AIGC背景下青少年网络诈骗风险分析与防范教育对策研究

李江娥　陈　锋

浙江安防职业技术学院，中国·浙江　温州　325000

【摘　要】生成式人工智能（AIGC）技术的迅猛发展，在为社会带来变革性动力的同时，也为网络诈骗提供了前所未有的技术赋能，对认知判断能力尚在发展中的青少年群体构成了严峻而隐蔽的威胁。本文旨在系统剖析AIGC背景下青少年新型网络诈骗的风险生成机制，AIGC新型网络诈骗动摇了青少年依赖感官经验建立的信任体系，易受到AIGC驱动的社会工程学攻击。针对这些新型风险，提出以培养“数字韧性”为核心的三维防治体系，旨在帮助青少年在AIGC时代建立抵御风险、适应挑战并实现健康成长的综合素养。

【关键词】AIGC；新型网络诈骗；数字韧性；风险分析；青少年网络素养

【基金项目】2024年浙江省妇联、浙江省妇女研究会课题《新时代青少年网络素养教育提升对策的研究——聚焦网络十大领域》（编号202423）。

引言

随着生成式人工智能技术的迅猛发展，其在推动社会各领域创新的同时，也带来了前所未有的网络安全挑战。人工智能生成内容（Artificial Intelligence Generated Content，AIGC）技术凭借其强大的内容生成和拟社会交互能力，正被不法分子用于构建新型网络诈骗体系，对认知判断能力尚不成熟的青少年群体构成严重威胁。《未成年人网络保护条例》的实施和党的二十大报告对“网络强国”建设的强调，为加强青少年网络素养教育提供了政策指引。在此背景下，深入剖析AIGC技术赋能网络诈骗的新机制，探索青少年在这一新型风险场域中的脆弱性特征，构建与之相适应的教育防护体系，具有重要的理论价值和现实紧迫性。本研究旨在通过系统分析AIGC背景下青少年网络诈骗的风险特征与生成逻辑，提出以“数字韧性”培育为核心的综合防治策略，为推进新时代青少年网络素养教育提供参考。

1　AIGC技术赋能网络诈骗的方式

1.1身份伪造诈骗

此类诈骗利用AIGC的生成与模仿能力，将简单的身份冒充升级为全方位的身份克隆：

（1）深度伪造视频通话诈骗。诈骗分子通过社交媒体获取目标的简短视频和音频，利用多模态融合技术与实时换脸模型，在视频通话中克隆出亲人、朋友或领导的容貌与声音，以遇急事需用钱等理由要求实时转账。受害者亲眼所见、亲耳所闻，心理防线极易被攻破，技术含量高、危害性大。

（2）AI语音克隆诈骗。利用生成对抗网络（Generative Adversarial Networks，GANs）或扩散模型，以一段几秒钟的公开语音为样本，即可克隆出高度逼真的声音，诈骗分子通过电话或语音消息，冒充亲友实施诈骗。相较于视频伪造，技术门槛更低，更易于大规模实施，在仅有语音沟通的场景下极具迷惑性。

（3）虚拟形象创建诈骗[1]。生成一张完全不存在的、高颜值、高亲和力的人脸照片，创建社交账号，为长期诈骗铺设了完美的第一印象，消除了受害者对头像真实性的怀疑。

1.2信息合成与钓鱼攻击

传统钓鱼邮件常有语法错误和格式问题。利用大模型（Large Language Models，LLMs），可以生成语法完美、语气逼真、无拼写错误的钓鱼邮件。它可以根据目标公司信息，冒充其管理或技术部门，编写出极具说服力的内部邮件。利用AIGC生成伪造的法院传票、银行催款单、中奖通知书、学校录取信等。这些文件格式规范，印章逼真，内容由LLMs编写，逻辑严密。其目的是用于制造恐慌或诱惑，迫使受害者在紧张或兴奋情绪下做出非理性决策。

1.3舆论操纵与敲诈勒索

这一手段需要结合社交媒体、游戏平台、内容平台传播虚假信息，AIGC可以根据不法分子的非法意图凭空制造出看似真实的信息，从而使得敲诈勒索和舆论攻击的破坏力提高。如将公众人物或普通人的面部合成至不雅视频或图片中、在商业竞争或舆论战中利用AIGC生成某公司高管发表的不当言论，一次快速在社交媒体上引发舆情海啸，造成巨大现实损失。

2　青少年心理特征与网络诈骗易感性分析

AIGC背景下，青少年心理特征呈现“高好奇、低警惕、强情感、弱判断”的复合特征，使其极易成为新型网络诈骗的“优质”目标。

（1）好奇心强与信息甄别能力不足的矛盾。作为“数字原住民”，青少年对AIGC技术有天然好奇心，驱动其主动接触新技术。但青少年的信息甄别能力滞后于技术

迭代，矛盾显著。如深度伪造“熟人求助”视频突破其认知防线，易被误判为真。

（2）情绪波动大与冲动决策倾向。青春期青少年情绪调控能力未成熟，易因贪念、恐惧、从众等情绪冲动决策。如刷单返利诈骗中，青少年受“快速赚钱”欲望驱使，未核实即转账；在“账户冻结威胁”诈骗里，诈骗分子借公检法等权威身份制造恐惧，迫使青少年在情绪压力下仓促决策。

（3）从众心理与社交媒体诱导效应。从众心理在AIGC时代有新特征，如虚拟社交依赖、存在显著城乡差异。社交媒体算法推荐形成“信息茧房”，青少年易达成群体共识，如群聊集体转账被骗；诈骗分子还借短视频、直播等骗取青少年同情心与钱财[2]。

3 AIGC背景下青少年网络诈骗风险识别

AIGC技术不仅升级了诈骗工具，更重塑了诈骗的底层逻辑。其对青少年构成的威胁是系统性的，主要源于技术滥用带来的认知解构风险与社会工程学实现的心理操控风险。

3.1认知解构风险

AIGC技术的滥用、恶意应用，从根本上动摇了青少年依赖感官经验建立起来的信任体系。AIGC新型网络诈骗基于GANs和扩散模型的深度伪造技术，能够生成在像素级精度上以假乱真的肖像、声音和视频,这种真实性足够强的输出内容在视觉和听觉层面达到了与真实记录无法区分的程度[3]。青少年的世界观尚在形成中，其判断力很大程度上依赖于五官感受到的直接经验，当最可靠的感官证据都可以被完美伪造时，其内在的信任基础将遭受剧烈冲击，可能导致其对一切数字信息产生虚无主义的不信任感，或走向另一个极端——盲目接受一切。

3.2心理操控风险

AIGC技术使社会工程学从简单的欺骗演变为长期的、系统性的心理操控，精准打击青少年发展中的心理特质。许多青少年在现实社交中存在孤独感或挫败感，LLMs驱动的聊天机器人可以模拟人类的情感、幽默和共情，进行7×24小时不间断的情感陪护。它不急于求成，而是通过数周甚至数月的时间，逐步了解目标的喜好与弱点，建立起深厚的情感依赖。当情感依赖建立到一定程度后，任何要求，如借钱救急、共同投资等都显得顺理成章。此时，青少年付出的不仅是金钱，更是情感上的毁灭性打击。

4 AIGC时代青少年网络诈骗三维防治策略

面对AIGC新型网络诈骗挑战，为帮助青少年在复杂数字环境中识别风险、应对冲击、恢复活力并智慧成长，本文构建了学校、家庭、社会协同教育的教育策略。

（1）学校教育系统化融入与沉浸式实训。学校作为青少年网络素养教育主渠道，需从零星宣讲升级为系统化、课程化、沉浸式教育，将“AIGC时代青少年反诈素养提升”目标融入校园学习生活各场景。其一，系统融入反诈教育，通过课程与沉浸式实训贯穿校园生活。其二，开展批判性数字取证训练，分析可疑信息、核对信息源及逻辑漏洞；进行紧急流程演练，强化应对标准并辅以心理调适与复盘；以反诈剧本杀等互动形式，深化对诈骗逻辑的理解。其三，成立数字安全社团，组织主题班会、鉴伪工作坊，评选数字韧性标兵，营造“反诈防骗、人人有责”文化，推动青少年从被动受害者转为主动防御者。

（2）家庭提供情感支持与行为引导。家庭是数字韧性教育的起点和情感基石，其核心作用在于提供无条件的支持环境与日常化的行为引导。一、为了了解孩子的动态，训练孩子的批判性思维，定期召开家庭会议，以开放、非批判的态度讨论网络见闻，使用开放式提问，引导孩子表达想法，而非直接下达禁令。二、以民主方式共同商定家规，内容包括：任何线上转账前必须进行线下二次确认、不扫描来源不明的二维码、社交账号隐私设置为最高级别等。三、通过组织家庭户外活动、鼓励线下交友、培养体育艺术等兴趣爱好，提供AI无法替代的真实成就感和情感联结。

（3）社会生态构建与正向引导策略。社会层面应构建“教育-技术-治理”三位一体防护网，推动青少年宫、科技馆等公共文化设施常态化开设“AIGC反诈科普”课程，利用VR/AR技术打造沉浸式体验舱，模拟诈骗场景提升青少年辨识能力。网信部门需督促平台履行主体责任，强制AIGC生成内容显著标识，在高风险场景设置强制提示机制。社区联合派出所、银行及志愿者开展反诈实训，通过竞赛活动深化邻里联动。同时建立跨部门协作机制，完善法规体系与技术标准，形成“政策-执行-反馈-优化”的闭环管理，切实提升青少年防诈反诈能力。

5 结语

本研究系统分析了AIGC技术对青少年网络安全的认知解构风险，另一方面借助个性化交互实施心理操控。面对这一挑战，传统的防护模式已显不足，亟需构建以“数字韧性”为核心的新型教育范式。通过学校、家庭、社会三维协同的防治体系，着力培养青少年在数字环境中的风险识别、应对及恢复能力。未来研究需持续追踪AIGC技术演进，深化实证研究，探索智能化反诈教育路径，为构建适应“人机共生”时代的青少年网络素养教育体系提供持续支持。

参考文献：

[1]靳雨婷.AIGC背景下新型网络诈骗手段与对策研究[J].网络安全技术与应用,2025,(02):143-145.

[2]程雪.青少年网络风险认知及其影响因素研究——以重庆市为例[D].重庆工商大学.2020.

[3]张俊杰,张纯琍.基于深度伪造技术的AI诈骗风险与预防[J].广西警察学院学报,2023,36(05):41-48.