互联网时代高校大学生防范网络电信诈骗安全教育研究

于成程
扬州大学

摘　要：互联网高速发展，网络电信诈骗成为威胁高校大学生群体安全的重要问题。本文通过分析网络电信诈骗的特点和成因，探讨高校大学生在面对网络电信诈骗时的防范意识和应对策略。通过对高校安全教育现状的研究，提出了一系列防范网络电信诈骗的教育对策和建议，以期提高大学生的防范意识和自我保护能力，减少网络电信诈骗事件的发生，保障大学生群体的安全。

关键词：高校大学生；网络电信诈骗；安全教育
【DOI】10.12252/j.issn.2096-6288.2025.02.008

引言

本文旨在通过详细分析网络电信诈骗的现状和特点，深入探讨高校大学生在面对网络电信诈骗时的防范意识和应对策略。首先，我们将分析网络电信诈骗的现状，包括其发展趋势、常见类型和实施手段。接着，探讨高校大学生在防范网络电信诈骗方面的现状，指出当前存在的主要问题和不足之处。然后，结合实际案例，提出切实可行的防范措施，包括加强网络安全教育、推广网络安全文化、完善防范制度和机制、开展实战演练以及加强与社会各界的合作等。最后，本文将总结研究成果，提出对未来高校防范网络电信诈骗安全教育的展望。

通过本文的研究，希望能够引起高校和社会各界对网络电信诈骗问题的重视，帮助大学生提高防范意识和自我保护能力，构建起完善的高校防范网络电信诈骗的安全教育体系，为大学生的安全和健康成长保驾护航。

一、网络电信诈骗的现状与特点

（一）网络电信诈骗的定义及类型

网络电信诈骗是指犯罪分子利用互联网和电信技术，实施各种形式的诈骗行为。这类诈骗手段多种多样。虚假招聘是指犯罪分子通过发布虚假的招聘信息，吸引求职者上当。在求职者提交个人信息或支付所谓的“报名费”“培训费”后，犯罪分子便会消失，造成求职者的经济损失和个人信息泄露。网购诈骗则是利用虚假的购物网站或冒充知名电商平台，通过诱人的价格和虚假的商品信息吸引消费者。一旦消费者支付了款项，商品往往无法到货，或者收到的商品与描述严重不符。中奖诈骗是诈骗分子通过短信、电话或邮件通知受害者中奖，要求支付“税费”“手续费”或提供个人信息以领取奖品。这类诈骗常常通过巨额奖金或豪华奖品吸引受害者上当。冒充亲友的诈骗手段是通过盗用或冒充受害者亲友的身份，以各种理由向受害者索取钱财。例如，犯罪分子可能冒充受害者的亲友，谎称遇到紧急情况需要借款，从而骗取受害者的钱财。这些网络电信诈骗行为不仅手段多样，而且具有很强的隐蔽性和迷惑性，给受害者带来了严重的经济损失和心理伤害。了解这些常见的诈骗类型和手段，对于提高公众的防范意识和减少被骗风险具有重要意义。

（二）网络电信诈骗的现状

近年来，网络电信诈骗案件频发，且呈现出手段多样化、专业化和隐蔽化的特点。根据公安部统计数据显示，高校大学生因网络电信诈骗造成的经济损失逐年增加，严重影响了学生的学习和生活。

（三）网络电信诈骗的特点

网络电信诈骗具有以下几个显著特点：手段隐蔽：诈骗分子通过虚假信息和网络技术手段，掩盖其真实身份，增加受害者识别难度。目标明确：高校大学生因其容易获取个人信息，且金融风险意识较弱，成为诈骗分子的主要目标。技术含量高：诈骗分子利用高科技手段实施诈骗，甚至借助人工智能和大数据分析，精准定位受害者。

二、高校大学生防范网络电信诈骗的现状分析

（一）高校大学生的网络安全意识

高校大学生作为互联网的主要用户群体，频繁使用网络进行学习、社交和娱乐活动。然而，尽管高校普遍开设了网络安全相关课程，但大学生的网络安全意识普遍较为薄弱。调查显示，大部分学生对网络电信诈骗的认识不足，防范意识不强。许多大学生对网络电信诈骗的严重性认识不足，认为自己不会成为诈骗的目标。这种侥幸心理使他们在面对潜在威胁时缺乏警惕性。虽然部分学生接受过网络安全教育，但他们对网络电信诈骗的具体类型和手段了解不多，缺乏识别和应对的实际能力。不少大学生在网络活动中不注意保护个人信息，随

意在社交媒体上公开个人资料，给诈骗分子提供了可乘之机。

（二）高校防范网络电信诈骗的教育现状

目前，高校在防范网络电信诈骗方面的教育措施较为单一，主要集中在入学教育和网络安全知识讲座，缺乏系统性和持续性。多数高校的防范教育主要集中在新生入学时的集中讲座，内容多为基本的网络安全常识，缺乏深度和广度。学生接受的信息有限，难以应对复杂多变的网络诈骗手段。入学教育通常是一时性的，后续缺乏系统的、持续的网络安全教育活动。学生在初入学时可能受到一定的警示，但随着时间的推移，这种警惕性会逐渐减弱。现有的教育形式主要以讲座为主，缺乏互动性和实操性。学生多为被动接收信息，缺乏参与感和实际操作机会。

（三）高校大学生防范网络电信诈骗的实际情况

在实际生活中，大学生防范网络电信诈骗的能力参差不齐。部分学生能够及时识别诈骗信息，但仍有不少学生因轻信虚假信息而上当受骗。有些学生由于平时关注网络安全知识，能够较好地识别常见的诈骗手段，例如识别虚假招聘信息和网购诈骗。但更多的学生由于缺乏防范意识和知识，容易被各种花样翻新的诈骗手段所迷惑。即便有些学生对网络电信诈骗有一定的了解，但在实际面对诈骗信息时，往往缺乏有效的应对措施。例如，在接到冒充亲友的诈骗电话时，一些学生由于情急之下未能冷静分析，最终上当受骗。部分学生在日常网络活动中不注意保护个人隐私信息，如随意填写网络调查问卷、在社交平台上公开个人联系方式等行为，使得诈骗分子更容易获取他们的个人信息进行精准诈骗。

三、高校大学生防范网络电信诈骗的教育对策

（一）强化网络安全教育

网络安全教育是防范网络电信诈骗的基础。高校应加强对大学生的网络安全教育，通过多种形式提高学生的网络安全意识和防范能力。应在课程设置上加入网络安全教育内容。开设专门的网络安全课程，系统讲授网络电信诈骗的类型、特点、防范措施等内容，帮助学生全面了解网络电信诈骗的危害和防范手段。

（二）推动网络安全文化建设

网络安全文化是防范网络电信诈骗的重要保障。高校应营造良好的网络安全文化氛围，广泛宣传网络电信诈骗的防范知识，增强学生的自我保护意识。高校应利用校园媒体、宣传栏、网络平台等多种渠道，广泛宣传网络安全知识和防范网络电信诈骗的技巧。制作宣传海报、宣传手册和视频短片等，通过生动形象的方式吸引学生关注，提高他们的防范意识。此外，高校还应定期举办网络安全主题活动，如网络安全月、网络安全论坛等，增强学生对网络安全问题的关注。通过这些活动，让学生了解最新的网络安全动态，掌握防范网络电信诈骗的最新知识和技能。同时，鼓励学生参与网络安全志愿者活动，组织学生自发进行网络安全宣传和教育，形成人人参与、人人重视的网络安全文化氛围。

（三）建立健全防范网络电信诈骗的制度

制度建设是保障网络安全教育效果的重要环节。高校应建立健全防范网络电信诈骗的制度，确保在发生网络电信诈骗事件时能够迅速反应，及时处理。一是应建立信息发布机制。高校应设立专门的网络安全信息发布平台，及时发布网络安全预警信息和防范指南，帮助学生了解最新的网络电信诈骗手段和防范措施。二是建立举报机制。高校应设立网络电信诈骗举报渠道，鼓励学生在发现可疑情况时及时举报。举报机制应包括匿名举报和奖励措施，保护举报人的隐私，激励学生积极参与防范工作。三是建立应急处置机制。高校应制定网络电信诈骗事件的应急处置预案，明确事件发生后的处理流程和责任分工，确保在事件发生后能够迅速反应，及时采取措施，减少损失。

（四）开展网络电信诈骗防范实战演练

实战演练是提高学生应对网络电信诈骗能力的重要途径。高校可以定期组织学生参与网络电信诈骗防范实战演练，通过模拟真实场景，提高学生的应对能力。演练应尽可能逼真，涵盖不同类型的网络电信诈骗情景，如电话诈骗、短信诈骗、网络聊天诈骗等。通过亲身体验，让学生感受到诈骗手段的真实威胁，增强他们的防范意识。此外，演练过程中应注重互动和反馈。在演练结束后，组织学生进行讨论和总结，分析自己的应对措施，找出不足之处，并提出改进建议。通过反思和改进，不断提高学生的防范能力。

（五）加强与社会各界的合作

防范网络电信诈骗需要全社会的共同努力。高校应加强与公安机关、互联网企业和社区的合作，形成防范网络电信诈骗的合力，共同构建安全的网络环境。一是与公安机关合作。高校应与公安机关建立紧密的合作关系，及时获取最新的网络电信诈骗信息和防范建议。公安机关可以定期派出专业人员到高校举办讲座和培训，增强学生的防范意识和技能。二是与互联网企业合作。高校应与知名互联网企业合作，共同开展网络安全教育活动。互联网企业可以提供最新的网络安全技术和防范工具，帮助高校提高网络安全教育水平。三是与社区合作。高校应加强与所在社区的联系，形成校内外联动的防范网络电信诈骗机制。社区可以提供当地的网络安全情况和防范经验，帮助高校更好地了解和应对网络电信诈骗

问题。高校也可以组织学生参与社区的网络安全宣传和防范活动，为社区的网络安全建设贡献力量。

四、网络电信诈骗防范教育的实施路径

（一）课程设置

高校应将网络电信诈骗防范教育纳入课程体系，开设专门的防范网络电信诈骗课程，系统讲授网络电信诈骗的类型、特点和防范措施。课程应包括内容，介绍网络电信诈骗的基本概念、历史演变及其社会危害性，使学生对该问题有全面认识。详细讲解各类网络电信诈骗的具体手段和真实案例，通过案例分析帮助学生了解诈骗分子的行骗过程和手段。教授学生如何识别网络电信诈骗，如何保护个人信息，遇到疑似诈骗时应采取的措施等。讲解相关法律法规，提高学生的法律意识，使其在面对诈骗行为时能够依法维权。课程的设置应注重理论与实践相结合，通过丰富的案例分析和互动教学，增强学生的理解和记忆。同时，课程内容应与时俱进，及时更新和补充新的诈骗手段和防范策略。

（二）实践教学

实践教学是防范网络电信诈骗教育的重要环节，通过组织学生参与各种实践活动，提升其实际操作能力。模拟真实的诈骗场景，让学生亲身体验诈骗过程，提高其识别和应对诈骗的能力。演练应尽可能逼真，包括电话诈骗、短信诈骗、网络聊天诈骗等不同类型的情景。组织学生对实际发生的网络电信诈骗案例进行分析和讨论，找出诈骗手段的漏洞和防范措施。通过集体讨论，学生可以相互交流经验，提高防范意识。利用网络安全实验室，进行相关技术训练，如防火墙设置、网络安全监测和个人信息保护等，提升学生的技术防范能力。定期举办防诈骗知识竞赛，通过竞赛形式增强学生学习防范知识的积极性和主动性，并在竞赛中巩固所学内容。

（三）技术手段

在互联网时代，利用信息技术手段开展防范网络电信诈骗教育显得尤为重要。高校应开发和使用各种技术工具和平台，以提高教育的效果和覆盖面。开发防范网络电信诈骗的教育软件，提供在线课程、案例库、知识问答等功能，方便学生随时随地学习防范知识。软件应具有交互性和趣味性，以吸引学生主动学习。建立防范网络电信诈骗的教育平台，集成教育资源、实践活动和交流社区等功能，为学生提供全面的学习支持。平台可以发布最新的诈骗案例和防范策略，及时更新内容。开发手机应用，提供防范知识、报警功能和紧急联系人等服务，方便学生在日常生活中使用。应用应具有用户友好的界面和便捷的操作方式。推荐和推广使用各种网络安全工具，如防火墙、杀毒软件、隐私保护软件等，帮助学生保护个人信息和防范网络攻击。

（四）综合考评

为了确保防范网络电信诈骗教育的效果，高校应建立综合考评体系，将学生的防范能力纳入综合素质评价。综合考评应包括理论知识、实践操作和技术应用三方面的内容，全面评价学生的防范能力。考核可以采取笔试、实操考试和项目评估等形式。制定科学合理的评价标准，明确各项考核内容的评分标准和权重，确保考评的公平性和客观性。评价标准应注重学生的实际防范能力，而不仅仅是理论知识。建立考评结果反馈机制，将考评结果及时反馈给学生，并根据考评结果为学生提供个性化的辅导和支持。反馈机制应包括成绩分析、问题诊断和改进建议等内容。对在考评中表现优秀的学生给予奖励，如颁发证书、奖学金和推荐就业机会等，激励学生主动学习和掌握防范知识。同时，可以将防范网络电信诈骗的学习和考评结果纳入综合素质评价体系，为学生的综合素质评价和未来发展提供参考。

结语

在互联网时代，高校大学生防范网络电信诈骗的安全教育具有重要意义。通过强化网络安全教育、推动网络安全文化建设、建立健全防范制度、开展实战演练和加强社会合作，可以有效提高大学生的防范意识和自我保护能力。高校应积极探索和实践多种教育形式，构建完善的防范网络电信诈骗的安全教育体系，为大学生的健康成长保驾护航。

参考文献

[1] 盛天姿，潘金刚．大学生在电信网络诈骗中的心理分析与防范机制研究 [J]．江苏经贸职业技术学院学报，2023(05)：40-42.

[2] 张文明．大学生网络电信诈骗特征与防范教育探究 [J]．兰州工业学院学报，2023,30(02)：135-137.

[3] 徐嘉来．大学生防范电信诈骗的国内外有效防范策略研究 [J]．法制博览，2023(03)：15-17.

[4] 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.

[5] 李元临．高校电信网络诈骗防范策略相关探析 [J]．法制博览，2022(07)：136-138.

作者简介：于成程，1993年10月，男，汉，江苏宿迁，硕士研究生，扬州大学，思政讲师，研究方向：思想政治教育。

基金项目：本文系2023年度江苏高校哲学社会科学研究一般项目：“协同育人”视域下高校防范网络电信诈骗的对策研究（编号：2023SJSZ1217）。