热衷网购型”学生,推送“冒充客服退款诈骗”的案例与识别要点;避免泛化预警导致学生忽视。二是辅导员一对一谈话:由辅导员对中风险学生开展1次一对一谈话,通过“倾听需求+风险提示”的方式,了解学生近期生活(如是否有兼职需求、情感困扰),针对性解答防骗疑问,同时记录谈话内容并录入风险评估系统,作为后续干预效果跟踪的依据。三是风险行为引导:对存在“频繁搜索兼职关键词”的中风险学生,高校就业指导中心推送正规兼职渠道(如校园勤工助学岗位、合作企业实习岗位),替代不明兼职平台;对“消费冲动性高”的学生,联合金融机构提供“理性消费咨询服务”,帮助学生制定消费计划,减少因“追求低价”陷入诈骗的可能。

高风险群体是诈骗案件的“高危人群”,需采取“实时监测+主动阻断+多方协同”的精准性阻断措施,确保“零案发”。一是实时行为监测与预警:依托大数据平台,对高风险学生的线上行为进行实时监测,当出现“访问涉诈网址”“与诈骗号码通话超过5分钟”“向

陌生账户转账超过5000元”等高危行为时,系统立即触发预警,同步推送消息至辅导员、高校保卫处与公安反诈中心,预警响应时间控制在10分钟内。二是多主体协同阻断:若监测到高风险学生正在进行诈骗交易,辅导员立即联系学生核实情况,公安反诈民警可介入,通过“案例讲解+法律警示”的方式,帮助学生认清骗局本质,避免财产损失。三是心理疏导与长期跟踪:部分高风险学生(如“社交孤独-渴望情感型”)可能因情感需求或经济压力陷入心理困境,高校心理咨询中心定期开展心理疏导服务,缓解焦虑、孤独等情绪;辅导员每月对高风险学生进行1次跟踪回访,持续监测风险变化,直至风险等级降至中低水平。

4 结论

本研究围绕大数据背景下大学生电信网络诈骗风险展开,明确了风险评估与干预的关键路径。研究发现,大学生诈骗风险源于线上行为、个人属性、心理认知、校园环境,并构建“经济拮据-寻求兼职型”“社交孤独-渴望情感型”“消费冲动-热衷网购型”三类高风险学生画像。基于此设计的分级干预体系,针对低、中、高风险群体分别实施普遍性预防、针对性预警与精准性阻断,结合多维度效果评估指标,可有效提升反诈精准度与时效性。然而,研究数据样本覆盖范围有限,未来可扩大样本类型,进一步优化干预策略的实操性,为“平安校园”建设与大学生财产安全保障提供更全面的理论与实践支撑。

参考文献:

- [1] 江波.新形势下高校反电信网络诈骗犯罪体系的构建:以四川S大学为例[J].四川警察学院学报,2022,34(4):74-80.
- [2] 周鑫怡.三全育人视域下大学生防范电信网络诈骗机制研究[J].高校后勤研究,2025,(9):30-35.
- [3] 单秉治,乔顺利.网络刷单诈骗犯罪电子取证的困境与出路[J].广西警察学院报,2023,36(05):100-114.
- [4] 姜督.电信网络诈骗犯罪精准治理研究[J].山东警察学院学报,2022,34(06):21-28.
- [5] 郭小伟.高校电信网络诈骗调查分析及防范体系构建[J].质量与市场,2020(24):127-129.
- [6] 张武清,汪双成,吕晓琴.高职院校新型电信网络诈骗防控机制研究[J].法制博览,2024(21):13-15.
- [7] 刘丽,刘仙蕊.基于大数据分析的电信网络诈骗预警系统研究[J].数字通信世界,2024(11):101-103.

作者简介:李荣霞(1984.06—),女,汉,重庆市璧山区,讲师,博士研究生,研究方向:教育学、思想政治教育。

项目信息:2025年重庆市教育委员会人文社会科学研究基地项目《新时代高校辅导员与思政课教师协同育人模式研究》(项目编号25SKJD129)。

重庆市教育科学规划课题2022年度一般课题《大数据背景下大学生电信网络诈骗风险评估与干预研究》(课题编号K22YG208165)。