

AI人工智能背景下大学生陷入网络诈骗频发的原因与对策研究

谈静怡 许程杰 左增强

江苏大学京江学院, 中国·江苏 镇江 212114

【摘要】本研究聚焦于AI人工智能时代大学生频繁遭遇网络诈骗的现象,深入剖析其背后的多方面原因,涵盖大学生自身特质、AI技术的不当利用、高校教育与管理短板以及社会环境的复杂因素等。并基于这些原因探讨相应的解决对策,旨在构建一个多层次、全方位的防范体系,以有效遏制网络诈骗在大学生群体中的蔓延,保障大学生的财产安全与身心健康,维护高校及社会的和谐稳定。

【关键词】大学生; AI人工智能诈骗; 原因与对策

引言

AI人工智能技术的迅猛发展深刻改变了社会的诸多方面,在带来便捷与创新的同时,也为网络诈骗活动提供了更为隐蔽和高效的手段。网络诈骗案件在大学生群体中的频发,不仅给学生个人及其家庭带来了经济上的巨大损失和精神上的沉重负担,也对高校的正常教学秩序、声誉形象以及社会的稳定有序构成了严峻挑战。因此,深入探究大学生陷入网络诈骗的根源,并寻求切实可行的应对策略,已成为当下亟待解决的重要课题。

1 大学生陷入网络诈骗频发的原因

1.1 大学生自身因素

1.1.1 社会经验匮乏与认知局限

大学生大多处于从校园到社会的过渡阶段,生活环境相对单纯,对社会的复杂性和阴暗面缺乏足够的认知与体验。在面对网络诈骗分子精心设计的复杂骗局时,往往难以迅速辨别真伪,容易被表面现象所迷惑,从而陷入诈骗陷阱。例如,在一些虚假兼职诈骗中,诈骗者以高额报酬为诱饵,大学生因不了解市场行情和正规兼职流程,轻易相信并缴纳各种所谓的“手续费”“押金”等。

1.1.2 心理弱点易被利用

①贪图小利心理。部分大学生存在不劳而获或轻松获利的侥幸心理,容易被网络诈骗分子抛出的“小恩小惠”所吸引。如一些“点赞返现”“抽奖赢大礼”等诈骗形式,看似简单易行且回报丰厚,使不少大学生在利益诱惑面前丧失警惕;②盲目信任权威与从众心理。大学生往往对一些所谓的“官方机构”“知名企业”或“专家学者”具有较高的信任度。诈骗分子便利用这一心理,伪装成相关权威身份,如假冒银行客服告知学生账户存在安全问题,需要进行资金转移操作;或者借助从众心理,声称某投资项目已有众多同龄人参与且获利颇丰,诱导学生跟风参与;③碍于情面与不好意思拒绝。在一些涉及人际关系的

诈骗情境中,如诈骗分子冒充同学、朋友借钱或请求帮忙购买物品,大学生由于碍于情面,未进行充分核实便轻易答应,导致被骗。

1.2 AI技术助力诈骗手段升级

1.2.1 智能语音与视频诈骗

AI语音合成技术能够逼真地模仿他人声音,诈骗分子可借此拨打诈骗电话,冒充学生的亲属、朋友或老师等,编造紧急情况,如“生病住院急需钱”等理由,骗取学生的信任并诱导其转账汇款。AI视频换脸技术则进一步增强了诈骗的欺骗性,通过制作虚假的视频通话,让学生亲眼看到“熟人”的面容,从而降低心理防线。例如,曾有诈骗分子利用AI换脸技术伪装成学生的海外亲戚,以遭遇意外事故需要资金救助为由实施诈骗。

1.2.2 精准信息推送与诈骗场景定制

借助大数据分析和AI算法,诈骗分子能够收集并分析大学生在网络上留下的海量信息,包括个人基本信息、消费习惯、兴趣爱好、社交关系等。基于这些精准的用户画像,诈骗分子可以针对性地制定个性化的诈骗方案,推送高度契合学生需求和心理预期的诈骗信息,使诈骗更具迷惑性和成功率。比如,针对有网购习惯的大学生,推送虚假的电商退款链接,利用其对购物流程的熟悉感和对退款的期待心理进行诈骗;对于有升学或考证需求的学生,则发送虚假的培训课程优惠信息或考试包过骗局等。

1.3 高校教育与管理体的不足

高校的安全教育课程在内容更新速度上难以跟上网络诈骗手段的快速迭代。许多高校的安全教育教材和课程内容仍然停留在对传统诈骗形式的介绍,对基于AI技术的新型诈骗手段涉及较少,导致学生在面对实际发生的新型网络诈骗时缺乏有效的应对知识和技能。例如,对于AI换脸诈骗、智能语音诈骗等新型诈骗方式,学生可能在遭受诈骗后才首次知晓其存在。

2 应对大学生网络诈骗频发的对策

2.1 强化大学生自身防范意识与能力

2.1.1 开展系统的网络诈骗防范教育课程

高校应将网络诈骗防范教育纳入大学生综合素质培养体系, 开设专门的必修或选修课程。课程内容应涵盖网络诈骗的历史演变、常见类型、典型案例分析、基于AI技术的新型诈骗手段解析以及防范技巧与应对策略等方面。通过系统的课程学习, 使学生全面了解网络诈骗的全貌, 掌握识别和防范诈骗的基本方法和技能。例如, 在课程教学中, 可以组织学生观看真实的诈骗案例视频, 进行案例讨论和分析, 让学生在实践中提高对诈骗的敏感度和辨别能力。

2.1.2 培养健康的网络行为习惯和心理素养

引导大学生树立正确的网络价值观和消费观, 培养健康的网络行为习惯。教育学生在网络环境中保持谨慎和理性, 不随意透露个人敏感信息, 不轻易点击来路不明的链接, 不盲目参与网络上的各种“诱惑性”活动。同时, 注重培养学生的心理素质, 增强其心理抗压能力和挫折应对能力, 避免因心理弱点被诈骗分子利用。例如, 开展心理健康教育讲座和心理咨询服务, 帮助学生认识自己的心理特点和潜在的心理风险, 引导他们学会自我调节和情绪管理, 在面对诈骗诱惑时能够保持冷静和理智。

2.2 提升对AI诈骗技术的应对与反制能力

2.2.1 加强技术研发与应用

政府、高校和企业应加大对网络安全技术和反诈骗技术的研发投入, 联合建立专门的研究机构或实验室, 集中力量攻克基于AI技术的网络诈骗防范难题。例如, 研发基于人工智能的诈骗信息智能识别系统, 该系统能够实时监测和分析网络信息流量, 自动识别和拦截可疑的诈骗电话、短信、邮件和网络链接等。

2.2.2 提高公众对AI诈骗技术的认知与识别能力

通过多种渠道广泛开展科普宣传活动, 向大学生及社会公众普及AI技术的基本原理、应用场景以及在网络诈骗中的常见手段和防范方法。例如, 制作生动有趣的科普短视频、动画、漫画等, 在社交媒体平台、网络视频平台、校园媒体等渠道进行传播, 以通俗易懂的方式向大众介绍AI语音合成、视频换脸等技术的特点和识别技巧。举办AI技术与网络安全知识讲座、研讨会和培训活动, 邀请专家学者、网络安全技术人员为大学生进行专业讲解和技术演示, 提高他们对AI诈骗技术的认知水平和识别能力。

2.3 完善高校网络诈骗防范教育与管理体制

2.3.1 优化网络诈骗防范教育内容与方式

高校应及时更新网络诈骗防范教育教材和课程内容, 将最新的网络诈骗案例、诈骗手段和防范技术纳入教学体系。同时, 创新教育方式方法, 采用多样化的教学手段, 如案例教学法、情境模拟法、角色扮演法、互动游戏法

等, 增强教育的趣味性和实效性。例如, 组织学生开展网络诈骗情境模拟演练活动, 让学生分别扮演诈骗分子、受害者、警方等角色, 通过模拟真实的诈骗场景, 使学生在实践中亲身体验诈骗的过程和应对方法, 提高他们的实际应对能力和团队协作能力。

2.3.2 加强校园网络安全管理与监控

高校应建立健全校园网络安全管理制度, 加大对校园网络基础设施的投入和建设, 完善网络安全防护体系, 如安装防火墙、入侵检测系统、防病毒软件等网络安全设备, 定期对校园网络进行安全检查和漏洞修复, 防止诈骗分子利用网络漏洞入侵校园网络系统。加强对校园网络平台的监管, 建立网络信息审核机制, 对在校园网络内发布的信息进行严格审核, 及时发现和删除可疑的诈骗信息, 净化校园网络环境。例如, 安排专人负责校园社交网络平台、论坛、贴吧等进行日常巡查, 对发现的诈骗信息及时进行处理, 并向学生发布预警提示。

3 结论

AI人工智能背景下大学生陷入网络诈骗频发是一个复杂的社会问题, 涉及大学生自身、高校、社会等多个层面的因素。解决这一问题需要各方共同努力, 形成合力。大学生要不断提高自身的防范意识和能力, 自觉抵制网络诈骗的诱惑; 高校要加强网络诈骗防范教育与管理, 为学生营造安全的校园网络环境; 社会各界要加强网络空间监管与执法力度, 完善社会信用体系建设, 从源头上遏制网络诈骗的发生。只有通过构建全方位、多层次的网络诈骗防范体系, 才能有效地保护大学生的财产安全和身心健康, 维护高校及社会的和谐稳定。

参考文献:

- [1] 许倩. 强教育与弱感知: 高校安全教育中正式和非正式制度对大学生风险感知的影响——基于电信诈骗的多案例研究[J]. 广东大学学报, 2022 (2): 33.
- [2] 白莉莉, 刘军怀. 大数据时代电信网络诈骗的防范与治理[J]. 楚天法治, 2023 (20): 40-42.
- [3] 陈继人. 电信网络诈骗的法律分析及预防对策[J]. 社会科学, 2023 (2): 170-172.
- [4] 李亚可. 我国电信网络诈骗犯罪的态势特征及打击思路探析[J]. 浙江警察学院学报, 2022 (2): 34-40.
- [5] 吴俊, 邵敏兰, 吴宇珂. 互联网时代高校大学生防范网络电信诈骗安全教育研究[J]. 法制博览, 2022 (28): 24-26.
- [6] 程子良, 翁添富. 大学生防范电信网络诈骗现状调查与对策研究——基于746名高校大学生的实证分析[J]. 高校后勤研究, 2022 (05): 58-62.

作者简介:

谈静怡, 女, 江苏扬州人, 江苏大学京江学院本科生在读。