大学生网络安全通识教育的重要性和对策

张　耀　王怡赫
河南工业大学马克思主义学院　河南郑州　450000

摘　要：随着信息化社会的到来，大学生在享受网络便利的同时，也面临着日益严峻的网络安全挑战。网络安全问题不仅关乎个人隐私保护，还直接影响到社会的稳定与发展。当前大学生在网络安全方面的认知和防护能力普遍较弱，高校的网络安全教育体系存在滞后性，难以满足实际需求。针对这一问题，提升大学生的网络安全意识和自我防护能力已成为刻不容缓的任务。为此，应从课程体系建设、教育内容创新、跨学科合作以及信息技术应用等方面入手，推动网络安全教育的多维发展。通过政府与高校的紧密合作，构建全社会共同参与的网络安全教育生态，能够有效提升大学生的网络安全素养，为构建更加安全的网络环境奠定基础。

关键词：大学生；网络安全；通识教育；教育对策

引言

随着数字化时代的迅猛发展，网络已成为大学生日常学习和生活的重要组成部分。无论是在学术研究、社交互动，还是在消费和金融活动中，网络安全问题都与每个人的切身利益息息相关。然而，当前许多大学生在面对复杂的网络安全威胁时，往往缺乏必要的安全防护意识和应对能力。根据多项调查数据显示，大学生群体中的网络安全风险意识普遍较弱，且防护措施滞后，易成为网络犯罪的目标。高校在这一领域的教育也显得不足，缺乏系统性的课程设计和实践环节。因此，针对大学生群体开展网络安全通识教育，提升其网络安全认知水平和自我防护能力，已成为当务之急。通过系统的教育模式和策略可以有效减少网络安全事件的发生，推动社会网络安全环境的改善。

一、大学生网络安全教育的现状与问题

1.大学生网络安全教育的现状

随着互联网技术的快速发展，大学生群体的网络使用频率和范围日益增大，网络安全问题也愈加突出。尽管大学生普遍具备一定的网络操作基础，但在网络安全方面的认知和防护能力却较为薄弱。目前，高校网络安全教育主要停留在基础性的知识层面，缺乏系统性与实践性的结合。许多大学生在日常网络使用中容易忽视潜在的安全威胁，例如钓鱼网站、病毒感染、个人信息泄露等，且应对这些问题的能力不足。调查显示，虽然学生对于网络安全事件有一定了解，但在实际操作中仍难以做到有效防护。高校的网络安全教育课程大多以理论为主，互动性和实践性较差，教学内容和形式没有与时俱进，没能全面覆盖最新的网络安全技术与威胁。此外，许多高校未将网络安全教育纳入必修课程，导致这一领域的教育普及程度较低，大学生的网络安全防护能力亟待提升。

2.大学生网络安全教育存在的问题

大学生网络安全教育面临多重问题，主要体现在教育内容滞后、教育形式单一及学生参与度不足等方面。

（1）随着网络技术的迅猛发展，许多高校的网络安全课程内容未能及时更新，仍集中于传统的基础知识，未能有效应对新兴的网络威胁，如勒索病毒、APT攻击等高级攻击方式。

（2）现有的教育形式过于依赖课堂讲授，缺乏互动性和实践环节，学生难以通过实践积累应对复杂网络安全事件的经验。许多高校仅通过零散的讲座或专题活动进行网络安全普及，缺少系统性和连贯性。

（3）部分高校未将网络安全教育纳入核心课程，导致学生对网络安全的重视不足，防护意识薄弱。

因此，网络安全教育急需加强内容更新与实践教学，提升学生的安全防护能力。

二、大学生网络安全通识教育的重要性

1.提升大学生的网络安全意识

在数字化时代，网络安全已成为社会稳定和个人

基金项目：本文系河南省哲学社会科学规划项目《基于州权理论的卡尔霍恩国家理论跟踪研究》阶段性成果，项目编号：2021CZZ018

生活的关键组成部分。大学生群体作为数字技术的主要使用者之一，其网络安全意识的提升具有重要的社会意义。当前，大学生在日常生活中频繁使用各类网络服务，包括在线支付、社交平台、学习平台等多方面应用，但许多学生对潜在的网络安全风险缺乏足够的认知，容易忽视个人信息保护的重要性。尽管部分大学生能够识别常见的网络威胁，如病毒攻击和钓鱼邮件，但对更复杂的安全隐患如数据泄露、身份盗用等仍缺乏应有的警觉性。随着网络犯罪手段的不断翻新，大学生的网络安全意识急需得到全面提升。通过加强网络安全教育，培养大学生对各类网络安全威胁的敏感性，增强其保护个人数据、识别虚假信息、避免网络诈骗的能力，不仅能够保护学生个人隐私，还能在更广的社会层面减少信息泄露和网络犯罪的发生。提升网络安全意识是增强大学生自我防护能力的基础，是应对日益严峻网络安全形势的重要前提。

2.提高大学生的自我防护能力

大学生的网络安全防护能力直接影响其在网络环境中的安全性与稳定性。当前，大部分大学生在使用网络时，往往没有进行足够的安全防护措施，例如使用弱密码、不定期更换密码、点击不明链接等，这些行为使其面临较高的网络风险。自我防护能力不仅仅是对常见威胁的预防，还包括对复杂安全事件的应对能力。提升大学生的网络安全防护能力，需要从两方面入手：一是提高技术性防护能力，二是增强应急反应能力。

技术性防护能力包括对各种防病毒软件、加密工具、身份验证手段等的熟练掌握，帮助学生在日常网络活动中采取有效的防护措施。

应急反应能力的培养则要求大学生能够在遇到网络安全事件时，及时识别问题、采取恰当的处理措施，并避免事态的进一步恶化。例如，当发现账户被盗用时，能够迅速修改密码、挂失银行账户并报警等，这一系列行动需要大学生具备足够的安全知识储备和实践经验。

因此，提升大学生的网络安全防护能力，不仅依赖于理论教育，更需要通过实践演练、技能培训等方式，加强其实际操作能力。

3.减少网络安全事件对社会的影响

网络安全事件的频繁发生不仅对个体造成直接损害，还对社会产生了深远的负面影响。从个人隐私泄露、财产损失到大规模的数据泄露、金融诈骗等，网络安全事件带来的影响具有普遍性和深远性。对于大学生群体而言，缺乏足够的安全防护意识和能力，不仅容易成为网络攻击的受害者，也可能无意中参与到网络犯罪活动中，如通过不当途径传播病毒、参与网络赌博等，从而影响整个社会的网络安全环境。如果大学生群体能够有效提升网络安全意识和自我防护能力，能够降低其自身和他人遭遇网络攻击的风险，进而减轻社会层面上网络安全事件的发生率。此外，大学生是未来社会的栋梁，其网络行为和安全意识的提升将直接影响到社会未来的信息安全格局。加强大学生网络安全教育，不仅是保护个体利益的需要，也是保障社会整体网络安全的必然选择。通过强化网络安全教育，社会可以培养出具备较强网络安全意识和防护能力的人才，从而有效减少网络安全事件的发生，保障社会的稳定与和谐[1]。

三、大学生网络安全教育的对策与建议

1.深化网络安全课程体系建设，增强实践性与针对性

在大学生网络安全教育中，课程体系的完善至关重要。当前，很多高校的网络安全教育偏重理论知识的传授，缺乏与实际应用相结合的实践内容，导致学生的安全防护能力未能得到有效提升。因此，构建一个系统、实践性强、针对性明确的网络安全课程体系成为必要的改进方向。

（1）课程内容应紧跟网络安全技术的发展和新兴的网络安全威胁。例如，考虑到勒索病毒、APT攻击等高级持续性威胁的普及，课程应加入相关防护知识和应急响应策略。

（2）课程设计应注重培养学生的实际操作能力，包括网络攻击与防护演练、漏洞扫描、入侵检测等。通过模拟真实网络攻防场景，学生能够获得与理论学习不同的实践经验，提高他们应对实际网络安全事件的能力[2]。

（3）课程应根据不同学科、不同专业的需求，进行定制化设计，确保学生能在专业背景下掌握与自身领域相关的网络安全知识。例如，计算机专业的学生应深入学习网络攻防技术，而非计算机专业的学生则应侧重于信息保护、隐私安全等内容。

2.推动跨学科合作，融入网络安全教育的多维视角

网络安全问题涉及多个学科领域，单一学科的知识难以全面应对复杂的安全挑战。因此，推动跨学科合作，融入多维视角进行网络安全教育，能有效提升大学生的网络安全综合素质。

（1）法律学科能够帮助学生理解网络安全中的法律框架和道德规范，特别是关于数据隐私、网络犯罪等方面的法律责任。通过系统的法律教育，学生能够意识到网络

安全不仅仅是技术问题，更涉及法律合规和伦理约束。

（2）社会学和心理学的知识也对网络安全教育具有重要意义。随着社交网络和数字平台的普遍使用，网络行为的社会学分析变得愈加重要。通过研究网络暴力、诈骗、隐私泄露等社会现象，学生能够更好地理解和应对网络空间中的社会风险。

（3）管理学角度的融合有助于提升学生的网络安全管理能力，包括企业信息安全管理、风险评估与应对等方面。通过跨学科的结合，学生不仅能掌握技术性的防护知识，还能培养综合分析能力，形成多维视角，从而更好地应对日益复杂的网络安全问题。

这种跨学科的教育模式为学生提供了一个全面的学习框架，使其具备解决实际网络安全问题的全方位能力[3]。

3.加强信息技术在教育中的应用，提高教育互动性和参与感

信息技术的快速发展为网络安全教育提供了新的机遇。将信息技术与教育相结合能够极大提升网络安全教育的互动性和参与感。利用现代网络平台、虚拟仿真技术、在线学习工具等手段，可以构建一个动态、互动的学习环境。例如，通过模拟网络攻击场景，学生能够在虚拟环境中亲身体验网络安全事件，从而深入理解防护措施的实际效果。此类模拟不仅增强了学生的实际操作能力，还能帮助学生更加直观地认识到网络安全的重要性。此外，基于大数据和人工智能的技术，教育者能够根据学生的学习进度和掌握情况，提供个性化的教学内容和实时反馈，确保每个学生都能获得适合自己的学习体验。通过在线讨论、在线测试等互动方式，学生能够更积极地参与到网络安全教育中来，从而提高整体学习效果。

4.政府和高校联动，构建全社会共同参与的网络安全教育生态

构建全社会共同参与的网络安全教育生态，离不开政府与高校的紧密合作。政府应当出台相关政策，推动网络安全教育的普及，尤其是在高校层面。可以通过制定政策要求高校将网络安全教育纳入到通识课程体系中，确保每位大学生都能接触到网络安全相关内容。

此外，政府可以通过资金支持、政策引导等方式，鼓励高校和企业、科研机构开展合作，利用行业资源推动网络安全教育的创新。例如，定期举办网络安全培训、讲座和竞赛活动，不仅能提升学生的实际操作能力，还能激发他们对网络安全的兴趣和探索精神。高校也应当加强与政府、企业的合作，推动网络安全课程体系的不断优化，提升教育内容的时代适应性和实践性。通过这种政府、高校与社会各界的联动合作，能够形成覆盖各个领域、层次的网络安全教育体系，为学生提供全面的网络安全教育支持[4]。

结论

随着信息社会的不断发展，网络安全问题对大学生的个人安全、学术研究以及社会稳定带来了深远影响。网络安全通识教育不仅能够提升大学生的安全防护意识，还能增强其应对网络风险的实际能力。加强网络安全教育体系的建设，结合信息技术和跨学科合作，将为学生提供更加全面、实践性的学习体验。同时，政府与高校的联动、全社会共同参与，将为网络安全教育营造更加良好的发展环境[5]。构建完善的网络安全教育体系，提升大学生的网络安全素养，最终将推动社会整体网络安全水平的提升，为应对未来日益复杂的网络安全挑战奠定坚实的基础。

参考文献

[1]李媛媛，袁玉林，随力瑞.基于KAP理论的大学生网络安全教育研究[J].中国安全科学学报，2024，34（05）：1-8.

[2]徐灿灿，张梦慧.“三全育人”视域下大学生网络安全教育路径研究[J].网络安全技术与应用，2024，（03）：82-85.

[3]李爱贞.新媒体时代大学生网络安全教育路径探析[J].信息系统工程，2023，（09）：153-156.

[4]万涛，谢昕.基于PBL的大学生网络安全通识教育[J].中国现代教育装备，2021，（21）：7-8+14.

[5]陈慧铭.大学生网络安全教育存在的问题及对策研究[D].华中师范大学，2019.