

探析大学生网络诈骗易感性的心理因素及干预启示

曹 晓

(浙江工业大学, 浙江 杭州 310014)

摘 要: 在网络深度融入学习生活的背景下, 大学生网络诈骗易感性问题已成为影响校园安全稳定与学生身心健康发展的重要议题, 开展相关研究具有重要的现实意义与实践价值。深入剖析大学生网络诈骗易感性的心理因素, 能够为构建科学有效的反诈干预体系提供核心依据, 助力提升大学生网络安全素养。基于此, 文章以大学生网络诈骗易感性为研究核心, 梳理了网络诈骗在大学生群体中的特征, 明确了网络诈骗易感性的定义与表现, 系统探究了影响大学生网络诈骗易感性的核心心理因素, 提出了针对性的干预策略与启示, 最终总结了研究价值与实践意义, 旨在为高校及相关机构开展反诈工作提供理论支撑与实践指引。

关键词: 大学生; 网络诈骗; 心理因素

中图分类号: G444

文献标识码: A

文章编号: 3006-001X (2025) 05-0001-10

DOI: 10.62022/FETR.issn3006-001X.2025.05.001

Exploring the Psychological Factors and Intervention Implications of College Students' Susceptibility to Online Fraud

Xiao Cao

(Zhejiang University of Technology, Hangzhou, Zhejiang 310014)

Abstract: In the context of the deep integration of the internet into learning and life, the issue of college students' susceptibility to online fraud has become an important topic affecting campus safety and stability as well as students' physical and mental health development. Conducting relevant research holds significant practical and practical value. An in-depth analysis of the psychological factors contributing to college students' susceptibility to online fraud can provide core evidence for building a scientific and effective anti-fraud intervention system, thereby enhancing college students' cybersecurity literacy. Based on this, the article focuses on the susceptibility of college students to online fraud, outlines the characteristics of online fraud among college students, clarifies the definition and manifestations of susceptibility to online fraud, systematically explores the core psychological factors affecting college students' susceptibility to online fraud, proposes targeted intervention strategies and insights, and ultimately summarizes the research value and practical significance. The aim is to provide theoretical support and practical guidance for universities and related institutions in their anti-fraud efforts.

Keywords: college students; online fraud; psychological factors

随着数字技术的快速发展, 网络已全面融入大学生的学习、生活与社交等各个领域, 为大学生获取信息、开展交流、拓宽视野提供了便捷渠道。但与此同时, 网络空间的开放性与虚拟性也使得网络诈骗行为愈发频繁, 大学生群体因自身成长阶段的特殊性, 逐渐成为网络诈骗的高发受害群体。大学生网络诈骗易感性不仅会导致学生个人财产遭受损失, 还可能对其心理状态与学业发展产生不良影响, 进而影响校园的和谐稳定。因此, 精准把握大学生网络诈骗易感性的核心心理因素, 构建契合大学生群体特点的干预体系, 已成为当前校园安全建设与大学生成长成才保障工作中的重要任务。

一、网络诈骗在大学生群体中的特征

(一) 诈骗手段的多样化与隐蔽性

当前, 面向大学生群体的网络诈骗手段呈现出显著的多样化特征, 诈骗分子凭借对大学生群体生活轨迹、心理需求的精准洞察, 能够精准捕捉其在学习、生活、社交、求职、升学等不同场景下的核心需求, 进而设计出针对性极强的诈骗形式, 实现“场景化精准施诈”。从常见类型来看, 已形成覆盖大学生日常核心需求的完整诈骗链条, 涵盖了刷单兼职诈骗、网络购物诈骗、冒充客服诈骗、游戏交易诈骗、盗用社交账号诈骗、求职招聘诈骗、培训辅导诈骗、冒充公检法诈骗、校园贷诈骗等多种形式。更为

作者简介: 曹晓, 博士, 副教授, 研究方向为大学生心理健康教育与网络行为引导。

突出的是,随着网络技术的迭代更新,诈骗手段正朝着“复合型”“智能化”方向不断翻新演化,不再局限于单一诈骗模式,而是通过多场景融合、多手段叠加提升诈骗成功率。例如,部分诈骗分子借助短视频平台、直播带货等新兴传播渠道,发布制作精良的虚假营销视频或直播内容,以“低价好物”“限时福利”“专属补贴”等噱头吸引大学生关注,诱导其通过私下链接交易;还有的诈骗分子创新推出“刷单+N”的复合型诈骗模式,在传统刷单兼职的基础上,衍生出“刷单+色情诱导”“刷单+网络赌博”“刷单+虚假投资”等新型骗术,通过前期小额返利建立信任,再逐步引导大学生陷入更深层次的诈骗陷阱,进一步扩大了诈骗的覆盖范围与危害程度。此外,针对大学生学业需求的诈骗手段也不断升级,出现了“论文发表代投诈骗”“考研复试保过诈骗”“资格证书代办诈骗”等细分类型,精准锁定有特定学业规划的大学生群体。

与多样化相伴而生的是诈骗手段的隐蔽性,这一特征通过技术赋能与流程设计的双重加持,显著增加了大学生识别诈骗的难度,使其更易陷入骗局。在技术层面,诈骗分子广泛运用大数据、人工智能、语音合成、图像伪造等前沿技术手段,通过非法爬虫、信息倒卖等渠道收集、分析大学生的个人信息,包括精准到具体专业的背景信息、消费能力与偏好的消费习惯、社交关系网络、学业规划与求职意向等核心数据,从而实现“千人千面”的精准施诈。在场景营造层面,诈骗分子会通过精细化的伪装手段,营造出真实可信的场景氛围,大幅降低大学生的警惕性,例如伪造与官方网站高度一致的虚假页面,不仅界面设计、色彩搭配完全复刻,还会模仿官方域名设置相似后缀,仅通过细微字符差异混淆视听;模仿正规客服的语气语调与沟通话术,甚至能准确报出大学生的订单编号、商品信息、收货地址等细节;通过技术手段克隆社交账号的头像、昵称、个性签名,甚至盗用历史聊天记录,实现“以假乱真”的身份伪装。具体来看,在冒充客服诈骗中,诈骗分子能够精准说出大学生的近期订单信息,以“订单异常卡顿”

“商品质量抽检不合格”“需办理退款补贴”等为由,引导大学生点击带有木马病毒的钓鱼链接,或要求其提供银行卡号、手机验证码等敏感信息,进而实施资金盗取;在冒充熟人诈骗中,诈骗分子通过克隆辅导员、同学、家人的社交账号,以“缴纳学杂费”“突发紧急情况借钱”等紧急事由,利用大学生的信任与同情心实施诈骗,由于账号信息与沟通语境高度真实,大学生往往难以在短时间内分辨对方身份的真伪。此外,部分诈骗分子还充分利用网

络的虚拟性与匿名性,采用分阶段、多环节的渐进式诈骗流程,将诈骗过程拆解为“建立信任—小额获利—诱导加码—套取信息—卷款跑路”等多个步骤,逐步降低大学生的心理防线,诱导其逐步陷入骗局,使得诈骗行为在实施过程中更具隐蔽性,难以被及时察觉。

(二) 大学生受骗的典型场景与损失程度

大学生受骗的典型场景与自身的学习生活需求高度相关,且受年级阶段、专业属性、生活习惯等因素影响,不同年级、不同专业的大学生在受骗场景上呈现出明显的差异性,形成了“阶段化高发”的特征。新生入学阶段是受骗的高发时期,大一新生由于刚脱离高中封闭的学习环境,进入陌生的校园环境后,对校园管理流程、周边商业环境与网络社交规则均不熟悉,同时缺乏独立处理事务的经验,极易成为诈骗分子的重点目标。这一阶段的诈骗分子多冒充学长学姐、校园工作人员、宿管人员等身份,利用新生的信任心理实施诈骗,常见的诈骗场景包括新生报到材料代办、校园卡激活代办、宿舍用品高价推销、军训服装代购、校园社团虚假缴费等。例如,部分诈骗分子在新生报到点附近徘徊,主动向新生提供“全程代办报到手续”服务,以“手续费”“资料费”等名义收取费用后失联;还有的以“学长学姐福利”为由,向新生推销质量低劣的被褥、生活用品,价格远超市场正常水平。在日常学习生活中,网络购物与兼职打工是大学生受骗的两大核心场景,随着“宅经济”“副业热”在大学生群体中的兴起,这两类场景的诈骗发生率持续攀升。很多大学生会通过电商平台、社交软件寻找高性价比商品,诈骗分子则利用其追求实惠的心理,以“尾货清仓”“海关扣押品低价出售”“内部员工折扣”等为由,诱导其脱离正规平台进行私下交易;而在兼职打工场景中,诈骗分子精准把握大学生渴望经济独立、减轻家庭负担的心理,以“低门槛、高佣金、日结”“无需技能经验”等极具诱惑力的条件为诱饵,推出大量虚假兼职信息,除了传统的刷单兼职外,还衍生出“数据标注兼职诈骗”“线上客服兼职诈骗”“短视频剪辑兼职诈骗”等新型形式。

在学业发展与职业规划的关键阶段,求职招聘、培训辅导、考研升学相关的诈骗场景呈现出高度集中的特征,成为高年级大学生受骗的主要风险点。大四学生及研究生面临毕业求职的巨大压力,急于获取优质就业机会,诈骗分子则利用这一心理,通过招聘网站、校园招聘群、社交平台等渠道发布虚假招聘信息,其诈骗手段呈现出“专业化”“高端化”的特点。例如,以“大型企业内推名额”

“国企央企直签岗位”“高薪管培生岗位”等为噱头,向大学生收取高额的“内推费”“报名费”“简历筛选费”,在收取费用后以“岗位已满”“考核未通过”等理由推脱,或直接失联;还有的诈骗分子伪装成正规企业HR,通过面试后以“入职前需参加专业培训”为由,诱导大学生报名高价培训课程,甚至推荐“培训贷”,导致大学生既未获得工作,还背负高额债务。在培训辅导场景中,针对大学生提升学业成绩、增强升学竞争力的需求,诈骗分子开设虚假的考研辅导机构、公考培训机构、语言培训机构等,通过虚假宣传“名师授课”“高通过率”“不过全退”等承诺吸引报名,收取高额培训费用后,要么提供质量极差的培训服务,要么直接卷款跑路。例如,部分虚假考研培训机构会伪造师资队伍信息,盗用正规机构的学员上岸案例,通过“一对一精准辅导”“复试保录”等噱头收取数万元培训费,在考研结束后便销声匿迹。此外,游戏交易场景也是大学生受骗的重要领域,尤其对于热衷网络游戏的大学生群体,诈骗分子围绕游戏账号、装备、皮肤等虚拟资产交易设计多种骗局。具体包括以“高价收购游戏账号”为由,诱导大学生在非正规交易平台操作,通过虚假转账截图骗取账号;以“赠送稀有游戏皮肤”“游戏装备低价出售”为诱饵,引导大学生点击钓鱼链接或向陌生账号转账;还有的通过游戏内聊天伪装“队友”,以“合买装备”“代练升级”等名义实施诈骗,这类诈骗由于贴近大学生的娱乐需求,隐蔽性较强,受骗概率较高。

从大学生受骗的损失程度来看,呈现出“以财产损失为核心、多元间接损失并存”的特征,其中财产损失金额存在明显的个体差异,总体呈现出从几百元到数万元不等的阶梯式分布态势,且损失金额与诈骗类型、大学生自身经济状况、防范意识紧密相关。从具体金额分布来看,大部分大学生的受骗损失金额集中在1000元~5000元之间,这一金额区间主要对应刷单兼职诈骗、网络购物诈骗、小额游戏道具诈骗等常见基础类型。此类诈骗中,诈骗分子通常采用“小额多次”的诱导策略,先以极低门槛让大学生投入少量资金并快速返利,逐步打破其心理防线,再引导其分阶段追加投入,最终累计造成千元级别的财产损失,这一金额既不会让大学生在初期产生过度警惕,又能为诈骗分子带来稳定收益。损失金额在5000元~20000元之间的中高额损失,则主要集中在游戏账号交易诈骗、求职内推诈骗、培训辅导诈骗等场景。例如,高端游戏账号交易中,账号估值往往较高,诈骗分子以“高价收购”或“低价出售”为由实施诈骗,单次诈骗金额可达数万元;部分

考研培训、公考培训的虚假机构,收取的培训费在1万元~2万元,一旦诈骗成功,会给大学生带来较大的经济压力。少数情况下,损失金额甚至超过20000元,这类情况多发生在虚假投资诈骗、校园贷关联诈骗等场景中,诈骗分子通过营造“快速暴富”的虚假预期,诱导大学生投入大额资金,甚至劝说其通过校园贷、网络贷款平台借款投资,最终导致大学生背负巨额债务。除了直接的财产损失外,大学生受骗后还会面临多维度的间接损失,且这类损失往往难以量化评估,但其危害程度不亚于财产损失。在心理层面,多数受骗大学生会产生强烈的焦虑、自责、自卑情绪,部分学生还会出现失眠、抑郁、社交恐惧等心理问题,严重影响其学习状态与日常生活;在社交层面,部分大学生因受骗而对他人产生信任危机,难以融入集体生活,甚至影响与家人、同学的关系;在学业与职业发展层面,若在求职、考研关键阶段受骗,不仅会造成经济损失,还可能耽误求职进度、影响升学备考状态,对长远发展产生不利影响。总体而言,大学生受骗后的损失程度是诈骗分子手段强度、大学生自身防范能力、经济承受能力、情绪调节能力等多因素共同作用的结果,不同场景、不同类型诈骗对应的损失金额与损失类型存在显著差异。

二、网络诈骗易感性的定义与表现

(一) 易感性的心理学内涵

从心理学视角来看,网络诈骗易感性是指个体在网络环境中,由于自身心理特质、认知水平、情绪状态等多种因素的综合作用,对网络诈骗信息产生的一种易感倾向,以及在面对网络诈骗诱惑或压力时,难以做出理性判断和正确应对,从而容易陷入诈骗陷阱的心理属性。这一概念强调个体内部心理因素与外部网络诈骗环境之间的相互作用,易感性的高低直接决定了个体在面对网络诈骗时的风险程度。

网络诈骗易感性的心理学内涵主要体现在三个核心维度。其一,认知维度的易感倾向,即个体对网络诈骗的认知存在偏差或不足,对网络诈骗的手段、特征、风险缺乏清晰的认识和准确的判断,从而难以有效识别诈骗信息。其二,情绪维度的易感倾向,即个体的情绪状态容易受到网络诈骗信息的影响,在贪婪、恐惧、焦虑等情绪的驱动下,难以保持理性,进而做出非理性的决策。其三,人格与需求维度的易感倾向,即个体的人格特质与心理需求与网络诈骗场景存在契合性,例如好奇心强、追求新鲜刺激、社交需求强烈等特质,容易被诈骗分子利用,从而增加陷

入骗局的风险。从本质上来说,网络诈骗易感性是个体心理系统在应对网络诈骗风险时的一种脆弱性表现,这种脆弱性并非一成不变,而是可以通过后天的教育、训练等方式进行干预和改善。

(二) 大学生易感性的特殊性与阶段性特征

大学生群体的网络诈骗易感性具有显著的特殊性,这种特殊性源于大学生所处的成长阶段与群体特征。一方面,大学生作为网络原生代群体,对网络的依赖程度较高,日常学习生活与网络的结合极为紧密,这使得他们接触网络诈骗信息的概率远高于其他群体,同时也为诈骗分子实施精准施诈提供了更多的信息渠道。另一方面,大学生长期处于相对单纯的校园环境中,社会阅历相对匮乏,对社会复杂现象的认知有待提高,对人性的多样性缺乏全面的了解,因此在面对网络诈骗中的虚假信息和诱惑时,警惕性相对较低,容易产生信任心理。此外,大学生的经济尚未完全独立,大部分经济来源依赖家庭支持,在追求经济独立、改善生活条件的心理驱动下,容易被“高收益”“轻松赚钱”等诈骗噱头吸引,进一步提升了易感性。

除了特殊性之外,大学生网络诈骗易感性还呈现出明显的阶段性特征,这种阶段性与大学生的年级变化、学业发展轨迹密切相关。大一新生阶段,易感性主要体现在对校园环境和网络环境的不适应上,新生由于刚脱离高中的封闭环境,对大学的学习生活模式和网络社交规则尚不熟悉,容易被冒充校园工作人员、学长学姐的诈骗分子欺骗,同时对网络兼职、网络购物等场景中的诈骗风险缺乏认知。大二、大三阶段,大学生逐渐适应了校园生活,学习压力相对稳定,社交范围不断扩大,对网络的利用更加多元化,易感性主要集中在网络购物、游戏交易、社交交友等场景,诈骗分子往往利用这一阶段大学生追求新鲜刺激、社交需求强烈的心理实施诈骗。大四及研究生阶段,易感性则主要与求职就业、考研升学、毕业论文指导等场景相关,由于面临毕业压力,大学生对求职信息、培训辅导信息的需求迫切,容易被虚假招聘、高价培训等诈骗信息迷惑,同时在急于完成毕业论文的心理驱动下,也可能被论文代写、数据造假等诈骗陷阱吸引。不同阶段的易感性特征,决定了针对大学生的反诈干预工作需要具有针对性,结合不同年级的特点开展精准干预。

三、影响大学生网络诈骗易感性的核心心理因素

(一) 认知偏差与风险感知能力有待提高

认知层面的偏差显现与风险感知能力有待提升,是影

响大学生网络诈骗易感性的核心心理因素之一。这一情况使得大学生在识别网络诈骗信息时精准度不足,在规避诈骗风险过程中应对有效性有待加强。大学生群体虽具备基础的知识储备与学习潜能,但在网络诈骗相关的认知领域仍存在明显不足,对网络环境的多元复杂性和诈骗风险的潜在危害性认知不够全面系统,风险感知的敏锐度有待提升,进而在一定程度上增加了陷入诈骗陷阱的可能性。

对网络环境的信任边界模糊与侥幸心理显现,是认知偏差的重要表现形式。大学生长期在网络环境中开展学习生活,充分享受网络带来的便捷与高效,逐步形成了对网络环境的信任心理,而这种信任心理在部分情况下会延伸至网络中的陌生对象与信息,导致其对网络虚假信息的警惕性有待提高。同时,不少大学生存在一定的侥幸心理,认为网络诈骗发生概率较低,自身遭遇此类事件的可能性较小,即便接触到身边同学或网络上的诈骗案例,也多将其归因于他人的疏忽大意或应对不当,未能充分重视自身可能面临的同类风险。例如,部分大学生在公共场合随意连接未加密的免费Wi-Fi,对由此可能引发的个人信息泄露风险认知不足;面对“中奖通知”“低价购物”等明显带有风险提示的信息时,也会因侥幸心理尝试点击链接,最终可能陷入诈骗陷阱。

诈骗信息识别能力的不足,是认知偏差与风险感知能力有待提升的另一重要表现。大学生对网络诈骗相关知识的掌握多呈碎片化状态,缺乏系统的学习积累与深入的认知理解,对常见诈骗手段的运作逻辑、套路特征及基础识别方法的掌握不够全面。多数大学生仅能识别部分简单的诈骗信息,对于诈骗分子借助大数据、人工智能等技术伪装的复杂诈骗信息,识别难度较大。例如,诈骗分子伪造的官方网站在界面设计、域名后缀等细节上与正规网站高度相似,由于大学生缺乏对应的专业识别知识,容易出现误判;对于诈骗分子通过社交平台发送的钓鱼链接,大学生也难以凭借链接特征准确判断其安全性。此外,部分大学生存在一定的知识错觉与过度自信倾向,认为自身熟悉网络操作流程、具备基础常识,能够准确辨别各类诈骗套路,这种认知倾向在一定程度上降低了其警惕性,使其在面对精心设计的诈骗陷阱时,容易放松戒备,进而做出不够理性的判断。

(二) 情绪驱动下的非理性决策

情绪状态对决策过程的影响较为显著,大学生在接触网络诈骗信息时,易受多种情绪因素作用,出现决策不够理性的情况,这也是导致其网络诈骗易感性有所提升的重

要原因。大学生正处于情绪发展的关键阶段，情绪体验丰富且反应较为强烈，情绪调节的灵活性与有效性有待提升，在贪婪、恐惧、焦虑等情绪的影响下，容易忽视客观存在的风险，优先关注情绪层面的需求满足，进而可能陷入诈骗分子设计的圈套。

贪婪、恐惧等情绪对判断过程的干扰较为直接。在贪婪情绪的影响下，大学生容易被“高收益”“低风险”“快速获利”等诈骗噱头吸引，对背后潜藏的风险缺乏足够认知。例如，在刷单兼职诈骗中，诈骗分子常以“低门槛、高佣金”为诱饵，大学生在第一单获得少量返利后，易受贪婪情绪驱动，后续投入更多资金，最终可能产生财产损失；在虚假投资诈骗中，诈骗分子通过展示虚假盈利数据，强化大学生的获利期待，进而诱导其投入大量资金，最终导致资金损失。而在恐惧、焦虑情绪的作用下，大学生的理性判断能力易受影响，可能出现盲目听从诈骗分子指令的情况。例如，在冒充公检法诈骗中，诈骗分子通过言语恐吓、风险夸大等方式，引发大学生的恐惧情绪，使其误以为自身涉嫌违法犯罪，进而按照诈骗分子的要求进行转账汇款；在冒充客服诈骗中，诈骗分子以“订单异常”“商品质量问题”“需承担赔偿责任”等为由，制造焦虑氛围，诱导大学生进行转账操作。

群体压力与从众心理的诱导，也可能导致大学生出现决策不够理性的情况，进而提升网络诈骗易感性。大学生具有较强的群体归属感，重视身边同伴的评价与行为态度，在群体压力的作用下，容易弱化自身判断，跟随群体行为倾向。诈骗分子精准把握这一心理特点，通过营造“多人参与”“获益”的虚假场景，施加群体影响，诱导大学生从众参与。例如，在刷单兼职诈骗中，诈骗分子会向大学生展示其他“刷单人员”的虚假盈利截图、聊天记录等，构建“多数人通过刷单获利”的虚假氛围，大学生在从众心理驱动下，可能认为这是可靠的获利方式，进而参与其中；在虚假购物群、投资群中，诈骗分子会安排人员发布虚假购物体验、投资收益信息，引导群内大学生跟随购买或投资，不少大学生在群体氛围的影响下，对风险的关注度降低，进而做出不够理性的决策。

（三）社会经验匮乏与心理成熟度滞后

社会经验积累不足与心理成熟度有待提升，是大学生群体的显著特征，这一特征使得大学生在面对网络诈骗时，有效的应对能力与科学的判断依据较为缺乏，进而在一定程度上提升了网络诈骗易感性。大学生长期在相对单纯的校园环境中成长，接触的社会环境类型较为单一，对社会

中的复杂现象与多元场景了解较少，缺乏与不同类型人群的交往经验，同时心理发展尚未完全成熟，独立思考的深度与解决问题的能力有待提升，这些因素共同作用，导致其在面对网络诈骗时，难以做出精准有效的应对。

独立生活能力有待加强与信息甄别经验不足，是社会经验积累不足的具体体现。不少大学生在进入大学前，生活上多依赖家庭照顾，独立处理日常事务的经验较为匮乏，进入大学后，在面对网络购物、兼职打工、社交交友等需要自主决策的场景时，判断的准确性与合理性有待提升。同时，大学生缺乏信息甄别的实践经验，面对网络中的海量信息，难以高效区分真实信息与虚假信息、有用信息与有害信息。在接触网络诈骗信息时，他们往往难以凭借自身经验验证信息的真实性与可靠性，容易被诈骗分子的话术引导与虚假承诺迷惑。例如，在求职兼职场景中，由于缺乏求职经验，大学生对招聘信息的真伪辨别能力不足，容易被虚假招聘信息误导；在网络交友场景中，因缺乏人际交往经验，难以准确判断对方身份的真实性，容易陷入社交诈骗相关的风险场景。

自我保护意识有待强化与依赖心理显现，是心理成熟度有待提升的重要体现。大学生对自我保护的重视程度不足，在个人信息保护、财产安全保障等方面的意识较为薄弱，在网络中容易随意泄露个人身份证号、银行卡号、联系方式、家庭住址等敏感信息，为诈骗分子实施精准诈骗提供了可乘之机。例如，部分大学生在网络社交平台上完全开放个人动态与资料信息，使得诈骗分子能够轻松获取其生活轨迹、兴趣爱好、人际关系等信息，进而针对性地设计诈骗套路。同时，不少大学生存在一定的依赖心理，在遇到问题时，更倾向于向他人求助，独立思考与解决问题的主动性有待提升。在面对网络诈骗中的疑问或压力时，他们缺乏通过正规渠道核实信息的意识与能力，反而容易依赖诈骗分子提供的“解决方案”，或在他人的诱导下做出不够理性的决策。例如，在接到冒充客服的诈骗电话时，大学生不懂得通过官方平台联系客服核实信息真伪，而是按照诈骗分子提供的电话或链接进行操作，最终可能导致财产损失。

（四）人格特质与心理需求的关联性

大学生的人格特质与心理需求存在显著的个体差异，部分人格特质与心理需求容易与网络诈骗场景形成契合，从而增加了网络诈骗易感性。人格特质是个体稳定的心理特征，直接影响个体的行为倾向和决策方式；心理需求是个体内在的心理诉求，驱动个体做出相应的行为选择。诈

骗分子往往会精准捕捉大学生的这些人格特质与心理需求,设计针对性的诈骗套路,诱导大学生陷入骗局。

好奇心强与追求新鲜刺激的倾向是部分大学生的典型人格特质,这种特质容易被诈骗分子利用,进而提升网络诈骗易感性。大学生处于身心发展的关键阶段,对新鲜事物充满好奇,喜欢尝试新的体验和挑战,这种心理在网络环境中表现得尤为明显。诈骗分子利用大学生的好奇心,设计出新颖、奇特的诈骗形式,吸引大学生的关注和参与。例如,部分诈骗分子通过短视频平台发布“神秘福利”“特殊体验”等相关的营销视频,以新奇的内容吸引大学生点击链接;还有的诈骗分子推出“新型游戏装备”“独家会员服务”等虚假信息,利用大学生追求新鲜刺激的心理,诱导他们进行转账购买。此外,对于一些未知的网络链接、陌生的社交请求,好奇心强的大学生往往更容易点击或通过,从而为诈骗分子实施诈骗提供了可乘之机。

孤独感与社交需求对诈骗的迎合是另一重要关联因素。大学生远离家乡和亲人,进入陌生的校园环境,容易产生孤独感,对社交存在强烈的需求,渴望通过网络拓展社交圈子,结交朋友。诈骗分子精准利用了大学生的这一心理需求,通过网络社交平台伪装身份,与大学生建立情感联系,逐步获取信任,进而实施诈骗。例如,在诈骗中,诈骗分子通常会伪装成温柔体贴的异性、志同道合的朋友等,与大学生进行深入的情感交流,在获取大学生的信任和依赖后,以各种理由诱导转账;还有的诈骗分子通过建立虚假的兴趣社群、交友群组等,吸引有社交需求的大学生加入,在群内营造温暖、和谐的氛围,逐步诱导大学生参与刷单、投资等诈骗活动。此外,部分大学生由于社交经验匮乏,在面对他人的主动示好时,容易产生感激和信任心理,难以分辨对方的真实意图,从而陷入诈骗陷阱。

四、基于心理因素的干预策略与启示

(一) 强化认知教育,提升风险感知能力

强化认知教育是提升大学生风险感知能力、降低网络诈骗易感性的核心策略,能够从根本上帮助大学生树立正确的网络安全认知,增强对网络诈骗的识别能力和防范意识。认知教育的核心目标是弥补大学生在网络诈骗认知层面的不足,纠正认知偏差,让大学生全面、系统地掌握网络诈骗的相关知识和防范技能。

高校应将网络安全教育纳入必修课程体系,构建系统化、常态化的教育模式。课程内容应结合大学生的认知特点和诈骗场景的阶段性特征进行设计,涵盖网络诈骗的常

见类型、典型案例、套路特征、识别方法、应对措施等核心内容,同时融入个人信息保护、网络行为规范等相关知识。在教学方式上,应突破传统的课堂讲授模式,采用案例分析、小组讨论、专家讲座等多种形式,增强教学的趣味性和针对性。例如,邀请反诈一线的工作人员进校园开展专题讲座,结合真实案例讲解诈骗手段的演变和识别技巧;组织学生对典型诈骗案例进行分析讨论,让学生在互动中深化对诈骗风险的认知。此外,还可以开发网络安全教育慕课、线上学习平台等,方便学生运用碎片化时间进行学习,实现认知教育的全覆盖。同时,通过模拟演练增强信息甄别能力,高校可以联合相关机构,搭建网络诈骗模拟场景,让学生在模拟环境中体验诈骗过程,学习识别和应对技巧。例如,开展模拟刷单诈骗、模拟冒充客服诈骗等演练活动,让学生在实践中学会辨别虚假信息、拒绝诈骗诱惑;组织学生参与网络安全知识竞赛、反诈情景剧表演等活动,以多样化的形式强化认知效果。

这种认知教育模式能够有效帮助大学生纠正对网络环境的过度信任和侥幸心理,系统提升信息甄别能力,从认知层面筑牢反诈防线。常态化的认知教育能够让网络安全知识深入人心,让大学生在面对网络诈骗信息时,能够快速做出准确判断,主动规避风险。同时,认知教育还能够培养大学生的网络安全素养,让他们养成良好的网络行为习惯,不仅能够有效防范网络诈骗,还能为其未来的学习和职业发展提供安全保障。

(二) 优化心理疏导机制,减少情绪化决策

优化心理疏导机制能够帮助大学生提升情绪调节能力,减少情绪化决策,从而降低因情绪驱动导致的网络诈骗易感性。心理疏导机制的核心目标是帮助大学生正确认识和调节自身情绪,增强心理韧性,在面对网络诈骗中的情绪诱惑和压力时,能够保持理性判断。

高校应建立完善的校园心理支持体系,缓解大学生的焦虑与压力。可以依托心理健康教育中心,组建专业的心理辅导团队,为大学生提供个体咨询、团体辅导、心理测评等多种形式的心理服务。针对不同年级大学生的心理特点和压力来源,开展针对性的心理疏导活动。例如,为大一新生开展适应新环境的团体辅导,帮助他们缓解入学焦虑;为大四学生开展求职压力疏导专题活动,帮助他们调整心态,理性应对求职过程中的各种诱惑。同时,建立心理危机预警机制,及时发现和干预存在心理问题的学生,避免因心理状态不佳导致的非理性决策。此外,培养大学生的批判性思维,增强理性判断能力,高校可以将批判性

思维培养融入日常教学和校园活动中,通过开设逻辑思维课程、组织辩论比赛、开展问题探究式学习等方式,训练大学生的独立思考能力和逻辑分析能力。引导大学生在面对网络信息时,学会多角度、全方位地分析信息的真实性和可靠性,不盲目相信权威、不轻易跟随他人,能够基于客观事实做出判断。

完善的心理疏导机制和批判性思维培养能够有效提升大学生的情绪调节能力和理性判断能力,让他们在面对网络诈骗中的贪婪、恐惧等情绪诱惑时,能够保持清醒的头脑,主动抵制诱惑;在面对群体压力和从众心理时,能够坚持自己的判断,不盲目跟风。这不仅能够降低大学生陷入网络诈骗的风险,还能促进大学生的心理健康发展,提升其综合素质。

(三) 完善社会支持网络, 弥补经验短板

完善社会支持网络能够为大学生提供多维度的支持和帮助,弥补其社会经验匮乏的短板,从而降低网络诈骗易感性。社会支持网络的核心目标是整合家庭、学校、社会等多方资源,为大学生构建一个全方位的防护体系,帮助他们在面对网络诈骗时能够获得及时的指导和帮助。

高校应加强家校联动,构建防骗信息共享平台。通过建立家长微信群、家长会、家校沟通函等多种形式的沟通渠道,及时向家长传递网络诈骗的最新动态、典型案例和防范知识,引导家长重视对孩子的网络安全教育。同时,鼓励家长与孩子就网络使用、兼职打工、社交交友等问题进行沟通交流,了解孩子的网络行为和心理状态,共同发现和解决潜在的风险。例如,在新生入学季,通过家长会向家长普及新生常见的诈骗类型和防范措施;在诈骗高发期,及时向家长推送预警信息,提醒家长关注孩子的财产安全。此外,鼓励大学生参与社会实践,积累风险应对经验,高校可以组织开展多样化的社会实践活动,如志愿服务、社会调研、企业实习等,让大学生走出校园,接触社会,在实践中积累社会经验和人际交往经验。同时,联合相关机构开展反诈实践活动,如组织学生参与反诈宣传志愿活动、走进社区开展反诈调研等,让大学生在实践中深化对网络诈骗的认知,提升风险应对能力。

完善的社会支持网络能够有效弥补大学生社会经验匮乏的不足,让他们在面对网络诈骗时能够获得家庭的关怀、学校的指导和社会的帮助。家校联动能够形成教育合力,从家庭和学校两个层面强化大学生的反诈意识;社会实践能够让大学生在实践中提升能力,积累经验,从而在面对网络诈骗时能够更加从容地应对。这种多维度的社会支持

能够为大学生的成长成才提供安全保障,助力他们更好地适应社会。

(四) 针对人格特质的差异化干预设计

针对人格特质的差异化干预设计能够精准匹配不同大学生群体的心理特点,提升干预工作的针对性和有效性,从而降低网络诈骗易感性。差异化干预的核心目标是根据大学生不同的人格特质和心理需求,制定个性化的干预方案,实现精准反诈。

高校应针对高好奇心群体开展定向警示教育,通过分析该群体容易陷入的诈骗类型和心理动因,设计针对性的警示内容和教育形式。例如,收集因好奇心驱使陷入诈骗的典型案例,制作成警示教育视频、图文手册等,通过校园广播、宣传栏、线上平台等渠道进行推送;组织高好奇心群体参与诈骗模拟体验活动,让他们在亲身体验中感受诈骗的危害,增强防范意识。同时,引导该群体树立正确的网络探索观念,学会在探索新鲜事物的同时,保持对风险的警惕。此外,针对社交需求强烈者提供健康社交引导,高校可以搭建多样化的健康社交平台,如组织兴趣社团、主题沙龙、文体活动等,为大学生提供正规、健康的社交渠道,满足他们的社交需求。同时,开展社交礼仪、人际交往技巧、网络社交安全等方面的培训活动,帮助他们提升社交能力,学会在网络社交中保护自己。例如,组织网络社交安全专题讲座,讲解网络交友的风险和防范技巧;开展社交情景模拟活动,让学生在模拟场景中学习如何分辨他人的真实意图,避免陷入社交诈骗陷阱。

差异化的干预设计能够精准把握不同人格特质大学生的易感点,实现“对症下药”,有效提升干预工作的效果。针对高好奇心群体的定向警示教育能够帮助他们在保持探索欲的同时,增强风险防范意识;针对社交需求强烈者的健康社交引导能够帮助他们在满足社交需求的同时,规避网络社交诈骗风险。这种个性化的干预方式能够让反诈工作更加精准、高效,为不同特质的大学生提供更加贴合的安全保障。

(五) 搭建智能预警平台, 强化风险前置防控

搭建智能预警平台是运用技术手段强化风险前置防控、降低大学生网络诈骗易感性的重要补充策略,能够实现网络诈骗风险的早发现、早预警、早干预,为大学生构建技术层面的防护屏障。该策略的核心目标是借助技术赋能,弥补人工干预的滞后性,提升反诈工作的精准度和时效性。

高校应联合网络技术机构,搭建校园专属的网络诈骗

智能预警平台,整合校园网络数据、学生网络行为数据、诈骗风险特征数据等多维度信息,运用大数据分析、人工智能识别等技术,建立网络诈骗风险识别模型。平台应重点监测学生的网络支付行为、网络社交行为、网络浏览行为等,对涉及高风险诈骗场景的行为进行实时识别和预警。例如,当学生点击钓鱼链接、与诈骗高危账号进行频繁互动、进行大额非日常转账等行为时,平台应及时触发预警机制,通过校园APP推送预警信息、短信提醒、辅导员联动告知等多种方式,向学生发出风险提示。同时,平台应建立预警响应机制,针对不同等级的风险预警,制定差异化的响应流程,对于高风险预警,安排专人跟进核实,及时介入干预,避免诈骗事件发生。此外,定期对预警数据进行分析总结,梳理大学生网络诈骗的高发时段、高发场景和高发行为特征,为优化反诈干预策略提供数据支撑。

智能预警平台的搭建能够实现网络诈骗风险的前置防控,将反诈工作从“事后处置”向“事前预防”转变,有效提升反诈工作的主动性和有效性。技术层面的防护屏障能够与人工干预形成互补,全方位覆盖大学生的网络行为场景,及时提醒大学生规避潜在风险。同时,预警数据的分析应用能够帮助高校精准把握大学生网络诈骗的动态特征,为后续反诈工作的优化调整提供科学依据,进一步提升干预体系的针对性和适配性。

(六) 健全协同联动机制,凝聚反诈工作合力

健全协同联动机制是凝聚多方力量、形成反诈工作合力的关键策略,能够整合高校、公安、社区、企业等多方资源,构建全方位、立体化的反诈防护网络,提升反诈干预工作的整体效能。该策略的核心目标是打破各方资源壁垒,实现信息共享、责任共担、行动协同,形成齐抓共管的反诈工作格局。

高校应主动与当地公安部门建立常态化协同联动机制,签订反诈合作协议,明确双方职责分工。公安部门应定期向高校推送最新的诈骗动态、典型案例和防范要点,为高校开展反诈教育提供专业支持;同时,协助高校开展反诈培训、模拟演练等活动,提升高校反诈工作队伍的专业能力。高校应及时向公安部门反馈校园内发生的诈骗线索和预警信息,配合公安部门开展案件侦查和处置工作。此外,加强与社区、网络服务企业等相关主体的联动合作,社区应协助高校开展面向学生及家长的反诈宣传活动,营造良好的社区反诈氛围;网络服务企业应配合高校加强校园网络环境治理,清理校园网络内的诈骗信息,屏蔽诈骗高危账号和链接。建立多方参与的反诈工作联席会议制度,

定期召开会议,通报反诈工作进展,研究解决工作中存在的问题,统筹推进反诈工作各项任务的落实。

协同联动机制的健全能够有效整合多方资源,凝聚反诈工作合力,形成全方位的反诈防护网络。公安部门的专业支持能够提升反诈工作的专业性和权威性,社区的参与能够扩大反诈宣传的覆盖面,网络服务企业的配合能够净化校园网络环境。各方力量的协同配合能够弥补单一主体开展反诈工作的局限性,提升反诈干预工作的整体效能,为大学生构建更加牢固的反诈防护体系,进一步降低网络诈骗易感性。

(七) 强化反诈氛围营造,培育校园安全文化

强化反诈氛围营造是培育校园安全文化、潜移默化提升大学生反诈意识的长效策略,能够让反诈理念深入校园的各个角落,融入大学生的日常学习生活,形成“人人识诈、人人防诈、人人反诈”的良好氛围。该策略的核心目标是通过常态化、多样化的氛围营造,增强反诈工作的融入性和影响力,引导大学生自觉树立反诈意识。

高校应整合校园宣传资源,构建多渠道、全覆盖的反诈宣传体系。充分运用校园宣传栏、校园广播、校园电视台、教学楼电子屏等线下宣传阵地,定期更新反诈宣传内容,展示典型诈骗案例、防范技巧、预警信息等;依托校园官网、微信公众号、微博、抖音等线上平台,发布反诈短视频、图文科普、案例解析等内容,增强宣传的趣味性和传播力。同时,结合重要时间节点,开展主题性反诈宣传活动,如“反诈宣传月”“新生反诈教育周”等,通过反诈知识竞赛、反诈手抄报比赛、反诈主题班会、反诈文艺汇演等多种形式,调动大学生参与反诈工作的积极性和主动性。鼓励学生成立反诈志愿者协会,组织志愿者开展校园内反诈宣传、peer教育等活动,通过学生之间的互动交流,提升反诈宣传的感染力和实效性。此外,将反诈元素融入校园文化建设,在校园文化活动、社团活动中融入反诈主题,让反诈理念成为校园安全文化的重要组成部分。

反诈氛围的持续营造能够培育浓厚的校园安全文化,让反诈意识潜移默化地深入大学生心中,帮助大学生养成主动防范网络诈骗的行为习惯。多样化的宣传形式能够提升反诈工作的吸引力,激发大学生的参与热情,形成全员参与反诈的良好局面。校园安全文化的培育不仅能够有效降低大学生网络诈骗易感性,还能提升整个校园的安全管理水平,为大学生们的成长成才营造安全、和谐的校园环境。

(八) 建立反诈效果评估机制,动态优化干预体系

建立反诈效果评估机制是保障干预策略落地成效、实

现动态优化的关键环节,能够及时发现干预工作中的不足,确保干预体系始终适配大学生网络诈骗易感性的变化特征。该策略的核心目标是通过科学的评估指标和方法,量化反诈工作成效,为干预策略的调整优化提供依据。

高校应构建多维度的反诈效果评估指标体系,指标内容需覆盖大学生的认知提升程度、风险感知能力变化、实际受骗发生率、干预策略参与度等核心维度。例如,通过问卷调查、知识测试等方式,评估大学生对网络诈骗知识的掌握程度和认知偏差纠正情况;通过分析校园智能预警平台数据、诈骗案例上报数据,评估实际受骗风险的降低效果;通过统计反诈课程出勤率、模拟演练参与率、宣传活动互动量等,评估干预策略的学生参与度。同时,建立常态化的评估流程,定期开展阶段性评估和年度综合评估,采用定量分析与定性分析相结合的方法,全面梳理干预工作的成效与不足。此外,根据评估结果建立干预策略动态调整机制,针对评估中发现的薄弱环节,及时优化干预内容和实施方式。例如,若发现某类诈骗手段的识别率提升不明显,需强化对应类型的案例教学和模拟演练;若发现特定年级学生的易感性仍较高,需针对性调整教育内容和干预形式。

反诈效果评估机制的建立能够推动反诈干预工作从“经验驱动”向“数据驱动”转变,提升干预体系的科学性和适配性。常态化的评估与动态优化能够确保干预策略始终紧跟诈骗手段的演变趋势和大学生心理变化特征,持续提升反诈工作成效。同时,评估结果能够为高校反诈工作的资源配置、重点部署提供科学依据,避免工作盲目性,实现反诈资源的高效运用,进一步筑牢大学生网络诈骗防护防线。

(九) 强化学生主体参与意识,构建自主反诈体系

强化学生主体参与意识是构建自主反诈体系、提升反诈工作长效性的核心策略,能够充分调动大学生的主观能动性,让大学生从“被动接受防护”转变为“主动参与反诈”,形成自我防护与互助防护相结合的良好格局。该策略的核心目标是激发大学生的反诈主动性和责任感,提升其自主防范能力和互助防护水平。

高校应搭建多元化的学生反诈参与平台,鼓励大学生深度参与反诈工作的各个环节。例如,设立反诈学生工作坊,组织学生参与反诈案例整理、宣传材料设计、模拟演练策划等工作,让学生在参与过程中深化对反诈知识的理解和掌握;开展“反诈先锋”评选活动,表彰在反诈宣传、风险预警、帮助同学规避诈骗等方面表现突出的学生,激

发学生的参与热情和责任感。同时,推动建立学生反诈互助网络,以班级、宿舍为单位,选拔具备较强反诈意识和能力的学生担任“反诈联络员”,负责日常反诈知识传递、风险提示、可疑信息上报等工作,形成“高校—院系—班级—宿舍”四级学生互助反诈网络。此外,引导大学生主动学习反诈知识,养成自主甄别网络信息的习惯,鼓励学生在遇到可疑信息时主动向学校、老师或同学求证,在发现诈骗线索时及时上报,形成“人人都是反诈主体、人人参与反诈防护”的自主反诈氛围。

学生主体参与意识的强化能够构建起可持续的自主反诈体系,让反诈防护融入大学生的日常学习生活。大学生的主动参与不仅能够提升自身的反诈能力,还能通过互助网络带动身边同学共同提升防护水平,扩大反诈工作的覆盖面和影响力。这种自主反诈体系能够与高校的官方干预策略形成互补,进一步提升反诈工作的长效性,为大学生的网络安全提供更加坚实的保障。

五、研究价值与实践意义

本研究围绕大学生网络诈骗易感性的心理因素及干预启示展开系统且深入的探析,兼具重要的理论价值、实践价值与教育价值,不仅能够为青年网络安全领域的学术研究深化提供全新的思路与方向,更能为高校反诈工作的精准落地、高效推进提供多维度的实践支撑,助力形成“理论指导实践、实践反哺理论”的良性循环,切实回应数字化时代背景下大学生网络安全保障的现实需求。

(一) 理论价值:拓展青年网络安全心理研究维度

本研究的理论价值核心在于进一步拓展了青年网络安全心理研究的深度与广度,为该领域的学术探索提供了更为系统的分析框架与新颖的研究视角。在当前数字化转型持续深化、青年群体网络行为愈发多元复杂的背景下,现有青年网络安全心理研究多聚焦于单一风险行为或单一心理因素,研究体系相对零散。本研究立足心理学核心理论基础,创新性地构建了“认知—情绪—社会经验—人格特质”四维分析模型,将大学生网络诈骗易感性的核心影响因素进行系统化整合与深度拆解,不仅打破了以往单一维度研究的局限,更清晰揭示了各心理因素之间的内在关联、相互作用机制以及对易感性的综合影响路径。这一分析模型不仅适用于大学生网络诈骗易感性研究,还可为青年群体网络沉迷、网络暴力参与等其他网络风险行为的心理机制研究提供可借鉴的分析范式,有效丰富青年网络心理学的理论体系内涵。同时,研究紧密聚焦数字化时代的鲜明

背景,深入探讨了网络原生代青年群体心理脆弱性的形成机理,重点分析了网络环境的开放性、虚拟性、即时性等特点与青年心理发展阶段的适配性问题,针对网络原生代青年认知发展、情绪调节、社会适应等方面的阶段性特点展开精准剖析,填补了数字化转型期青年网络安全心理研究的部分空白,为后续相关领域的学术研究提供了坚实的理论基础与明确的研究方向,推动青年网络安全心理研究向更具针对性、系统性的方向发展。

(二) 实践价值:提升高校网络安全教育实效性

本研究的实践价值主要体现在为高校提升网络安全教育实效性提供了科学、精准的理论依据与可操作、可落地的实施路径,助力高校打破传统反诈工作的瓶颈,构建起精准化、系统化、长效化的反诈工作体系。当前高校网络安全教育存在“内容同质化、形式单一化、对象无差别化”的问题,教育效果难以充分彰显。本研究通过大量理论梳理与逻辑推演,系统梳理了大学生网络诈骗易感性在不同年级、不同人格特质群体中的阶段性特征与核心心理动因,精准定位了新生适应期、学业提升期、求职就业期等关键阶段的反诈重点,明确了高好奇心、高社交需求等不同特质群体的薄弱环节,为高校制定分级分类的防骗教育方案提供了直接、具体的实践指导。基于研究提出的针对性干预策略,高校能够精准匹配教育资源,针对新生的环境适应问题设计适应性反诈教育模块,针对高年级学生的求职升学需求开展专项反诈培训,有效避免安全教育“一刀切”的低效问题。此外,研究突破了传统安全教育重知识传递、轻心理干预的局限,创新性地提出构建“认知教育+心理支持+技术防护”的多元干预体系,明确了各体系之间的协同配合机制,例如将心理疏导融入认知教育全过程,通过技术手段实现风险前置预警与教育精准推送,能够有效提升高校反诈工作的针对性与有效性,推动高校网络安全教育从“被动应对诈骗事件”向“主动预防风险发生”转变,切实降低大学生网络诈骗发生率,为校园安全稳定提供有力保障。

(三) 教育价值:促进大学生心理资本的全面发展

本研究的教育价值集中体现在将反诈教育与大学生核心素养培育进行有机融合,突破了“反诈教育仅为风险防范”的传统认知,助力大学生心理资本的全面提升,为其长远发展与终身成长提供坚实有力的支撑。大学生作为国家未来发展的核心力量,其核心素养的培育直接关系到个人成长质量与社会发展潜力。本研究提出的干预策略不仅聚焦于降低网络诈骗易感性这一直接目标,更注重以反诈

教育为载体,通过系统的认知教育、丰富的实践体验、精准的心理疏导等多元方式,全方位培养大学生的风险决策能力、信息甄别能力与批判性思维能力。这些核心素养是大学生在网络时代应对各类风险挑战的必备能力,能够帮助大学生在学习科研、求职就业、日常社交等各类场景中准确判断信息真伪、理性做出决策,有效避免因认知偏差或情绪冲动导致的各类风险行为。同时,研究强调通过社会实践、互助网络构建等方式,引导大学生走出校园、接触社会,在实践中积累社会经验、提升人际交往能力,增强大学生的社会适应力与心理韧性,帮助大学生在面对挫折与压力时保持积极乐观的心态,提升情绪调节能力与问题解决能力。这种将安全防护与素养培育深度融合的教育模式,精准契合了新时代大学生全面发展的教育目标,能够实现反诈教育与素质教育的协同推进、同向发力,不仅能够提升大学生的网络安全素养,更能促进大学生心理资本的持续积累与全面提升,为其成长为适应新时代发展需求的高素质人才奠定坚实基础。

六、结束语

大学生网络诈骗易感性问题关乎大学生的身心健康发展与校园的安全稳定,构建科学有效的干预体系具有重要的现实意义与长远价值。高校作为大学生培养与教育的核心主体,今后应系统强化认知教育以纠正偏差,优化心理疏导以减少情绪化决策,完善社会支持以弥补经验短板,并针对人格特质开展差异化干预,同时积极搭建智能预警平台、健全协同联动机制、营造校园反诈文化、建立效果评估体系,更要强化学生主体参与,构建全方位、精准化、可持续的“教育—防护—支持”闭环,从而全方位提升大学生的网络诈骗防范能力,帮助大学生树立正确的网络安全观,养成良好的网络行为习惯,为大学生在网络时代的健康成长保驾护航,同时也为校园安全建设与和谐网络环境构建奠定坚实基础。

参考文献:

- [1] 焦娟,姜淑梅.大学生网络诈骗受害心理剖析与防控策略[J].教育思想理论研究,2025,3(10):254-257.
- [2] 郑珍.AI时代大学生电信网络诈骗受害的现状、原因及防控路径[J].湖南人文科技学院学报,2025,42(05):104-112+120.
- [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:南京信息工程大学,2025.
- [4] 高原.大学生网络诈骗易感性的影响因素[D].杭州:浙江大学,2021.