大学生网络安全素养提升路径与教育机制构建

陈慧义
齐鲁工业大学（山东省科学院） 山东济南 250253

摘 要：随着信息技术的高速发展和互联网的普及，网络安全问题日益凸显，大学生作为网络的主要使用群体，其网络安全素养的提升显得尤为重要。本文系统分析当前大学生网络安全素养现状，探讨提升路径与教育机制构建的必要性。通过构建理论框架，结合实践案例，提出多层次、系统化的网络安全教育策略，涵盖课程设置、实践训练、技术支持与文化引导。研究认为，只有整合高校资源、政府政策和社会力量，形成协同育人机制，才能有效提升大学生的网络安全意识和防护能力。本文为高校网络安全教育改革提供理论参考和实践路径。

关键词：大学生；网络安全素养；教育机制；提升路径；协同育人

引言

信息技术的迅猛发展极大改变了社会生产生活方式，网络已成为大学生日常学习、交流和生活的重要平台。与此同时，网络安全风险不断升级，网络诈骗、信息泄露、恶意攻击等问题频发，给大学生个人隐私和财产安全带来严重威胁。当前，部分高校网络安全教育尚未形成系统有效的机制，学生的网络安全意识和防护能力存在明显不足。提升大学生的网络安全素养已成为高校教育的重要任务和国家网络安全战略的关键环节。本文旨在通过分析大学生网络安全素养现状，探索科学合理的提升路径和教育机制构建方案，推动高校网络安全教育的系统化、专业化和创新化，保障学生健康安全的网络环境，促进其信息化时代综合素质的发展。

一、大学生网络安全素养现状分析

1.网络安全意识普遍薄弱

尽管网络已深度融入大学生生活，但其安全意识仍显不足。部分学生对网络风险认识模糊，缺乏主动防护意识。数据显示，大多数大学生无法准确辨别网络钓鱼、恶意软件等威胁，随意点击不明链接和下载来源不明软件，导致安全事故频发。网络安全宣传存在“走过场”现象，内容形式单一，难以引起学生持续关注。

2.安全技能缺乏系统培训

目前高校多以理论宣讲为主，缺少针对性强、实践性高的网络安全技能培训。学生缺乏密码管理、防火墙使用、恶意程序识别及应急处理等实用技能，面对复杂多变的网络环境时应对不足。实训资源匮乏、课程体系不完善限制了安全技能的提升，致使学生理论与实践脱节，难以构建完整的安全防护能力。

3.教育机制缺乏协同联动

网络安全教育涉及信息技术、法制教育、心理健康等多领域，但高校普遍缺乏跨部门协同机制，教育资源分散且重叠度高。政策支持不足，激励机制缺失，难以形成持续推进的教育合力。学校、家庭及社会的沟通互动有限，未能形成有效联动网络，制约了网络安全素养的全面提升。

二、大学生网络安全素养提升路径探索

1.强化课程体系建设

构建一个涵盖基础理论、技术技能、法律法规以及心理素质等多维度内容的课程体系，是提升大学生网络安全素养的根本保障。网络安全作为一个跨学科领域，涉及计算机科学、信息技术、法律政策及心理学等多个方面，高校在课程设计时应综合考虑各个维度，确保教育内容的科学性和系统性。具体而言，课程内容应细分为不同层次和类别，满足不同专业背景和学习阶段学生的需求，形成由浅入深、循序渐进的教学架构。

此外，课程设计不仅仅停留在理论传授层面，更应强调实践能力的培养。引入案例教学法，以真实的网络安全事件为案例，帮助学生深入理解网络攻击的原理、

课题项目：本文系齐鲁工业大学（山东省科学院）教学研究项目“高校安全教育推进机制研究与实践”成果（编号：z202304-4）。

作者简介：陈慧义（1978-10--），男，汉族，山东省兰陵县人，硕士研究生，讲师，主要从事安全教育的研究工作。

防护措施及法律责任。项目驱动教学则鼓励学生参与实际项目，从问题发现、方案设计到实施验证，提升综合解决能力。通过模拟真实工作环境的实验项目，学生能够更好地将理论知识应用于实践，锻炼发现问题和解决问题的能力。

与此同时，课程体系还需不断更新与完善，紧跟网络安全技术的快速发展和新的安全威胁。例如，人工智能安全、云安全和物联网安全等新兴领域的内容应及时纳入课程体系，确保学生掌握前沿技术与最新防御手段。学校还应结合行业标准和认证体系，设置相关认证课程，提高学生未来就业的竞争力。通过多元化和层次化的课程体系建设，大学生的网络安全素养能够得到全面而系统的提升。

2.推动实践教学与技能训练

网络安全能力的提升关键在于大量实践训练和真实场景模拟。理论知识固然重要，但缺乏实践操作的支持，学生难以真正掌握安全技能并应对复杂的网络威胁。高校应加大投入，建设设备先进、功能完善的网络安全实验室，为学生提供全面的操作平台。这些实验室应涵盖攻防对抗、漏洞扫描、入侵检测、加密技术等关键技能训练内容，帮助学生熟悉各种安全工具和技术流程。

实践教学的内容应丰富多样，不仅包括课堂实验，还应拓展至校内外竞赛和攻防演习。网络安全竞赛为学生搭建了展示技能和团队协作的舞台，激发其学习兴趣和动力。定期举办攻防演习，通过模拟真实网络环境中的攻击与防御，提升学生的应急响应能力和实际操作水平。

产教融合是推动实践教学的重要途径。通过引入互联网企业和安全厂商的专家资源，建立校企联合实训基地，让学生在真实项目环境中锻炼技能。行业专家的指导不仅能够丰富教学内容，更能帮助学生理解企业对网络安全人才的具体需求，增强职业导向性。校企合作还可促进学生实习和就业，形成教育与产业的良性循环。实践教学的不断深化，为大学生提供了扎实的技能基础，培养出既懂理论又善实操的网络安全人才。

3.构建多方协同育人机制

网络安全素养的提升不仅依赖高校教育，还需要家庭和社会的共同参与，形成多方协同的育人体系。高校应主动整合校内不同部门资源，形成跨学科、跨职能的协作机制。例如，信息技术部门负责技术培训和资源建设，思想政治教育部门注重安全意识和责任感培养，心理健康中心关注学生的心理调适与压力管理。各部门资源共享，优势互补，提升教育整体效能。

校外合作同样重要。高校应加强与互联网企业、政府网络安全监管机构以及专业培训机构的沟通与合作，联合开展网络安全宣传、培训和实战演练，搭建多元化的实践平台。政府可提供政策支持和安全法规指导，企业则能提供技术与资源支持，形成政产学研用的紧密协作，提升教育针对性和实效性。

家庭教育在学生网络安全素养培养中扮演不可忽视的角色。家长应关注学生网络使用行为，引导他们正确、安全地使用网络资源，培养良好的网络使用习惯。学校与家庭应建立沟通机制，及时分享学生的学习情况和网络行为表现，形成教育合力。

社会层面应营造安全、健康的网络环境，通过舆论引导和法律法规的落实，遏制网络犯罪和不良信息传播，为大学生的网络安全学习和应用提供良好的外部条件。通过多方协同，构建一个全方位、立体化的网络安全素养教育体系，促进大学生综合素质的提升，有效应对日益复杂的网络安全挑战。

三、大学生网络安全教育机制创新

1.利用信息技术提升教育效果

随着信息技术的飞速发展，网络安全教育的形式与内容也迎来了深刻变革。大数据分析和人工智能技术的引入，为个性化教育提供了坚实技术支撑。通过对学生学习行为数据的采集和智能分析，可以深入洞察学生在网络安全知识掌握上的薄弱环节和兴趣点，进而动态调整教学内容与教学策略，实现精准教学。基于数据驱动的教学优化不仅提高了教学效率，也增强了学生学习的针对性和主动性。

此外，在线学习平台和移动应用的开发，为学生提供了多样化的学习渠道和资源，丰富了网络安全教育的载体。互动性强的学习工具，如在线测验、实时答疑、模拟攻击防御游戏等，不仅提升了学习的趣味性和参与感，也有效促进知识的内化和技能的掌握。

虚拟现实（VR）技术则为网络安全教育带来了沉浸式体验，学生可身临其境地模拟网络攻击与防御场景，感知安全威胁的真实感，提升安全意识和应急反应能力。通过构建真实情境，虚拟现实技术能够有效弥补传统课堂难以实现的实践教学缺陷，增强教育的实效性和体验感。未来，随着技术的不断成熟，人工智能驱动的个性化辅导和智能评估将进一步成为网络安全教育的重要组成部分，推动教育模式向智能化、精准化方向发展。

2.完善激励评价体系

科学合理的评价体系是提升网络安全教育质量的核

心保障。当前，评价机制往往偏重知识考核，忽视学生安全行为和实践能力的培养。构建多维度的评价指标体系，涵盖学习态度、理论知识掌握、实践操作能力以及安全意识的行为转化，对于全面衡量学生的网络安全素养至关重要。

评价方式应注重过程与结果的结合。过程性评价强调学生在学习中的积极参与度、实践操作表现和团队协作能力，有助于激励学生持续投入学习。结果性评价则通过阶段性考试、技能测评、竞赛成绩等形式，对学生学习成效进行客观量化。

为了增强激励效果，高校应引入证书制度，将网络安全技能认证与学分挂钩，提升学生学习的成就感和荣誉感。设置专项奖励和激励政策，鼓励学生参加校内外安全竞赛、创新实践项目及社会公益活动，促进理论与实践的紧密结合。同时，评价结果应及时反馈教学管理层面，为教师优化教学内容和方法提供依据，形成良性循环，促进网络安全教育质量的持续提升。

3. 加强师资队伍建设

师资力量直接决定网络安全教育的教学质量和水平。高校应高度重视网络安全教师的专业能力培养，建立多层次、全方位的培训体系，提升教师的技术素养和教学能力。通过定期组织技术培训、行业实践和学术交流，教师能够及时掌握网络安全领域最新动态和前沿技术，保持教学内容的先进性和实用性。

鼓励教师参与科研项目和产学研合作，提升理论研究与教学实践的深度融合。通过团队建设和教学研讨活动，促进教师间经验共享与创新教学方法的探索。高校还应引入互联网企业和安全机构的专家资源，开展联合教学和讲座，丰富课程内容，增强教学的针对性和行业适应性。

建立激励机制，激发教师的教学热情和创新活力。例如，将教学成果纳入职称评审和绩效考核体系，鼓励教师在教学方法、课程内容和实践平台建设方面进行创新。完善教师职业发展路径，支持其持续学习与专业成长，为网络安全教育提供坚实的人才保障。

四、案例分析与实践应用

1. 某高校网络安全素养提升实践

某高校基于对学生网络安全素养现状的调研，整合校内资源，构建多层次的网络安全教育体系。学校不仅完善了网络安全课程体系，增加案例分析和实战演练，还积极搭建网络安全实践平台，提供模拟攻击防御和漏洞检测等操作环境。通过组织安全知识竞赛和攻防演练，极大激发了学生的学习兴趣和实践积极性。

学生参与率的提升显著增强了教育的覆盖面和影响力。教学满意度调查显示，多数学生认为课程内容实用，实践环节有助于掌握关键技能。网络安全事件的发生率明显降低，学生的信息安全防护意识得到了有效提升。学校还积极引导学生参与国内外网络安全竞赛，提升综合素养和竞争能力，促进人才培养质量的稳步提高。

2. 互联网企业与高校合作模式

互联网企业凭借丰富的行业资源和技术优势，成为高校网络安全教育的重要合作伙伴。某知名企业与多所高校建立战略合作关系，联合开展网络安全培训、实战演练和创新项目。企业专家参与课程设计和课堂教学，分享最新安全威胁信息和防护技术，增强课程的实践针对性。

合作模式不仅提供了真实案例和实战平台，还拓展了学生的职业视野和就业渠道。企业定期举办讲座和技术沙龙，促进学生了解行业发展趋势和岗位需求。联合开展的攻防竞赛和实习项目，提高学生的技术能力和团队合作精神。高校与企业的深度合作，为网络安全人才培养提供了强有力的支撑，推动校企协同育人机制的不断完善。

结束语

大学生网络安全素养的提升是构建安全网络空间的重要基础，关乎学生个人权益和国家信息安全战略的实施。通过构建系统化、科学化的提升路径和创新教育机制，能够有效增强大学生的网络安全意识与技能，推动其全面发展。信息技术的赋能为教育提供了广阔空间，多方协同促进资源整合，构筑了坚实的育人平台。

未来，应持续完善课程体系，丰富实践教学内容，提升师资力量，创新评价激励机制，推动网络安全教育向智能化、精准化方向发展。高校要不断深化教育理念，强化产教融合，整合政府、企业及社会资源，共同营造安全、健康的网络环境。唯有如此，才能使大学生具备应对复杂网络挑战的能力，保障信息社会的稳定和持续发展。

参考文献

[1] 张玲.网络环境与文献信息资源共享[J].津图学刊，2000，(01)：20-28.

[2] 董波.网络营销——企业经营新理念[J].互联网周刊，2000，(13)：26.

[3] 曹礼贵，申卫国.电脑网络技术的安全管理[J].湖南医科大学学报(社会科学版)，2000，(01)：93-94.

[4] 袁建华，张怀仁.浅析教育改造在监管安全中的地位和作用[J].犯罪与改造研究，2000，(04)：37-39.

[5] 张嗣胜.建设安全文明镇促进经济繁荣发展[J].特区经济，2000，(04)：54-55.