

# 高校计算机网络信息安全及防护策略分析

魏涛

(江西科技学院, 江西南昌 330098)

摘要: 互联网技术的不断发展为人们学习和生活带来便利性, 同时也带来挑战性。在新媒体时代, 人们运用计算机网络教学、生产日益普遍, 面临的网络安全形势也日益复杂。高校作为应用计算机数量最密集的单位之一, 网络信息安全和防护至关重要, 一旦高校的网络受到攻击, 将造成极大的损失。基于此, 文章将分析高校计算机网络信息安全及防护的意义, 高校计算机网络信息管理的不足之处, 以及在此基础上重点分析高校计算机网络信息安全及防护的创新路径, 目的是顺应计算机网络信息管理和安全防护的新形势, 为高校计算机网络信息安全及防护提供一些参考。

关键词: 高校; 计算机; 网络信息; 安全防护

《教育部关于加强教育行业网络与信息安全工作的指导意见》提出全面提高教育行业网络与信息安全意识, 形成与教育信息化发展相适应的、完备的网络与信息安全保障体系, 支撑教育现代化事业健康持续发展。计算机网络深入到人们生活的方方面面, 与人们生活密不可分, 尤其是高校已经顺应时代发展, 将计算机网络技术融入教学和管理之中, 有效提高高校教学和管理效率。高校作为使用计算机数量密集的单位, 需要贯彻落实文件精神, 加强网络信息安全管理, 防止出现计算机网络中病毒、被黑客攻击的情况, 这会大大影响高校科研进展、日常教学工作的展开。

## 一、高校计算机网络信息安全及防护的意义

### (一) 有利于维持高校教学活动

高校是培养高质量人才的重要阵地, 能够为国家和社会输送推动经济发展的专业素质人才, 以此推进建设创新型国家, 中国特色社会主义建设。高校依托互联网背景建立计算机网络安全信息及防护体系是教育改革的重要内容, 有效推动了高校日常教育教学管理, 实现对高校教育资源的整合应用。为应对复杂的网络安全形势, 高校应该建立科学稳定的信息安全及防护体系, 保证高校计算机网络的健康安全, 从而确保高校科研成果的安全, 高校教学活动符合预期目标。高校将计算机网络技术融入教学体系之中有效促进教学体系的现代化发展, 因此高校需要加强高校计算机网络信息安全防护的严谨性, 为高校开展教学活动提供基础设施和软件安全支持, 避免网络威胁对高校教学活动造成影响。

### (二) 有利于推动高校信息化建设

在当今时代, 信息化建设已成为推动各行各业迈向现代化的核心驱动力, 高等教育领域亦是如此。随着高校教学改革的不断深化, 教学体系的革新与升级势在必行, 其中计算机网络技术与高校发展深度融合正是这一变革的关键。计算机网络技术全面融入高校发展的各个环节, 不仅能够实现教学体系的现代化转型, 而且能够促进高校教学与计算机技术的有效对接, 为教育体系的优化提供坚实的技术支撑。在此基础上, 高校应充分利用计算机网络技术的优势, 构建安全高效的校园网络环境, 以教学信息化为核心, 强化计算机网络安全体系的建立。这一举措旨在维护教育体系的创新活力与稳定运行, 同时确保高校信息数据的安全稳定。为实现理想效果, 高校需根据自身实际情况, 量身定制科学的保障机制, 加大对网络资源的投入, 支持计算机网络信息安全体系的建设。最终, 通过这些措施, 高校将能够成功打造出一个智能化的校园环境, 为学生提供更加便捷、安全、高效的校内网络服务体系。

### (三) 有利于净化校园网络环境

随着计算机网络信息和教育体系的深度融合, 高校教学体系

建设已经步入正轨。但是, 高校还需要在此基础上加强计算机网络信息安全和防护建设, 维持校园网络环境的健康安全, 促进教学内容的丰富多元, 提高高校师生的数字化素养。高校计算机网络信息安全和防护建设至关重要, 有利于维持校园网络安全, 为提高学生思想道德品质营造良好的校园环境。时代发展日新月异, 互联网技术渗透到学生学习和生活的各方面, 大学生使用网络日益频繁, 接触网络信息频率更高, 而大学生处在形成正确成熟的世界观、人生观、价值观的重要时期, 对互联网上良莠不齐的信息有时难以辨别真假美丑。针对这种情况, 高校应该净化校园网络安全, 构建网络信息安全和防护体系, 过滤网络上的不良信息, 降低大学生与网络不良信息的接触频率, 以此引导大学生身心健康发展, 培育学生健全的人格。

## 二、高校计算机网络信息管理的不足之处

### (一) 配置方面问题

在高等教育环境中, 教师与学生的日常学习交流依赖计算机网络信息的利用。然而, 计算机配置方面的种种不足, 例如常见的计算机漏洞、内部文件异常, 以及网络适配器更新滞后等问题, 不仅影响师生的使用体验, 而且可能影响数据的稳定传输, 导致数据丢失。鉴于互联网技术的飞速发展与应用需求的日益增长, 提升计算机硬件配置与软件更新, 成为促进高校计算机网络系统高效稳定运行的关键一环。因此, 高校管理层应加强提高计算机配置的重视程度, 并将观念付诸实践。

### (二) 系统漏洞问题

在高等院校师生使用计算机网络的过程中, 存在对计算机网络安全问题不够重视的问题, 其中, 最大的问题就是系统漏洞。系统漏洞会给黑客可乘之机, 给黑客入侵高校计算机网络的通道。黑客借此连接高校计算机设备, 窃取计算机内的关键信息, 从而实施违法活动, 这是高校计算机网络信息安全及防护管理中常见的问题, 需要高校网络管理人员特别关注。

### (三) 计算机病毒问题

在高校计算机网络信息安全及防护中, 木马和计算机病毒是其中一项威胁因素。高校师生数量多, 为方便使用, 经常使用移动存储设备, 导致个人设备中的计算机病毒植入到校园内的计算机之中。一旦木马和计算机病毒被植入电脑之中, 他们便会利用自身程序入侵电脑, 导致电脑瘫痪, 无法使用, 甚至破坏计算机中存储的文件, 大大影响教师的教学活动和学生的学习研究活动。

### (四) 用户安全意识薄弱问题

在高校计算机网络使用中, 用户的安全意识薄弱是威胁计算机网络信息安全的重要因素之一。部分师生对计算机使用的安全认识和技术不了解, 导致计算机网络出现故障, 例如, 缺乏信息

意识,导致用户身份证、学号等涉密信息被发布到网上;密码设置简单,容易遭到黑客攻击;错误删除某些安全防护程序;安装有经过安全监测的程序等,因此,高校计算机网络信息安全及防护需要加强师生的安全防范意识。

### 三、高校计算机网络信息安全及防护的创新路径

#### (一) 做好文件加密和备份处理,加大网络系统访问控制

当下互联网安全形势比较严峻,为防止重要文件被破坏,高校师生应对重要文件做好加密和备份工作,一方面,在电脑存放重要文件时应利用系统的加密功能设置字母和数字相结合的复杂密码,并且定期更换密码,不留给黑客可乘之机,最大程度防止他人破解密码;另一方面,师生在存储重要文件时要养成备份的习惯,最大程度避免重要文件的泄露。此外,很多高校出现网络安全问题是因为访问控制活动没有有效展开,基于此,高校网络管理中心需要加强对校园网访问控制管理活动的力度,有效杜绝外部病毒和黑客攻击,杜绝外部软件植入校园网。高校可以通过技术手段控制访问校园网的用户、借助身份证避免无关人员访问等措施来提升校园网管理的有效性。

#### (二) 加强与第三方的合作,培养网络安全技术人才

当下,高校需要具有较高水平网络信息安全及防护能力的高素质人才,高校中网络管理人员的信息安全和防护应用能力相对较低,导致高校在新媒体时代下面临着网络安全问题的威胁。基于此,高校应加强与第三方的合作,加大力度培养网络安全技术人才,通过和科技企业建立良好的合作关系,使科技企业为高校提供网络信息安全和防护方面的技术指导和支撑,以期优化校园网络信息安全,提高师生的数字素养和网络安全防护意识。与此同时,高校可以和企业合作制定人才培养计划,加大资金投入,大力投入相关资源,为高校培养专业的网络信息安全及防护人员提供坚实的保障。在新媒体时代下,信息化技术快速发展,高校提高安全防范能力才能维护师生的校园信息安全,为师生在高校学习研究提供最佳的互联网服务和安全保障。

#### (三) 做好网络安全宣传工作,增强师生防范意识

高校计算机网络信息安全及防护不只是网络安全部门的事情,也需要全校师生的参与。高校宣传部门可以在师生日常生活和学习中加强网络信息安全教育,增强师生的信息安全意识。在这一过程中,高校计算机网络信息安全和防护工作能够进一步推进,为日后的网络信息管理打下坚实基础。基于此,高校宣传部应根据高校特点,开展和计算机网络相关的活动,通过各种有效方式吸引全校师生参加,调动高校师生学习网络信息安全知识的主观能动性。首先,高校宣传部可以开展和网络信息安全及防护有关的座谈会、培训班等活动,提高师生的信息安全防护技能。其次,高校宣传部可以在公众场所张贴醒目的标语,在校内广播播放计算机网络信息安全及防护的安全常识,营造浓厚的信息安全防护氛围,使高校师生在吃饭、散步之中潜移默化地增强信息安全防范意识。最后,高校可以通过社团活动、网络转发等形式加大对网络安全法的宣传力度,使师生认识到网络信息安全的重要性,也认识到网络信息背后隐藏的安全隐患,这样,高校师生在使用互联网时会更加注意,使用杀毒软件清除病毒、自觉安装正版软件等等,保证电脑系统平稳运行,减少病毒干扰。

#### (四) 推动设备建设,优化管理系统

在构建高校计算机网络信息安全体系时,高校应紧密结合国家信息化发展战略的核心要义,强化网络防御能力,促进防护网络的全面构建。高校应依托现有的信息化建设和理念,致力于校园网络基础设施的智能化升级,为网络安全运营奠定坚实的基础,

与此同时,建立一套适应时代需求的设备维护机制,确保网络管理体系的完整性。第一,高校做好基础设施建设,将高校发展理念和校园网络基础设施的深度融合,保证这些设施既便于未来升级改造,又具备良好的扩展性。在此基础上,高校应加速推进校园有线与无线网络的建设,实现对平板电脑、智能手机、笔记本电脑等多类终端的全面支持,为师生营造一个便捷、高效、安全的校园网络环境。通过完善基础设施,高校能够构建一张覆盖全校的内部网络。第二,高校需要构建信息存储安全管理体系,将计算机软件的安全管理纳入体系之中,应用安全管理软件、入侵检测系统及防火墙等先进技术,为高校计算机网络信息安全体系的稳定运行筑起坚实的防护墙。与此同时,高校加大对网络信息安全检测能力的投入,不断完善网络防护体系,确保防御机制的有效运作,为高校网络空间安全提供强有力的后盾支持。

#### (五) 加强合理应用,完善管理机制

高校加强计算机网络信息安全及防护的建设,需要完善管理机制,加强互联网技术的合理应用。第一,高校应加强防火墙的应用。防火墙指的是对高校计算机信息树立起一座像墙一样的安全保护屏障,合理应用防火墙有助于减少计算机安全问题的产生,防止外界黑客、病毒对校园信息安全造成危害。现实情况下,大多电脑会提示用户电脑安全问题,吸引用户注意力,但是没有相应地为用户提供防火墙,因此,高校应针对这一问题,制定相应的措施,通过考虑客户客观情况,识别客户的信息数据,针对性地完善防火墙的功能,使防火墙建设和用户需求相匹配,保护用户的数据存储安全。第二,高校应该在建设计算机网络信息安全及防护技术的基础上完善管理机制,将互联网安全防护制度精细化,将计算机网络安全管理工作落到实处。与此同时,高校应制定实施计算机网络信息安全的责任管理机制,如果高校计算机安全及防护机制出现问题,需要将责任落实到个人,加强网络管理者的责任感。如果因为高校相关人员违反规章制度发生安全问题,高校应及时处理,加强培训,避免出现互相推脱的情况。

### 四、结束语

综上所述,高校计算机网络信息安全及防护有利于维持高校教学活动,有利于推动高校信息化建设,有利于净化校园网络环境。当下,高校计算机网络信息安全及防护管理面临一些挑战,例如,配置方面问题,系统漏洞问题,计算机病毒问题,用户安全意识薄弱问题,希望通过做好文件加密和备份处理,加大网络系统访问控制;加强与第三方的合作,培养网络安全技术人才;做好网络安全宣传工作,增强师生防范意识;推动设备建设,优化管理系统;加强合理应用,完善管理机制一系列措施能够加强高校计算机网络信息安全及防护体系,保障教学教育管理工作顺利进行。

### 参考文献:

- [1] 韩爽. 高校计算机网络信息管理及其安全防护策略 [J]. 数码世界, 2020 (11): 261-262.
- [2] 姚子扬. 论高校网络安全问题及防护对策 [J]. 科技风, 2020 (18): 135.
- [3] 李晶晶, 杨红森. 计算机网络信息技术在高校中的应用及其安全防护 [J]. 数字技术与应用, 2020, 38 (03): 196-197.
- [4] 盛权为. 大数据背景下高校计算机信息安全防护策略 [C]// 教育理论研究 (第六辑). 长沙医学院; , 2019: 1.
- [5] 邱焕然, 张铷钊. 高校计算机网络信息安全及其防护对策 [J]. 家庭生活指南, 2019 (01): 268.