文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

网络安全意识培养融入计算机通识教育的研究

王永
西安科技大学高新学院
DOI:10.12238/acair.v3i3.15553

[摘　要] 在当今数字化时代,信息技术的迅猛发展使得计算机广泛应用于生活的各个角落,成为人们日常不可或缺的重要工具。然而,网络安全问题也随之而来,其重要性日益凸显。将网络安全意识培养融入计算机通识教育,对于提升全民的网络安全素养具有深远意义。本文从课程体系构建、教学方法创新和评价体系建立三个维度展开研究,旨在探索如何在计算机通识教育中有效融入网络安全意识培养。通过优化课程设计、创新教学方式以及完善评价机制,本文为高校计算机课程改革提供了有益的参考和借鉴,以期为培养具备良好网络安全素养的人才奠定坚实基础。
[关键词] 网络安全意识；计算机通识教育；课程体系；教学方法；评价体系
中图分类号：G633.67　**文献标识码：**A

Research on Integrating Network Security Awareness Cultivation into Computer General Education

Yong Wang
Xi'an University of Science and Technology High tech College

[Abstract] In today's digital age, the rapid development of information technology has made computers widely used in every corner of life and become an indispensable tool for people's daily lives. However, cybersecurity issues have also emerged, and their importance is becoming increasingly prominent. Integrating the cultivation of cybersecurity awareness into computer general education has profound significance for enhancing the cybersecurity literacy of the entire population. This article conducts research from three dimensions: curriculum system construction, teaching method innovation, and evaluation system establishment, aiming to explore how to effectively integrate network security awareness cultivation into computer general education. By optimizing course design, innovating teaching methods, and improving evaluation mechanisms, this article provides useful reference and inspiration for the reform of computer courses in universities, in order to lay a solid foundation for cultivating talents with good network security literacy.
[Key words] cybersecurity awareness; Computer general education; Curriculum system; Teaching methods; Evaluation system

引言

在数字化浪潮席卷全球的当下,计算机已成为现代社会的核心工具,而网络安全问题也如影随形,威胁着个人隐私、企业利益乃至国家安全。计算机通识教育作为普及信息技术的重要途径,亟待融入网络安全意识培养,以应对日益严峻的网络威胁。然而,如何在有限的课程时间内实现知识传授与意识培养的有机结合,仍是一个亟待解决的问题。本文将从课程体系构建、教学方法创新和评价体系完善三个方面展开深入研究,探索在计算机通识教育中融入网络安全意识的有效路径,为提升全民网络安全素养提供理论支持与实践参考。

1 网络安全意识培养融入计算机通识教育的课程体系构建

1.1课程目标设定

在构建计算机通识教育课程体系时,明确的课程目标是实现有效教学的基础。课程目标的设定应涵盖知识、能力和意识三个层面,以全方位提升学生对网络安全的认知与实践能力。

1.1.1知识目标

课程首先需明确学生应掌握的网络安全基础知识,这包括网络安全的基本概念、常见的网络威胁类型(如病毒、木马、网络钓鱼等),以及主流的防护技术(如防火墙、加密技术、入侵检测系统等)。通过系统的知识传授,学生能够对网络安全领域形成清晰的认知框架,为后续的实践操作奠定坚实的理论基础。

1.1.2能力目标

除了知识的传授,课程还应注重学生能力的培养。具体而言,

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

学生需要具备识别网络安全风险的能力,能够在复杂的网络环境中敏锐地发现潜在的安全隐患。同时,学生应掌握防范网络攻击的技能,学会运用各种防护工具和技术来抵御外部威胁。此外,处理安全事件的能力也至关重要,学生应能够在安全事件发生时迅速采取有效的应对措施,降低损失并恢复系统正常运行[1]。

1.1.3意识目标

网络安全意识的培养是课程的核心目标之一。通过课程学习,学生应深刻认识到网络安全的重要性,并在日常生活中自觉遵守网络安全规范,如不随意泄露个人信息、不点击不明链接、不使用弱密码等。这种意识的养成将使学生在未来的网络生活中更加谨慎和自律,从而有效减少因个人疏忽而导致的安全问题。

1.2课程内容设计

在课程内容设计方面,我们精心规划了多个模块,旨在全面覆盖网络安全的理论知识与实践应用,帮助学生系统地掌握网络安全的核心内容。

1.2.1网络安全基础

本模块旨在为学生奠定坚实的网络安全理论基础。通过深入浅出的讲解,学生将了解网络安全的基本概念,包括网络空间的安全定义、边界与内涵。同时,课程将回顾网络安全的发展历程,从早期的简单防护到如今复杂多变的安全环境,让学生清晰地看到技术进步与威胁演变的脉络。此外,还将着重强调网络安全在当今数字化社会中的重要性,帮助学生建立对网络安全的整体认识,为后续学习奠定基础。

1.2.2常见网络安全威胁

在这一模块中,我们将详细剖析当前网络环境中常见的安全威胁。通过深入讲解网络钓鱼的手段与防范方法、恶意软件的传播途径与破坏机制,以及数据泄露的常见原因与后果,学生将对网络安全风险的多样性有更深刻的理解[2]。课程将结合实际案例,展示这些威胁如何影响个人隐私、企业运营乃至国家安全,从而增强学生对网络安全风险的敏感度。

1.2.3网络安全防护技术

本模块聚焦于网络安全防护技术的原理与应用。学生将学习防火墙的分类与配置、加密技术的算法与应用场景,以及身份认证机制的多种实现方式。通过理论与实践相结合的教学方式,学生不仅能理解这些技术的原理,还能掌握如何在实际环境中运用它们来构建安全的网络环境。课程还将引导学生思考如何根据不同的安全需求选择合适的防护技术组合,以实现最佳的防护效果。

1.2.4网络安全实践案例

理论与实践相结合是本课程的重要特色之一。在这一模块中,我们将通过分析真实的网络安全事件案例,让学生直观地感受网络安全威胁的现实危害。课程将详细剖析事件的起因、经过与应对措施,引导学生思考如何在类似情境中采取有效的防护策略。通过案例分析,学生不仅能够积累实践经验,还能培养分析问题与解决问题的能力,为未来应对复杂多变的网络安全挑战做好准备。

1.3课程结构安排

1.3.1理论与实践相结合

合理安排理论教学和实践教学的比例,通过实验、项目等方式让学生在实践中加深对网络安全知识的理解。

1.3.2课程衔接与递进

根据学生的认知规律,设计课程内容的衔接和递进关系,使学生能够逐步掌握网络安全知识和技能。

2 网络安全意识培养融入计算机通识教育的教学方法创新

在当今数字化时代,传统的教学方法已难以满足学生对网络安全知识的多样化需求。为了提高教学效果,激发学生的学习兴趣,培养其实践能力和创新思维,我们从案例教学法、项目驱动教学法和线上线下混合式教学三个方面进行了创新探索。

2.1案例教学法

案例教学法通过分析真实案例,引导学生思考和解决问题,将抽象的理论知识与实际问题相结合,增强学生的学习兴趣和实践能力。以下是实施步骤:

2.1.1精选案例

案例选择是成功的关键。我们挑选了具有代表性、典型性和时效性的网络安全案例,如“勒索病毒事件”“数据泄露事件”等。这些案例涵盖热点问题,反映最新技术动态和安全威胁。通过生动案例,学生直观感受网络安全问题的严重性和复杂性,激发学习兴趣。

在选择案例时,注重多样性,涵盖网络攻击、恶意软件传播、数据泄露、身份盗窃等事件。每个案例都经过严格筛选,确保内容真实、数据准确,能够引发学生思考。例如,“勒索病毒事件”展示了网络攻击的巨大危害,“数据泄露事件”揭示了数据管理漏洞。这些案例帮助学生全面了解网络安全,为深入学习奠定基础。

2.1.2案例分析

在案例教学过程中,教师引导学生对案例进行深入分析。学生需要围绕事件的起因、经过和后果展开讨论,分析其中涉及的技术问题、管理漏洞以及法律风险。通过小组讨论、课堂辩论等形式,学生能够从不同角度思考问题,培养他们的批判性思维和分析问题的能力。同时,教师在讨论过程中适时引导,帮助学生梳理思路,确保讨论的深度和广度[3]。

案例分析的过程不仅是对事件的回顾,更是对问题的深入剖析。教师会引导学生从技术、管理、法律等多个维度进行分析。例如,在分析“勒索病毒事件”时,学生需要探讨病毒的传播途径、攻击方式、防护措施以及事件对企业运营的影响。通过小组讨论,学生能够分享不同的观点和见解,激发彼此的思维火花。教师则在讨论中提供必要的背景信息和专业知识,帮助学生更好地理解案例中的复杂问题。

2.1.3案例总结

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

案例总结是案例教学的关键环节,旨在帮助学生从实际案例中提炼经验教训,加深对网络安全知识的理解。教师引导学生回顾案例中的关键点,总结成功经验和失败教训。例如,在“勒索病毒事件”中,学生总结出定期备份数据、及时更新系统、安装防护软件等有效措施,同时认识到忽视漏洞和缺乏应急响应机制的严重后果。这些总结不仅巩固了知识,还提升了学生解决实际问题的能力。

2.2项目驱动教学法

项目驱动教学法是一种以项目为导向的教学模式,通过让学生参与实际项目,培养他们的实践能力和创新思维。这种方法能够将理论知识与实际操作紧密结合,增强学生的学习动力和成就感。

2.2.1设计项目

项目的设计应紧密结合网络安全的实际需求,具有一定的挑战性和实用性。我们设计了多个与网络安全相关的项目,如“校园网络安全防护方案设计”“个人网络安全防护系统搭建”等。这些项目不仅涵盖了网络安全的核心知识点,还涉及实际应用中的技术选型、方案设计和实施过程。通过参与这些项目,学生能够将课堂上学到的理论知识应用到实际问题中,提升他们的综合能力。

2.2.2项目实施

在项目实施过程中,学生需要分组合作,共同完成项目任务。教师在这一阶段主要扮演指导者的角色,为学生提供必要的帮助和支持。教师通过定期检查项目进度、解答技术难题、组织小组讨论等方式,确保项目的顺利进行。通过团队合作,学生不仅能够培养团队协作能力,还能学会如何在团队中发挥自己的优势,共同解决复杂问题。此外,项目实施过程中的实际操作经验能够让学生更好地理解网络安全技术的应用场景和效果。

2.2.3项目评价

项目评价是项目驱动教学法的重要环节。通过项目成果展示和评价,学生能够了解自己的不足之处,同时也为教师提供教学反馈。在项目展示环节,学生需要向全班同学和教师展示他们的项目成果,包括项目的设计思路、实施过程和最终效果。教师和其他同学可以通过提问、点评等方式,对项目进行深入的分析和评价。评价标准不仅包括项目的完成度和技术水平,还包括团队合作能力、创新能力等方面的综合表现。通过这样的评价方式,学生能够清晰地认识到自己的优势和不足,为今后的学习和实践提供改进方向。

2.3线上线下混合式教学

线上线下混合式教学是一种结合线上教学资源和线下课堂教学优势的教学模式。它能够充分利用网络教学平台的便捷性和课堂教学的互动性,提高教学效果和学习效率。

2.3.1线上资源建设

线上资源的建设是混合式教学的基础。我们利用网络教学平台,建设了丰富的网络安全教学资源,包括教学视频、课件、在线测试、案例库等。这些资源不仅涵盖了网络安全的理论知识,还提供了大量的实践操作指导和案例分析。学生可以根据自己的学习进度和需求,自主选择学习内容,进行线上学习和练习。同时,线上资源还提供了互动讨论区、答疑区等功能,方便学生与教师和其他同学进行交流和互动。

2.3.2线下课堂教学

线下课堂教学是混合式教学的重要组成部分。在课堂教学中,教师通过讲解、讨论、答疑等方式,引导学生深入学习网络安全知识。教师可以根据线上资源的学习情况,有针对性地讲解重点和难点内容,帮助学生更好地理解知识。同时,教师还可以结合线上资源中的案例和实践操作,组织学生进行课堂讨论和实践演练。通过线下课堂教学,学生能够与教师和其他同学面对面交流,及时解决学习过程中遇到的问题,增强学习的互动性和趣味性。

3 网络安全意识培养融入计算机通识教育的评价体系建立

通过考试、作业等方式,评价学生对网络安全基础知识的掌握情况。通过实验、项目等方式,评价学生在网络安全防护方面的实践能力。通过问卷调查、行为观察等方式,评价学生的网络安全意识是否得到增强。在教学过程中,通过课堂表现、作业完成情况、实验操作等进行形成性评价,及时了解学生的学习进度和存在的问题。在课程结束时,通过考试、项目成果展示等方式进行终结性评价,全面评价学生的学习效果。引导学生进行自我评价和同伴评价,让学生了解自己的优点和不足,同时也增强学生的自我反思能力和团队协作能力。将评价结果及时反馈给学生,让学生了解自己的学习情况,明确改进方向。根据评价结果,教师对教学内容、教学方法和教学过程进行反思和改进,不断提高教学质量。

4 结语

将网络安全意识培养融入计算机通识教育是适应时代发展的必然要求。通过构建科学合理的课程体系、创新教学方法和建立完善的评价体系,可以有效提升学生的网络安全意识和防护能力。在今后的研究中,还需要进一步探索如何将网络安全意识培养与学生的实际生活紧密结合,使学生能够在日常生活中自觉践行网络安全规范,为构建安全、和谐的网络环境做出贡献。

[参考文献]

[1]刘建伟,杜瑞颖,毛剑,等.浅析大类通识教育背景下网络空间安全专才培养模式建设[J].工业和信息化教育,2019(4):5.

[2]林嘉燕.“互联网+”时代大学生信息安全通识教育研究[J].数字技术与应用,2020,38(1):3.

[3]肖俊生,闫培玲,郑凤武.计算机网络原理驱动的网络安全课程教学研究[J].中国宽带,2023,19(9):148-150.

作者简介：

王永(1987--),男,汉族,陕西西安人,硕士,讲师,研究方向：网络安全和人工智能。

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.