

人工智能背景下大学生网络诈骗风险防范现状及应对路径研究

王支萍

山东外国语职业技术大学, 山东 日照 276826

摘要: 人工智能技术深度应用给经济社会带来了巨大的便利, 但是也使网络诈骗手段呈现出智能化、精准化、隐蔽化的趋势, 大学生由于网络使用频率高、社会经验缺乏而成为易受侵害的人群。文章从人工智能背景出发, 对大学生网络诈骗风险防范的现状进行系统的梳理, 分析防范工作存在的教育内容滞后、技术预警不足、协同机制不健全、心理干预缺失等问题, 从技术赋能、教育引导、制度保障、心理支持四个方面提出相应的解决办法, 并通过具体的实践案例来说明策略的实施途径和效果, 为高校提高大学生网络诈骗风险防范能力提供系统的参考。

关键词: 人工智能; 大学生; 网络诈骗; 风险防范; 应对路径

0 引言

人工智能技术飞速发展, 给人们的生活方式和生产方式带来了巨大的改变, 智能语音、图像生成、大数据分析等技术被广泛使用之后, 也成了网络诈骗新的手段。近几年来, 深度伪造换脸、AI 语音克隆、精准画像施骗、智能群呼等新型诈骗手段不断出现, 网络诈骗的总体形态由原来的广撒网式转向精准化、定制化、智能化, 其迷惑性及危害性明显增大。大学生群体在日常生活中活跃于社交、购物、求职、学习等各种网络场景之中, 网络使用频率高、触网时间长, 再加上部分学生社会经验缺乏、风险意识薄弱, 因此在网络诈骗面前具有较高的暴露度和受害率。切实加强大学生网络诈骗风险防范, 已经成为高校安全管理、立德树人工作面临的重要课题。因此有必要对人工智能背景下大学生网络诈骗风险防范现状进行系统的分析, 并寻找出行之有效的应对途径。

1 人工智能背景下大学生网络诈骗风险防范的现状

1.1 网络诈骗手段呈现智能化升级

人工智能技术在网络诈骗中被滥用之后, 诈骗手段也发生了深刻的改变。身份伪装上, 诈骗者用深度伪造技术合成出与被害人亲属、老师或者公职人员声音、影像一致的视频, 使得受害者对视频的真实性产生怀疑, 即使视频中存在语音通话, 也很难辨别真假。诈骗者依靠大数据分析来对非法获取的社交记录、消费习惯、学业信息、位置轨迹等展开用户画像工作, 进而给不同的群体提供个性化的诈骗话术, 这样便使得诈骗内容具备更强的针对性与迷惑性, 大学生所接收到的诈骗信息常常精确地包含姓名、学校乃至课程信息。智能群呼、智能建号、自动换绑、AI 客服等自动化工具的使用使得诈骗者可以在很短

的时间内对大量的目标进行批量攻击, 传统的手工拨号已经被智能系统所代替。技术手段的加入使得传统的防范原则的效用大大降低, 大学生仅仅依靠日常的经验已经不能识破经过智能化包装的诈骗圈套, 防范难度也越来越大。除此之外, 智能化诈骗已经形成了一条分工明确的产业链条, 上游提供技术支持、数据支持, 中游做话术设计、精准投放, 下游完成资金转移、洗白工作, 各个阶段互相配合, 隐蔽性强, 加大了监管打击的难度。

1.2 大学生群体面临的风险态势严峻

大学生所处的网络环境是复杂的、多样的, 存在诸多潜在的风险, 涉及校园生活的各个方面, 风险分布具有多样性、分散性。学生在校期间经常使用在线选课、校园缴费、社团报名、宿舍门禁等平台, 个人信息在各个环节中流动, 存在泄露风险; 课余时间, 一些学生喜欢参与网络兼职、游戏交易、二手物品买卖、社交软件交友等活动, 这些活动常常是刷单返利、虚假交易、冒充客服、杀猪盘等诈骗行为的集中地; 学业和生活压力之下, 一些学生急于实现经济独立, 很容易被所谓的高薪兼职、零门槛创业、校园贷注销等虚假信息所迷惑。同时大学生的信息辨别能力、风险抵御能力还不成熟, 对于精心设计好的诈骗话术很容易产生误判, 再加上 AI 技术使得诈骗信息在语言表达、声音图像等各方面更加真实, 大学生受到网络诈骗的风险也在不断上升。据有关统计显示, 大学生群体在所有网络诈骗受害者中所占的比例越来越高, 已经成为了犯罪链条中的重要目标, 防范工作迫在眉睫。一旦被骗, 学生不仅会遭受经济损失的打击, 还会遭受学业、社交、心理等各方面的连锁影响, 有些家庭还会背上沉重的债务, 危害不可小视。

1.3 高校防范工作已初步开展但仍有不足

目前大多数高校把防范网络诈骗纳入到学生安全教育工作中来,以主题班会、专题讲座、宣传推送、反诈海报等形式进行防骗宣传,部分高校还联合公安机关建立了反诈宣传阵地,在一定程度上取得了一定的成效。但是就总体来看,高校防范工作仍偏重于案件发生后的宣传提醒,缺少系统的、常态的防控机制。防范教育内容大多只针对常见的电信诈骗类型,对于AI换脸、语音克隆、智能钓鱼等新型诈骗手法的介绍缺乏深入分析,教育形式主要是单向灌输,缺乏学生的参与感与获得感。校园层面的技术防控手段比较少,没有对异常通话、可疑链接、涉诈应用的智能化监测能力,单靠单一事故通报式的教育方式已经不能满足现实需要了,必须从教育内容、形式、频次等各方面进行系统优化。

2 大学生网络诈骗风险防范存在的问题

2.1 防范教育内容与形式相对滞后

高校目前的防骗教育内容大多局限于传统的诈骗类型,对于人工智能背景下出现的新诈骗手段缺少系统的解释,学生无法掌握深度伪造技术的基本原理以及识别方法,在面对AI合成的诈骗内容的时候辨别能力欠缺。讲座、班会等集中宣讲方式的信息保留率低,不能引起学生的主动关注,容易出现教师讲得投入、学生听得随意的现象,教育效果难以保证。教育内容更新的速度远远落后于诈骗手段的更新速度,当学生真的遇到新的诈骗时,他们所具备的防范知识早已过时,教育供给同风险需求之间存在着明显的差距,使得防范教育无法起到应有的警示作用,学生的安全教育信任度、关注度也随之降低,陷入恶性循环之中。

2.2 技术预警与监测能力相对薄弱

高校对于技术手段防范网络诈骗存在明显缺陷。一方面,大部分高校没有专业的信息安全团队,校园网络安全防护依靠基础防火墙和人工巡检,不能对海量网络数据中的涉诈信息进行智能识别和实时预警,对于隐藏在正常通信中的诈骗行为缺少有效的甄别手段,监测范围小、数据少,无法支撑精准研判。另一方面高校与公安机关反诈平台对接不力,涉诈信息实时共享受阻,学生手机端收到的诈骗电话、钓鱼链接等风险行为不能及时被监测到并加以干预。技术防控的缺乏使防范工作只能停留在事后处理上,不能在诈骗发生之前形成有效的拦截,造成很多学生因为没有及时收到风险提示而受到损失。

2.3 多方协同治理机制不够健全

网络诈骗防范牵涉到高校、公安机关、电信运营商、网络平台等众多主体,但是目前各方之间的协同联动还不到位。高

校和公安机关之间信息共享主要依靠定期通报,缺少了实时互通的处置渠道,学生在遭遇诈骗之后的报案止付、资金冻结、线索追踪等环节之间衔接不畅,造成止损的最佳时机错过。网络平台对于校园周边异常账号以及可疑链接的监测整治工作存在着较大的差异,电信运营商对于境外异常来电和短信的拦截能力较弱,各个主体之间的职责界限不清、信息孤岛现象依然存在,不能构建起从事前预防、事中拦截到事后处置的完整治理闭环,防范工作系统性、整体性有待提高,各主体之间合力不足导致防范效果大打折扣,难以形成齐抓共管的治理格局。

2.4 受害学生心理干预存在缺位

大学生遭受网络诈骗之后,除了会遇到直接的经济损失之外,还会承受很大心理压力以及负面情绪。有些学生因为害怕受到责备或者嘲笑而产生自责、羞愧、恐惧等情绪,有的还会出现焦虑、抑郁、社交回避等心理问题,严重地影响了正常的学习与生活。但是大多数高校还没有建立专门的心理支持、危机干预机制来应对诈骗受害者,辅导员在处理案件时更注重报案、追回损失,对学生心理状况的关心不够,缺少专业的心理疏导资源及时介入,学生遭受打击后心理康复缺乏有效的保障,个别极端情况下还会出现次生的安全风险,心理层面的缺失使防范工作缺少了一块。

3 人工智能背景下大学生网络诈骗风险防范的应对路径

3.1 技术赋能:构建智能化预警与反制系统

高校应充分发挥人工智能技术的优势来提高自身的反诈能力,创建起校警合作的智能化预警机制。某高校同市反诈中心一起部署了校园反诈智能预警平台,该平台依靠AI算法对校园网络里的异常通信行为展开实时监测,可以自动识别境内外的异常来电、仿冒网站链接以及涉诈的应用程序,并按照风险等级给学生发出分级预警信息,而且会把信息通报给辅导员去核实。平台上线一学期,共识别出并拦截了四百多次涉诈风险行为,成功劝阻了数十名正在遭受刷单诈骗、冒充客服诈骗的学生转账汇款,挽回了学生损失八十余万元,诈骗案件发生率明显降低。智能预警系统把反诈防线前移到诈骗发生之前,大大提高了防范工作的及时性、准确性,是技术赋能高校反诈工作的一种有效做法。

3.2 教育引导:构建立体化数字素养培育体系

防范网络诈骗的根本是提高大学生的数字素养和风险意识。高校要将网络安全教育融入到人才培养体系当中,创建起覆盖全员、贯穿全程的教育机制。以高校新生入学教育为例,在其

开设的数字安全必修课里,以 AI 诈骗识别、个人信息保护、网络行为规范等为主要模块开展教学,采取真实案例剖析和情景模拟演练并行的方式组织实施教学活动,特别设置了使用 AI 换脸视频实施诈骗时辨别真假的训练部分,让学生对真假素材加以对比之后清楚地体会到深度伪造技术的特性,进而学到辨别真假的技术手段。学校成立校园反诈宣讲团,以经过系统培训的学生骨干为成员,在宿舍、班级开展同伴教育,及时传播最新诈骗手法和防范知识。经过一个学期的实践,该校涉诈类事件报案数量比上个学期下降了约四成,学生主动参加反诈知识学习的积极性明显提高,校园防骗氛围明显改善,学生之间互相提醒、互相沟通的意识增强,教育引导的实效得到充分显现,实现了从被动防骗到主动识骗的转变。

3.3 制度保障:完善多方协同治理机制

网络诈骗防范要靠多方主体共同参与,高校应该牵头创建常态化的协同治理机制。一方面,加强警校合作,创建涉诈事件快速响应通道,确定学生遇到诈骗时第一时间向辅导员汇报、辅导员配合报案、公安机关紧急止付的标准化处置流程,最大程度上缩短反应时间,提高挽损率。另一方面,推动高校同网络平台、电信运营商合作,对校园周边区域内的可疑账号、虚假链接、涉诈电话进行重点监控并及时封堵。以某地公安机关和多所高校为依托,每周给高校推送最新的诈骗手法和预警信息,高校根据高校的动态更新防范教育内容,同时为高校开通紧急止付绿色通道,学生发现被骗后可以立即启动止付程序,使处置时间最短。该联盟成立以来,辖区高校涉诈案件挽损率明显提高,跨部门协同处置的堵点得以疏通,多方协同的治理效能逐渐显现,高校在防范工作中的统筹协调能力得到明显加

强,为长效治理打下了制度基础,也为其他高校提供了一个可以借鉴的协同范式。

3.4 心理支持:健全受害学生关怀与康复机制

高校在做好事中拦截、事后处置的同时,也要重视受害学生心理康复。学校可以依托心理健康教育中心创建专项援助机制,对遭遇诈骗的学生立刻展开心理评价与疏导工作,从而让其正确面对损失,摆脱自责情绪,重新获得心理安全感。辅导员马上报警、止付,心理咨询师对学生进行一对一心理辅导,用理性分析的方式使学生认识到自己的错误,并从中吸取教训,学校给予学生助学金、临时困难补助等帮助。在之后的跟踪中,学校把它当作一个重点对象,一直留意学生的心态变化,直到它恢复到正常的学生活动当中为止,从而构建起一条完整的关怀链条。完善的关怀机制既体现出学校的人文温度,又避免了受害学生因为心理创伤而产生次生问题,给防范工作补上了重要的闭环环节,使整个防范体系在关注财产损失的同时兼顾了人的主体地位,体现了以人为本的育人理念。

4 结语

人工智能背景之下网络诈骗手段的智能化升级,给大学生群体的风险防范能力带来巨大的考验。高校要立足现实、正视问题,从技术赋能、教育引导、制度保障、心理支持四个方面入手,建立预防、预警、处置、善后相衔接的全过程防范体系,提高学生防范新型网络诈骗的能力。只有不断加强防范工作的智能化、协同化水平,切实提高大学生的数字素养和风险意识,在人工智能的时代为学生筑牢安全屏障,保护好青年学子的财产安全和身心健康。

参考文献:

- [1]陈军弟.人工智能背景下高校电信网络诈骗防范教育探析[J].广西教育,2026,(9):110-113.
- [2]张雪霞,李娟,崔冬雪.网络时代高校思政教育教学创新实践探索[M].北京:中国纺织出版社有限公司,2023.
- [3]刘一舟.大学生电信网络诈骗的被害成因与防控对策研究[D].南京信息工程大学,2025.

基金项目: 本文用于 2026 年度山东省哲学社会科学创新发展研究会科研课题《人工智能时代大学生网络诈骗风险防范的现状与路径探究》(Z-SKY26030)研究使用。