大数据背景下大学生信息安全意识培养探索

李润启
内蒙古医科大学　计算机信息学院　内蒙古呼和浩特　010059

摘　要：在大数据的时代背景下，高等院校中信息安全教育显得尤为关键。伴随着数据资源的深度开发与利用，高校学子们的个人资料正遭受着隐私泄露和网络侵袭的双重风险。但目前，教育领域的信息安全教学存在教学内容单调、体系化程度不高的现象，这直接导致学生们信息安全观念淡薄，面对繁杂的网络环境时防护能力不足。本文深度剖析了信息安全教学中所面临的若干难题，包括教学内容与现实脱节、教学体系不完善以及学生对于信息安全问题的忽视等核心问题。针对这些挑战，文章提出了一系列应对策略，如强化信息安全课程建设、完善信息安全意识培育体系、丰富教学手段等，目的是提高大学生的信息安全防范意识，增强其在海量数据环境下的自我保护能力。借助全面而富有创造性的教学方法，高等教育机构能够显著提升学生的信息安全综合素质，确保他们在信息化社会中能够维护个人隐私和网络安全。

关键词：大数据；信息安全；大学生意识；教育策略

引言

近年来，大数据（big data）一词越来越多地被提及，人们用它来描述和定义信息爆炸时代产生的海量数据。大数据与网络相辅相成，一方面，网络的发展为大数据带来了更多数据、信息与资源；另一方面，大数据的发展为网络提供了更多支撑、服务与应用。大数据是网络的基础，这意味着大数据更多来源于网络，因此，在大数据时代保障网络安全，使得大数据的利用合法、安全，必将成为高难度的世界课题。目前，大学生依赖网络程度越来越高，无论是学习、娱乐或是购物等方面，根据《中国互联网信息中心CNNIC发布的第37次中国互联网络发展状况统计报告》，2015年人均周上网时长达26.2个小时，相当于每天上网3.75小时，其中学生群体、特别是大学生成为贡献上网时长的主力军。

一、大数据时代信息安全的重要性

1.信息安全对大学生隐私的保护

在数字化浪潮席卷之际，高校学子们的个人隐私正遭遇着前所未有的威胁。互联网技术的广泛应用，使得学生们的姓名、身份证号码、通讯方式、行踪等私密信息在学习、生活及社交互动中不断被搜集与应用。众多学子对于信息安全的重要性认识不足，往往在不经意间在网络上暴露了关键信息，从而变成了网络诈骗、身份盗用等不法行为的受害者。不少社交网络和电商网站强制用户提交详尽的个人信息，而这些信息一旦遭到黑客攻击或平台数据发生泄漏，隐私权遭受侵害的风险便会大大增加。信息外泄不仅可能带来经济损失，还可能造成心理负担，乃至影响学子的学业发展和求职机会。鉴于此，提升学子们的信息安全意识至关重要，需要通过教育途径指导他们如何在网络世界中守护个人信息。同时，高等院校也需加强网络安全设施的建设，为学子们营造一个安全稳定的网络空间，从根本上降低信息泄露的可能性。

2.网络安全与社会稳定的紧密关联

在大数据时代的背景下，网络安全与社会的和谐安定密不可分，信息的快速传递及其安全防护对社会稳定性的影响至关重要。互联网及信息技术的深入应用使得网络安全问题不再仅仅关乎个人隐私的泄露，而是扩展到了公共安全、经济秩序乃至国家安全的层面。新型的风险如黑客入侵、网络信息战以及网络恐怖活动等不断出现，对社会稳定构成了重大威胁。比如，金融行业的数据遭泄露可能引起市场波动，政府系统的安全被突破则可能导致社会动荡和不安。作为未来社会支柱的大学生群体，他们的网络安全意识强弱直接影响着整个社会

项目基金：内蒙古医科大学2023年度校级教育教学改革研究与实践项目：大数据时代增强大学生信息安全素养的探索与研究（项目编号：NYJXGG2023058）。

作者信息：李润启，男（1977.08–），汉族，河北南宫人，硕士，讲师，研究方向：计算机技术和信息安全。

的网络安全状况。但目前，很多大学生对于网络安全的重要性缺乏足够的认识，他们缺乏应对网络威胁和防止信息泄露的技能。因此，提升大学生网络安全教育水平，不仅是保护他们个人利益的必要措施，也是确保社会稳定的关键行动。通过开展全面的网络安全教育，让学生能够有效识别和防御各类网络风险，这样在未来他们就能为社会的安全稳定贡献自己的力量。

二、大学生信息安全意识培养的主要问题

1.信息安全教育内容的局限性

现阶段我国高校在信息安全教学方面面临着明显的短板，其核心问题在于教学内容过于狭隘及与现实脱节。众多院校的教程依旧固守传统的网络安全入门知识以及初级防护手段，未能紧跟信息安全领域的最新发展动态。实际上，信息安全所面临的威胁早已不止于传统的病毒、木马攻击，更涵盖了数据窃取、网络钓鱼、社交操纵等多种复杂攻击手段，而这些新型威胁在现有课程中往往被一笔带过。同时，许多课程过分强调理论知识传授，却忽略了学生实践技能的培养，导致他们在面对实际信息安全问题时手足无措。这种教学上的不足使得学生虽然掌握了信息安全的基础知识，却难以在现实生活中灵活运用。高校应改革课程体系，融入最新的安全威胁信息，并强化实操训练，以提高学生应对信息安全挑战的实际能力。

2.信息安全意识培养缺乏系统性

在课程设置上，信息安全教育常常是零星分布于个别课程之中，并未形成独立且完整的课程体系。这种散乱的教学布局使得学生们对信息安全知识的掌握缺乏连贯性和完整性，难以构筑起全面的安全防护意识。此外，信息安全教育的连贯性不足，往往是在特定时期或事件触发后才被关注，缺少持续的、系统的教育规划。例如，不少高校仅在新生报到或是遭遇网络安全事故之后才匆匆开展相关教育，而日常教学中却忽视了持续性的教育安排。同时，信息安全知识在不同学科之间的融合度不高，缺少跨学科的综合培养，使得学生们难以将安全知识灵活运用于各种实际情境。由此可见，高等院校亟需建立一个更加全面的信息安全意识培养体系，从教学内容、教学方法到教学时间分配等多个维度进行综合规划和优化整合。

3.大学生对信息安全关注度不高

高校学子对于信息安全的重要性认识不足，这在很大程度上制约了信息安全意识的提升。大量学子对于信息安全的概念理解浮于表面，误以为它仅仅关乎技术层面，却忽略了它在个人隐私保护、学业发展、职业规划等多个领域的深远作用。这种片面的看法导致他们在日常生活中很少主动维护个人信息安全，对信息泄露可能带来的风险视而不见。学子们对信息安全知识的学习热情不高，这主要是因为信息安全教育的教学材料和方式过于单调，缺乏足够的吸引力。有些学子甚至觉得信息安全问题与他们相去甚远，认为自己不太可能成为网络攻击的对象，因此缺乏学习信息安全知识的积极性。这种淡薄的关注态度不仅阻碍了他们信息安全意识的建立，还让他们在遭遇信息安全挑战时缺乏必要的防护手段。比如，在利用社交网络、电子邮箱等服务时，他们常常忽视了密码安全、账号防护等基础安全措施的重要性。为了增强高校学子对信息安全的重视程度，有必要在教学内容和方式上做出创新，结合真实案例来加深他们对信息安全紧迫性的认识。

三、大学生信息安全意识培养的策略研究

1.加强信息安全教育内容建设

为了增强高校学子在信息安全领域的防范意识，关键在于不断丰富和完善信息安全教育的课程体系。目前，信息安全教学往往聚焦于网络安全的初级知识，比如防病毒、密码设置等基础内容。但随着科技的快速进步，网络攻击手段也趋向多样化，数据泄露、社交欺诈、网络诱骗等新型风险逐渐成为安全领域的一大挑战。因此，教学材料需与时俱进，迅速整合新的安全威胁及防护策略。信息安全教育不应仅限于技术层面，还应包括法律规范、道德伦理等维度，以帮助学生全方位地认识到信息安全的重要性及其对个人乃至社会的深远影响。

在课程设计的层面，应重视理论知识与实践技能的融合。除了常规的课堂讲授，还应增设各类实践性课程，例如实验室的攻防演练、模拟数据泄露应对等，通过动手实践来增强学生的操作技能和应急反应能力。这样的实践环节可以帮助学生更加直观地认识到信息安全问题的复杂性和紧迫性，进而培养出更加强化的安全防护意识。同时，课程设计应考虑到学生的不同专业背景，针对性地开发教学单元，确保每位学生都能学到与其所学专业紧密相关的信息安全知识。

2.健全信息安全意识培养制度

高校需打造一个全面的教育体系，把信息安全教育的培养纳入学校的教学大纲之中。这涉及到在各个学科的教学中穿插信息安全的知识点，保证学生在掌握专业技巧的同时，也能了解并运用信息安全的基本技巧。譬如，在理工科如计算机科学与工程等专业，可以将信息

安全设置为必选课程，而在人文社科领域，则可将信息安全教育作为选修课或公共课程的一部分。信息安全的教育培训需要保持连贯性和持久性，不应仅仅局限于新生入学时的启蒙教育或是特定事件后的临时培训。高校应当制定长远的战略规划，把信息安全意识的提升贯穿于大学教育的始终。比如，每个学期可以组织相关的主题讲座或研讨活动，邀请行业内的安全专家来讲解最新的安全资讯和技术进展，以此来不断更新和加强学生的安全防护意识。

高校还需构建信息安全意识培养的评价体系，通过定期的测验和调研，对学生的信息安全知识和意识程度进行评估。这不仅有助于掌握教学成效，也能为教学内容和方式的优化提供数据参考。评估结果应当作为学生综合素养评价的一部分，并纳入到学校的教学质量审核体系中。另外，高校应设立信息安全紧急事件响应机制，并定期实施应急预案的演练，以提升学生在面对真实安全事件时的快速反应和正确处理能力。

3.促进信息安全教育形式的多样化

传统的教学模式在唤起学生对信息安全领域的热情与重视上常常显得力不从心，故而，丰富信息安全教育的手段显得尤为关键，它是增强教学成效的核心手段之一。可以借助现代的多媒体手段，打造高度互动的教学资源，比如开发网络课程、制作动态教学视频、设计仿真教学软件等，旨在营造一个轻松愉悦且充满趣味的学习氛围，让学生在轻松、有趣的环境中掌握信息安全的核心内容。将课堂教育与课余活动有机融合，同样是实现教育多元化的关键路径。学校可以举办信息安全竞赛、黑客马拉松、CTF挑战赛等多样化活动，以竞技和挑战的方式激发学生主动探索和学习信息安全知识的动力。这些活动不仅有助于提升学生的动手实践能力，更能点燃他们对信息安全领域的兴趣火花，为培育未来的信息安全行业精英奠定基础。

校园信息安全教学应积极整合校内外各类资源，推动跨领域、跨部门的协同工作。高校可以引入业界及科研机构的信息安全专家，举办专题讲座或专业技能培训，传授最新的安全技术动态与实例分析，使学生深入了解行业面临的安全难题及其应对策略。同时，通过与相关企业的深度合作，为学生提供信息安全领域的实践机会，让他们亲身体验并解决现实中的安全问题，实现理论知识与实践技能的有机结合。多元化的教学手段不仅适应了学生群体的多样化学习需求，也提升了信息安全教学的实用现实性。借助多种教学途径，学生们不仅能够掌握更为全面的信息安全知识体系，还能在动手操作中提升解决具体问题的能力，进而有效增强信息安全意识的培育成效。

结语

在大数据时代背景下，提升信息安全意识显得格外关键，特别是在高等教育领域。本篇文章对现阶段高校信息安全教育的状况进行了详尽探讨，指出了众多迫切需要解决的难题，例如教学内容与现实脱节、教育体系不完整，以及学生们对信息安全重要性认识不足等问题。这些问题的存在严重制约了信息安全意识的培育，使得学生们在面临日益繁杂的网络风险时，难以迅速而有效地应对。为了克服这些困难，文中提出了强化信息安全教学内容、完善信息安全意识培育体系，以及多样化教育模式的对策。通过充实教学内容、构建全面的教育体系，以及运用多元化的教学手段，有望全方位提高学生的信息安全意识，使其在应对信息安全风险时更为自信和镇定。进一步地，这些对策的落实不仅有助于学生个人隐私和数据安全的保护，也为社会培养了更多具备安全意识和责任感的公民。

参考文献

[1]熊友玲，孙茜.大数据背景下高校信息网络安全及防范对策概述[J].网络安全和信息化，2023（7）：121-123.

[2]贾钢涛.新时代加强高校意识形态安全教育的新探索——评《大数据时代高校意识形态安全教育研究》[J].重庆邮电大学学报：社会科学版，2021，33（1）：1.

[3]李亚鑫，吴曼，刘晓玲.大数据时代大学生个人信息安全保护策略研究——以河北工程技术学院为例[J].文学少年，2021（29）：0265-0265.

[4]李岩.生态环境大数据技术专业大学生网络安全意识培养实践研究[J].环境工程，2023，41（7）：I0007-I0007.

[5]马晓明，杨国燕.大数据时代高校“信息安全技术”OBE翻转课堂的探索与实践[J].教育教学论坛，2023（18）：113-116.

[6]宁东.基于大数据背景下高职院校网络与数据安全治理体系研究——以天津城市职业学院为例[J].天津职业院校联合学报，2023，25（11）：64-69.