

“互联网+”发展下的高校计算机实验室网络安全管理

唐剑平

广州应用科技学院 广东肇庆 526072

摘要: 互联网信息技术的快速发展,加速了“互联网+”时代的到来,也对高校计算机网络安全管理的发展有了更高的要求。但是高校计算机实验室网络安全管理水平还有待进一步的提高,这样才能更好的保护实验室的各种信息和数据。下面,本文基于“互联网+”发展下的高校计算机实验室网络安全管理进行分析和探讨,希望对高校计算机实验室网络安全管理能够有所帮助。

关键词: “互联网+”; 高校; 计算机实验室; 网络安全管理

前言

随着互联网技术的广泛应用,为高校的多个领域提供了极大的便利,学校的各个专业对计算机实验室的使用率也越来越高,各种各样的网络安全问题也层出不穷。为了保证师生可以安心的使用计算机实验室,那对于解决计算机实验室网络安全管理中出现的问題势在必行。只有这样才能保证教师的教学效率和教学效果,保证学校学生的信息数据和科研数据不会出现泄漏的情况,让学校持续发展。

1. “互联网+”发展下的高校计算机实验室网络安全管理的重要性

高校在“互联网+”的影响下,不仅在学校管理中引进了大量先进的网络技术,很多专业的课程也增加了计算机实践课,来帮助学生更好的掌握专业知识,提高实践能力。这虽然让学校的管理工作和学生的学习都变得更加便利,但也对网络安全管理提出了更高的要求。只有加强高校计算机实验室的网络安全管理,才能让这一切都能有所保障^[1]。一旦高校计算机实验室的网络安全管理出现问题,不仅可能会造成学生个人信息的泄漏,教师教课资源和学生实践数据的丢失,甚至学校的保密性科研成果也会被他人窃取,这对于高校造成的损失是不可估量的。所以高校要重视计算机实验室的网络安全管理工作,从多方面出发,共同致力于提高计算机实验室的网络安全管理水平。

2. “互联网+”发展下的高校计算机实验室网络安全管理中的问题分析

2.1 部分师生网络安全意识薄弱

部分非计算机专业的教师,在使用计算机时,由于网

络安全意识薄弱,并未及时对计算机进行病毒查杀、漏洞修补等安全防护,使得计算机的安全防护比较薄弱,容易中病毒或者被他人侵入,导致某些重要的信息被泄漏或者丢失。

高校部分学生的心智发育尚未完全成熟,对新鲜事物的敏感性较强,在计算机实验室上课时,可能会为了更多的了解某个事物,而在无意识中,采取“翻墙”等会对实验室网络安全造成影响的行为。同时由于部分学生的网络安全意识薄弱,对网络上各种信息的辨识能力不强,不能清楚的分辨非法网站和病毒文件,导致被盗取个人信息和个人财产^[2]。甚至有些学生过分追求物质上的享受,但由于自身条件有限,便通过网络平台进行“校园贷”“裸贷”,最终可能因为还不上贷款影响自己的学习和生活。

2.2 管理人员的能力有待提高

高校计算机实验室的网络安全管理,不仅包含计算机软硬件的安装与维护,还包含实验室数据的管理和保护,因此对实验室管理人员的能力要求较高。但目前高校计算机实验室的软硬件更新和故障维修不太及时,实验室的网络安全措施做的也不太到位,这些对于教师的教学效果会有一定的影响,长此以往也不利于学校的发展。

2.3 网络安全管理资金不足

部分高校虽然重视计算机实验室的网络安全管理工作,但是对进行网络安全管理的资金投入较少,导致计算机实验室的设备没有得到及时的更新,一些新型的网络安全管理技术受到计算机设备的影响,也不能发挥出应有的优势。这样就会使一些不法分子抓住漏洞,窃取学校师生的个人信息或者科研成果,给学校带来巨大的损失和伤害。

2.4 网络安全管理制度不完善

高校计算机实验室虽然都有相应的网络安全管理制度,但还需要继续完善。特别是操作规范方面,因为没有明确的规定,学生在使用计算机设备时,没有按照正确的操作方式进行操作,导致计算机出现问题时,无法对其进行相应的教育和惩罚。在管理方面,也没有明确管理人员的义务和责任,导致在出现问题时,不能追究到具体的责任人,影响高校计算机实验室的网络安全管理效果。

3. “互联网+”发展下的高校计算机实验室网络安全管理的对策分析

3.1 提高师生的网络安全意识

非计算机专业的教师要主动和计算机专业的教师进行沟通和交流,向他们学习计算机网络安全相关的知识,并将其运用到实际的计算机实验室网络安全管理中,避免发生不必要的损失。同时,在计算机实验室上课时,向学生讲述维护计算机网络安全的重要性,结合具体的网络安全意识薄弱造成的悲剧实例,引起学生对网络安全的重视,提高学生的网络安全意识。

高校也可以结合本校学生的实际情况,开展相应的网络安全教育课程,为学生普及网络安全知识,帮助学生了解更多网络安全知识,可以辨别常见的网络安全骗局。特别是对于近年来频发的校园网络诈骗事件,进行详细的讲解和分析,让学生能够清楚的了解其中的弊端,提高网络安全意识,远离网络诈骗。除此之外,高校还可以组织和举办网络安全实践活动,如网络安全知识进校园、网络安全社会实践等多种活动,激发学生了解网络安全的兴趣,让网络安全知识得到更广泛的传播^[3]。

3.2 增强管理人员的能力

互联网技术日新月异,高校计算机实验室的网络安全管理人员也应该不断学习新的知识和技术,如上网实名制、上网日志留存、数据备份加密、防篡改等网络安全新技术,提高实验室网络安全水平。对于实验室计算机设备的软硬件也要及时更新,避免因为软硬件过于老旧,影响计算机的运行速度,导致教师的教学进程缓慢。

高校也要选择一些专业的、能力较强的人员负责高校计算机实验室的网络安全管理,并加强对他们的培训和考核,督促他们不断提高自身网络安全管理的能力。同时,高校可以定期聘请一些优秀的计算机人才,对学校计算机

实验室的网络安全管理进行检查和维护,并对学校计算机实验室网络安全管理人员进行培训,帮助他们快速提升网络安全管理能力。

3.3 合理增加网络安全管理资金

计算机实验室网络安全管理的重要性对高校来说不言而喻,高校应该合理增加网络安全管理资金,让计算机设备的软硬件都能得到及时的更新,保证新型的网络安全管理技术能够充分发挥应有的安全防护效果,让学校的网络安全防御更强。此外,高校也应对计算机设备的日常维护和故障维修投入一定的资金,日常维护工作做的到位,可以很好的延长计算机的使用寿命,故障维修也比直接购买新的计算机设备省钱^[4]。

高校在日常加大网络安全管理的资金投入,使计算机实验室网络安全管理得到提升,也可以降低数据被盗窃的可能性,减少了不必要的损失,这其实也从另一方面促进了高校更好的发展。

3.4 完善网络安全管理制度

首先,要完善操作规范相关的管理制度。对学生的计算机操作方式进行规范的培训,要求学生在操作时,严格按照规范的操作方式进行操作,避免操作不规范引发的各种网络安全问题。同时,对学生的操作进行监督和管理,如果发现某位学生没有按照规范进行操作,可以先对他进行指导和教育,屡教不改者对其采取相应的惩罚措施。

其次,要明确管理人员的责任和义务。对管理人员的责任和义务进行明确的规定,并制定相应的惩罚制度,让他们在日常的管理工作中知道自己该做什么,该怎么做,如果在管理工作中出现问题,直接追责到人,按照相应的惩罚制度对其进行惩罚。这样可以让网络安全管理人员主动规范自身的行为,在管理工作中尽职尽责,让计算机实验室的网络安全管理更有保障。同时,对于优秀的管理人员也要给予相应的表扬和认可,让网络安全管理工作人员对工作充满信心和干劲,一起把网络安全管理工作做得更好。

4. 结语

在享受“互联网+”带来的便利的同时,高校也要加强对计算机实验室网络安全管理工作,保证学校各种信息和数据的安全性。通过提高师生的网络安全意识,让他们学会辨别各种网络骗局。同时,要增强管理人员的能力,不断提高他们的专业能力,为计算机实验室的网络安全保驾护航。高

校也要合理增加网络安全管理的资金, 保证计算机设备的软硬件能够得到及时的更新, 并完善网络安全管理制度, 提高计算机实验室的网络安全管理水平。

参考文献

[1] 沈燕美, 程国玉. 高校计算机实验室安全管理与改革的研究 [J]. 数字通信世界, 2023, (09): 170–172.

[2] 杨乐. 关于高校计算机实验室网络安全管理的研究 [J]. 办公自动化, 2022, 27(09): 56–58+42.

[3] 赵旭华. 高校计算机实验室网络安全管理研究 [J]. 中国教育信息化, 2021, (01): 60–65.

[4] 文理卓, 李东宸, 郑宪等. 浅析高校网络安全管理及对策探讨 [J]. 中国管理信息化, 2019, 22(14): 153–154.